UNIVERSITY OF DERBY

A FRAMEWORK FOR UNDERSTANDING INTELLECTUAL PROPERTY RISKS TO COLLABORATION WHEN USING DIGITAL TWIN BASED DECISION SUPPORT SYSTEMS

Jennifer Clementson

Doctor of Philosophy 2025

A FRAMEWORK FOR UNDERSTANDING INTELLECTUAL PROPERTY RISKS TO COLLABORATION WHEN USING DIGITAL TWIN BASED DECISION SUPPORT SYSTEMS

JENNIFER CLEMENTSON

A submission in partial fulfilment of the requirements of the University of Derby for the award of the degree of Doctor of Philosophy.

College of Science and Engineering September 2025

Contents

List of Tables

List of Figures

List of Abbreviations and Definitions

Abbreviations

AEC	Architectural, Engineering and Construction
ASCII	American Standard Code for Information Interchange
AWS	Amazon Web Services
CAD	Computer Aided Design
CASP	Constraint Answer Set Programming
DaaS	Data as a Service
DB	Deutsche Bahn
DEMATEL	Decision Making Trial and Evaluation Laboratory (Si et al, 2018)
DO	Digital Object
DSD	Digital Schiene Deutschland
ECCA	Engineering Resilient Systems Cloud Computing Architecture
FINTECH	"Digital innovations and technology-enabled business model innovations in the financial sector." (British Standards Institution, 2024a)
FRAND	Fair, reasonable and non-discriminatory terms
GDPR	General Data Protection Regulations
gRPC	Cross-platform, open-source Remote Procedure Call (RPC) framework, used to connect services.
GSN	Goal Structuring Notation
HaDEA	European Health and Digital Executive Agency
HVAC	Heating, Ventilation and Air Conditioning
IIoT	Industrial Internet of Things
IISE	Institute for Innovation in Sustainable Engineering, University of Derby
IGEM	Institution of Gas Engineers & Managers https://igem.org
IP	Intellectual Property
IPR	Intellectual Property Rights
JSON	JavaScript Object Notation (https://www/json.org)
LeMo	Leveraging Big Data to Manage Transport Operations
MaaS	Maintenance as a Service
MBSE	Model Based Systems Engineering
MQTT	Message Queuing Telemetry Transport (https://mqtt.org)
NDT	National Digital Twin
PHM	Prognostics and Health Management
RO	Research Objective
ROSCO	Rolling Stock Leasing Company
RSSB	Rail Safety and Standards Board Ltd, UK
SACM	Structured Assurance Case Metamodel (https://www.org/spec/SACM/2.1/PDF)
SEBok	Systems Engineering Body of Knowledge (SEBok, 2024)
SLA	Service Level Agreement
STEP	STandard for the Exchange of Product model data. Standard ASCII based format for the exchange of data such as 3D object

	in CAD as defined in ISO 10303-21 “Clear Text Encoding of the Exchange Structure” (British Standards Institution, 1994)
SysML	Systems Modelling Language (https://omg.org)
TACT	Trustworthiness, Auditability, Credibility, Transferability (Daniel, 2018)
TOC	Train Operating Company
TRIB	Transport Research and Innovation Board
WIPO	World Intellectual Property Office
XaaS	Anything or Everything as a Service

Definitions

Cyber Physical System	“Engineered systems that are built from, and depend upon, the seamless integration of computational and physical components.” (National Science Foundation, 2024)
Digital Entity	Computational entity comprising data and procedural elements. (Based on terminology definition in clause 3.1.5 of BS ISO/IEC 30173:2023 (British Standards Institution, 2023)
Digital (Virtual) Model	Digital representation of a Physical Entity. Comprises several types of model to include the engineering model comprising geometry, materials, components and behaviours; statistics model comprising mathematical analysis to infer relationships between variables; and information model relating a set of facts, concepts and procedures.
Digital Object	Record comprising a set of bit sequences which includes the metadata about the object properties, its content, its relationships with other objects and its behaviour.
Digital Twin	Digital representation of a Physical Entity (Digital Model) with data connections that enable convergence between the physical and digital states at the appropriate synchronisation rate. Capable of providing an integrated view throughout a Physical Entity life-cycle. (Based on terminology definition in clause 3.1.1 of BS ISO/IEC 30173:2023(British Standards Institution, 2023)
Digital Twin System	System comprising inter-operating Physical Entities, Digital Entities, data connections, models (including Digital Models), data, interfaces and services which provides functionality for the Digital Twin. (Based on terminology definition in clause 3.1.21 of BS ISO/IEC 30173:2023 (British Standards Institution, 2023)
End User	Person(s) who directly use the Physical Entity.
Essential Requirements	For railways in Europe these are the requirements defined in EU legislation such as Annex III of ‘Council Directive 2016/797 (2016): Safety, Reliability and Availability, Health, Environmental Protection, Technical Compatibility, Accessibility.
Framework	Supporting structure with components, ideas and principles and the relationships between them justified in relation to its scope and purpose.

FRAND Terms	Voluntary licensing commitment requested from an IP owner by a standards organisation where the IP may become essential to comply with the standard.
Goal Structuring Notation	A structured, graphical notation for assurance cases (Kelly and Weaver, 2004)
National Digital Twin	An ecosystem of connected Digital Twins (The Centre for Digital Built Britain, 2018).
Physical Entity	Asset, system or process with a functional purpose in the physical world that can be the subject of sensing, actuating and controlling. (Based on terminology definition clause 3.1.4 of BS ISO/IEC 30173:2023 (British Standards Institution, 2023)
Risk	An exposure to potential harm or loss.
Structured Assurance Case Metamodel	A standard structured graphical notation for representing assurance cases specified by OMG,2020
Systems Engineering	“A transdisciplinary and integrative approach to enable the successful realization, use and retirement of engineered systems using systems principles and concepts, and scientific, technological and management methods.” (INCOSE, nd)
System-of-Systems	Connected Physical Entities

List of Publications

Clementson, J., Teng, J., Wood, P., Windmill, C. (2021) 'Legal Considerations for Using Digital Twins in Additive Manufacture - A Review of the Literature', *Advances in Transdisciplinary Engineering Series, Volume 15, Advances in Manufacturing Technology XXXiV,* ISBN 978-1-64368-198-6 (print), pp 91-96, Available at: https://:doi.org/10.3233/ATDE210018 Presented to ICMR21 8th September 2021

Clementson, J., Wood, P., Windmill, C., Teng, J. (2021), 'Managing Intellectual Property Issues with Digital Twins', *Proceedings of INCOSE UK Annual Systems Engineering Conference (ASEC) 2021, Leeds, 23rd and 24th November 2021* Presented to ASEC 2021 on 24th November 2021

Statement of Intellectual Ownership

This research and writing within this thesis are all the author's own. The author's design of all interviews and questionnaires carried out as part of the research were reviewed by the Supervisory Team and the approach submitted to the University of Derby College of Science and Engineering Ethics Committee. The previous page lists papers that were published based on this PhD research.

Abstract

Digital technologies that enable Digital Twin Systems are driving demand for more sophisticated system-of-systems decision support services which depend on the collaboration of a complexity of stakeholders, for managing data, developing algorithms and managing the service infrastructure. Such systems are based on the commercial investment of design and know-how by competing design and manufacturing organisations. Traditionally the intellectual property (IP) and trade secrets were contained within design teams in a mix of formats and disparate data sources, but the greater connectivity of data could alter the risk profile from both legitimate and illegitimate causes. Some risks can be anticipated, such as revealing greater understanding of the design and behaviour to a wider stakeholder group, but other risk mechanisms may not be well understood and risk ambiguity could be a barrier to collaboration. There are advantages to manufacturers, in understanding how their systems perform, and for users, to plan maintenance, but to realise these benefits, risks need to be identified, understood and managed despite the early stage of adoption.

This research study was designed and implemented to construct a framework for understanding how IP can influence the risk to multi-stakeholder collaboration using Digital Twins for life-cycle decision support; and to explore how it could be applied to manage risk.

The constructed risk framework contributes an improved understanding of the inter-related factors that underpin the evaluation and mitigation of IP risks to collaborations using Digital Twins. Such issues were not well understood at the start of the research study. The new framework also supports evidencing life-cycle management of risks, linking cause-consequences with mitigating tools as the basis of providing evidence supported assurance.

The research study has originality in the model, data and application. The methodology includes application of a concurrent mixed methods research design dominated by qualitative analysis based on Charmez (Charmez, 2014) constructive grounded theory in a systems engineering context. The framework model uniquely brings together legal and systems engineering viewpoints to support the assessment and mitigation of stakeholder dependency risks. Novel data was sourced and analysed in development of the framework from semi-structured interviews and questionnaires and emerging case studies. The framework was uniquely applied to rail rolling stock cases with application inferred more generally.

Acknowledgements

The support of the supervisory team of Professor Paul Wood, Dr Chris Windmill and latterly Dr Urvashi Gunputh at the University of Derby and Dr Jason Teng at Potter Clarkson in providing critical review, challenging viewpoints and providing encouragement and support through the process is acknowledged and much appreciated. It is also important to acknowledge the broader academic support of the University of Derby, in particular academics within the Colleges of Science and Engineering and Business, Law and Social Sciences for critiquing approaches and progress through annual progress reviews and enabling access to helpful librarians and events and research resources through the Innovation and Research team.

The research was dependent on individuals within industrial and legal organisations who contributed their time to complete questionnaires and participate in interviews and follow up. I am most grateful for their support and look forward to sharing the findings with them. In the early stages of the research, access to industrial organisations was supported and facilitated by institutions and trade organisations and I would particularly like to thank the Rail Forum UK, Railway Industry Association and Institution of Gas Engineers & Managers and their membership for their support in the early stages of the project.

Chapter 1 Introduction

1.1 Research Context & Rationale

The global expansion of digitisation, initially referred to by some as the fourth industrial revolution (Industry 4.0) (World Economic Forum, 2019) provides potential for Digital Twins to revolutionise business operations and enhance industry productivity by providing timely information about Physical Entities to improve decision making. Changes inevitably reveal barriers and challenges: technological, organisational and regulatory. For many regulated industries, such as Rail and Energy, dependent on systems which remain operational for decades, the change transition inevitably involves assets and processes from a pre- or partial digital age.

The University of Derby carries out manufacturing research and was anecdotally encountering concerns from this transition. In one example uncertainty around the legal implications of digitising physical assets and paper-based records and managing, using and adapting the digitised records was encountered. The initial concern related to uncertainties about the Intellectual Property (IP) risks of using the CAD file in both 2D CAD file and 3D form, with STEP format as a form most universally circulated for various purposes such as 3D Printing. In this case, the files were intended to be used for developing manufacturing quality assessment services to support manufacturing process decisions.

Separately it became clear that industries related to the built environment were at the heart of the UK government driven National Digital Twin (NDT) initiative in the UK with guiding principles, The Gemini Principles (The Centre for Digital Built Britain, 2018) and a roadmap (Enzer *et al.,* 2019) for connecting Digital Twins relating to transport (rail, aviation, road), energy, water, waste and telecoms for supporting decision making for societal benefit. This potential and growing demand to use a System-of-Systems of Digital Twin Systems to underpin decision support was also more widely evident in literature discussing the use cases for applications in enterprises particularly for operational life-cycle management and decision support in smart manufacturing (Moyne *et al.*, 2020) and industries such as health, energy and transportation (Rasheed *et al.,* 2020).

Digital Twins can have links between digital and Physical Entities for life, as discussed in Chapter 2, suggesting collaboration between stakeholders would need to be maintained and managed over the long term and this may lead to different business models and particular

technical solutions to manage risk, especially for the complex System-of-Systems cases. However, the NDT roadmap (Enzer *et al.,* 2019) and initial literature review of Digital Twin use cases revealed a low level of implementation maturity with Digital Twins and absence of guidance at sector and implementation level for understanding and managing risks to ongoing collaboration. The literature also included specific comment on legal uncertainties including ambiguities about protections of models in digital form as had been identified as part of the 3D printing activities (Mendis *et al.,* 2020, Daly, 2016, Murray, 2016). From this context an initial hypothesis and working assumption was explored in an initial research activity (section 1.2) to provide the basis for the research project.

1.2 Research Problem

The initial hypothesis, called 'H1' is:

Intellectual Property Risks potentially impact multi-stakeholder collaboration using Digital Twin Systems for decision support.

If true the working assumption was that there would be a need for understanding and managing the risks to establishing and maintaining multi-stakeholder collaboration using Digital Twins for decision support through life-cycle stages, from design, manufacture, through operation and maintenance to disposal, from an IP viewpoint.

As a perception of risk can impact stakeholder behaviour in collaborations (Grudinschi *et al*, 2014), opinions expressed in academic literature about IP risk to achieving outcomes using Digital Twins and Cyber-Physical Systems was considered evidence of potential impact to collaboration. A structured literature review of business, technical and legal literature (section 2.2) was carried out to test the hypothesis. This concluded that the hypothesis was true, enabling the prior work to be explored and the research project to be planned.

1.3 Summary of Prior Work

An initial scoping literature review during 2020 considered prior work relating to risks and issues with the adoption of technologies associated with Industry 4.0 such as IIoT, Digital Twins, Additive Manufacture, Cyber-Physical Systems, cloud technology and Smart Sensors for the purpose of decision support together with the associated legal risks. In addition, the review considered prior work related to the management and assurance of such systems and prior work related to multi-stakeholder collaboration risk. The review is discussed in section

2.3 and identifies potential IP concerns and ambiguities relating to Digital Twins and more generally, digital engineering, which could impact collaboration, further supporting the initial hypothesis. However, the risks and issues in prior work literature are explored from the independent viewpoint of a lawyer, computer scientist, systems engineer or business academic and the issues are not well integrated nor understood in relation to Digital Twins used for decision support. There are therefore gaps both in better understanding the characteristics and mitigation of risks through a Physical Entity life-cycle and linking the viewpoints to explore and better understand the interaction of legal, technical and assurance processes in relation to risk, with a view to contributing to the development of guidance for collaborating stakeholders.

Even other scoping studies, for example, Sinclair *et al*'s (2019) extensive review of completed cyber-physical research programmes to identify knowledge gaps found a gap in identifying standards and agreements to deal with legal issues for security, privacy and liability, and while Wang *et al*'s, (2020) patent scoping study identified IP as a growing key component of Digital Twin solutions, the potential risks to business collaboration were not explored. Even later scoping studies of Digital Twin research, emerging several years later, found that despite the increases in Digital Twin research, the research fields were "scattered" and "limited" (Wang *et al.*, 2024).

1.4 Research Questions & Aims

The initial literature review conclusion that IP Risks could impact multi-stakeholder collaboration using Digital Twins together with the prior work review, which revealed gaps in understanding these risks and how to mitigate them, resulted in the assertion of the central questions to be answered by this research study. These are:

Research Question 1 - What factors are important for describing how IP can influence multi-stakeholder collaboration risk using Digital Twin Systems for decision support?

Research Question 2 - How do these factors relate to describe overall risk and provide the basis for collaborating stakeholders to manage and assure that risks are mitigated?

Answering these research questions will enable the research project to achieve the following aims:

Aim 1 – To explore and describe a framework for understanding how IP can influence multi-stakeholder collaboration risk using Digital Twin Systems for decision support through the Physical Entity life-cycle.

and to:

Aim 2 – To explore how this framework could be applied to assure that life-cycle IP Risks to Digital Twin Collaborations are effectively managed.

1.5 Research Objectives

The aims are achieved by carrying out the following objectives:

- RO1 - Define the collaboration risk context to scope the research project. In particular:
  - define and characterise the Digital Twin decision support purpose and use cases requiring multi-stakeholder collaborations through a Physical Entity's life-cycle. (see Chapter 2.4.2)
  - clarify the types of IP risk associated with the identified Digital Twin use cases. (see Chapter 2.4.3)
  - identify existing frameworks, standards and industry practices for mitigating and managing risk to the decision support purposes in example sectors. (see Chapter 2.4.4)
- RO2 - Define, justify and implement a research methodology appropriate to the early stage of adoption of Digital Twin applications, which answers the Research Questions and Aims within the defined context. (see Chapters 3 to 6)
- RO3 - Evaluate the constructed framework (see Chapter 7):
  - against the claim that it answers Research Question 1.
  - against the claim that it answers Research Question 2.
  - against the claim that it achieves Aim 1 and Aim 2.

1.6 Research Scope

The elicitation of factors from literature covered a broad range of industry sectors, however the research design included semi-structured interviews and questionnaires from the rail sector and gas pipeline as example sectors and most contributions were from the rail sector. As such, perceptions of risk, in so far as they contribute to understanding of risk factors, are

dominated by a rail sector perspective and although many contributors worked for international organisations or had career experience working with other sectors, they were based in the UK and are considered to have a UK and EU perspective in particular. The evaluation participants, from industry, were working within the rail sector at the time of the evaluation.

Although the elicitation of factors from literature covered a broad range of decision support purposes, the case studies considered in the evaluation stage were for rail rolling stock maintenance decision support purpose within UK and EU contexts. Rail rolling stock are complex systems with distinct, evidenced procurement, operation and maintenance and mid-life upgrade life stages. There are only a few original equipment manufacturers supplying across the EU, using a shared supply chain. This allowed a focus on comparison of countries of application, operation and ownership.

The World Intellectual Property Office (WIPO) provides an overall international frame for IP but there are specific national rules, implementations and interpretations and given the case study focus on EU and UK such perspectives were the main focus. However where a particular literature source broader than this scope provided a perspective related to collaboration risk using complex systems, such as the SF Express v Cainiao (discussed by Wang, 2019) data dispute, this was reflected in the study. Legal practitioners and academics contributing to the evaluation were based in the UK but had international experience.

For the purposes of the study IP is considered to include trade secrets (Gorbatyuk, 2016).

The development of the framework for understanding IP risk to collaboration considered the characteristics and scope of existing risk management frameworks starting with ISO 31000:2018 (British Standards Institution, 2018) and related legal part BS ISO 31022:2020 (British Standards Institution, 2020). The study considered the characteristics of assurance frameworks and methodologies, which are applicable to achievement of a lifecycle Physical Entity decision support Purpose and the specific case study focus of assurance of outcomes related to rolling stock maintenance. As assurance frameworks tend to focus on specific emergent properties such as safety, security and sustainability, the consideration of characteristics of asset management frameworks such as BS ISO 55001 (British Standards Institution, 2024c) and security risk framework BS ISO 27001 (British Standards Institution, 2023a) were also considered in scope.

1.7 Research Design Summary

As Digital Twins and their applications are complex socio-technical systems, a staged Systems Engineering approach to the research was adopted as discussed in Chapter 3. Three iterative stages were considered, Stage 1: Problem identification and definition, which framed the research aims and objectives, initial hypothesis and developed the initial research activities; Stage 2: Analysis and Design, which implemented the data collection and analysis and led to an outline framework and related hypotheses, and finally Stage 3: Evaluation, which tested the framework against claimed hypotheses.

Stage 2 adopted a mixed methods approach dominated by qualitative analysis as the core component to explore and describe the framework. A constructive Grounded Theory methodology (Charmez, 2014) was selected for eliciting factors from qualitative sources and revealing theory underpinning their relationships to inform the framework. The approach overall was abductive with data collated and analysed simultaneously. The data was collected in a process of theoretical sampling, updating and recoding the initial list of factors until no new relatable factors are identified and the relationships between them are clarified. Data was derived from literature (qualitative), semi-structured interviews (qualitative) and questionnaires (qualitative and quantitative) to provide a diversity of sources and to mitigate bias from any single data collection method until theoretical saturation was reached.

In the final evaluation stage (Stage 3) the hypotheses relating to the framework were tested through a combination of expert and stakeholder reviews and application of the framework to publicly available cases. A Trustworthiness, Auditability, Credibility, Transferability (TACT) framework (Daniel, 2018) was used to guide the evaluation stage design.

1.8 Research Outcomes

The research study achieved the intended aims and objectives, as discussed in Chapter 8, and provides a constructed framework that contributes improved understanding of collaboration risks and mitigations in digital twin based decision support systems. The framework was evaluated by industry representatives and legal practitioners against the original aims and potential application of the framework was explored through three rail sector cases using information available in the public domain. Future research projects include applying the framework to live projects in real-time and extending evaluation to other sectors as well as developing and testing some of the mitigation tools.

1.9 Significance of the Research

The research study has contributed both practical and theoretical significance as follows:

- Practical Significance – The constructed IP risk framework supports industrial stakeholders considering decision support solutions using complex digital systems such as Digital Twins to evaluate collaboration risks, evaluate implementation options and document assurance that risks relating to IP are mitigated and managed. It enables legal specialists to support clients with mitigation solutions traced to their purpose and system solution. It also provides understanding for policy makers in sectors seeking to incentivise and support stakeholders undertake complex digital solutions. This could be of particular value where the decision support purpose relates to a broader social good such as health, mobility or environmental protection.
- Theoretical Significance – The research project contributes understanding of the relationship between legal, technical and business influences in managing IP risks to collaboration for decision support using complex systems such as Digital Twin Systems. It more generally contributes understanding of the inter-relationship of legal, technical and business risk for complex systems.

1.10 Research Novelty

The research study has the following novelty:

- Constructed Framework – Uniquely brings together a legal viewpoint (IP) with systems viewpoint to support the assessment and mitigation of stakeholder dependency risks.
- Data – Novel data sources are analysed in development of the framework from semi-structured interviews and questionnaires and emerging case studies.
- Application – The development of the framework was uniquely developed for the needs of collaborating stakeholders and specifically and uniquely applied to rail rolling stock cases with application inferred to other industries especially linear infrastructure sectors such as rail infrastructure assets and gas pipeline.

1.11 Structure of the Thesis

Chapter 1: Introduction	Provides an introduction to the research study, including rationale, summary of the prior work that underpins the research question, aims and objectives and a summary of the scope, research design approach and outcomes. The section concludes with comment on the significance and novelty of the research and provides a structure of the following thesis chapters.
Chapter 2: Literature Review	Describes the role of and approach to literature review through each stage of the research study. This is followed by discussion of the: • structured literature review to test the initial hypothesis. • scoping review of prior work to inform the research question, aims and objectives. • literature review to explore and define the context of the research study contributing to Research Objective 1.
Chapter 3: Research Methodology	Identifies the approach to developing the research methodology followed by specific discussion of the research design considerations; philosophical position; theoretical perspective; chosen research methodology; quality, rigour, ethics and reflexivity in the research process.
Chapter 4: Research Methods	Discusses the data collection methods, sampling strategies and approaches to data analysis, integration, and evaluation.

Chapter 5: Construction of the Risk Framework	Discusses the implementation of the research methods to answer the research questions and achieve the aim of an IP Risk Framework.
Chapter 6: Described Risk Framework	Describes the risk framework including the relationship between categories and factors relevant to answering the research questions and the relationship to existing risk management standards to highlight the new understanding. Also discusses potential applications of the risk framework to achieve Aim 2
Chapter 7: Evaluation of the Risk Framework	Discusses the evaluation of the risk framework against achievement of the research questions and aims by experts and through application of cases.
Chapter 8: Conclusions and Recommendations	Provides a review of the original aims and objectives and summarises the research study conclusions. Additionally summarises the contributions to academic knowledge and professional practice and study limitations before concluding with recommendations for further research and a summary of dissemination activity.

Chapter 2 Literature Review

2.1 Introduction

Each of the three stages of the systems research design outlined in section 1.7 implemented literature reviews. However, the purpose and approach to literature review within each stage was specific to the research design and objectives for that stage. In Stage 1 there were sequential steps of literature review with some iteration between steps to define and confirm the problem and goal (section 2.2). The second step was to identify and assess prior work related to the problem and goal (section 2.3) and the scope and context of the problem (section 2.4) before confirming the research questions and aims to inform the development of the research plan for Stages 2 and 3 (section 2.5).

The original literature searches were repeated periodically during the research study to check for emerging work of relevance. Section 2.6 discusses those studies identified as most relevant and how they related to the current study.

The steps of the literature review in Stage 1 are summarised in Figure 1 below and forms the focus for this chapter.

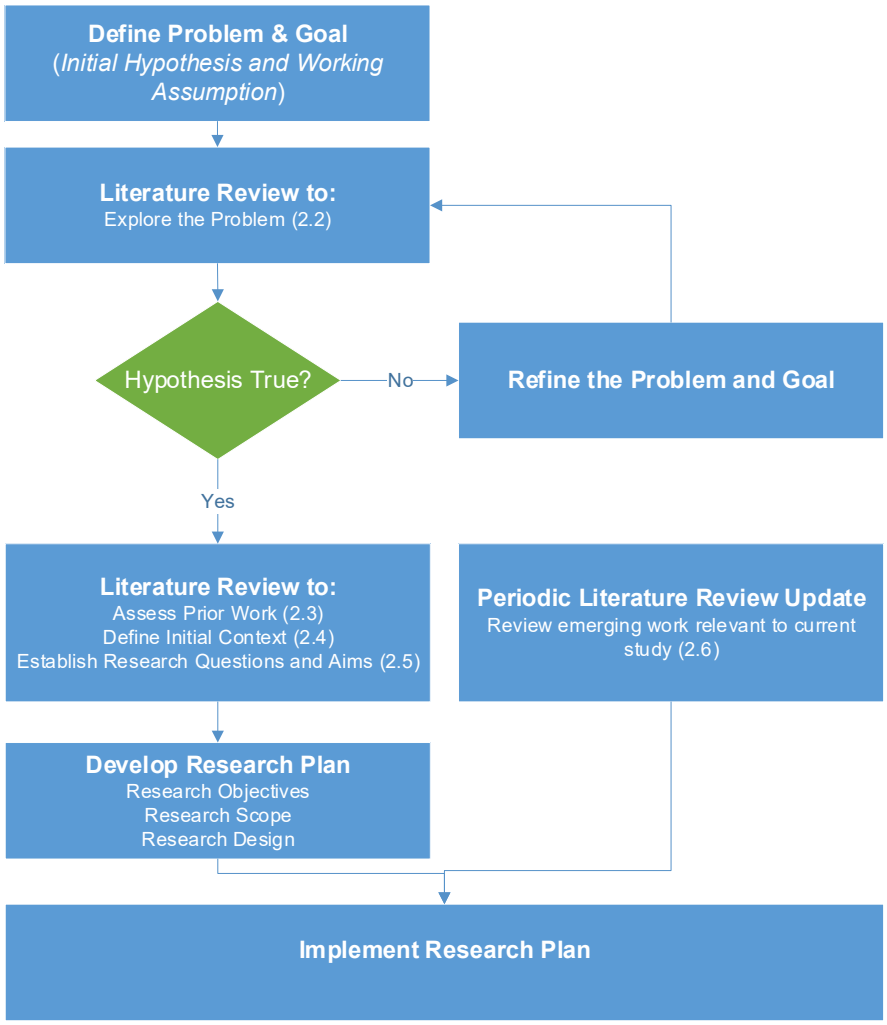


Figure 1 - Literature Review in Stage 1- Problem Definition

2.2 Problem & Goal

The problem is expressed as an initial hypothesis, H1:

IP Risks potentially impact multi-stakeholder collaboration using Digital Twin Systems for decision support.

If true, the goal, is expressed as working assumption, WA1:

Stakeholders require guidance to manage IP risks to collaboration using Digital Twins.

The purpose of the literature review was to find international evidence supporting or disproving this initial hypothesis and working assumption. If true, this would provide the basis for further research. If false, the greater understanding from the initial research would allow a new or updated hypothesis to be stated and tested.

According to Munn *et al*, 2018 a systematic review approach is appropriate for this purpose. As such the review criteria were selected to focus narrowly on the specifics of the hypothesis.

A systematic literature review approach, based on Kitchenham and Brereton, 2013, was carried out to explore this question from a range of academic databases covering legal, business and technical perspectives, using the following criteria:

Eligibility Criteria	Article Title, Abstract, Keywords Include: ("Intellectual Property" AND "Digital Twin" AND "Risk") Article Title, Abstract, Keywords Include: ("Legal" AND "Digital Twin" AND "Risk") Article Title, Abstract, Keywords Include: ("Intellectual Property" AND "Cyber-Physical System" AND "Risk")
Databases	HeinOnline, Emerald, IEEE Xplore, Scopus
Resource Type	Journal Paper or Conference Paper
Screening Approach	First Step: Title and Abstract (manual screening with automated citation search for HeinOnline, which searches all text). Second Step: Full Text Review of candidate papers for relevance to the hypothesis and screening against inclusion and exclusion criteria. Identify papers that infer that the hypothesis is true or false and identify examples of supporting statements. Third Step: Review references of all selected papers to identify any additional papers of relevance and review against the hypothesis.
Inclusion and Exclusion Criteria	Language: English Conference or Journal Paper Full Paper: Available to download

	Excludes a collection of papers, notes or legislative code or commentary on such collections. Timescale: 1985-2020. (Supporting the research stage)

Table 1: Search Criteria for Literature Review Related to H1

The results are presented in Table 2.

Database	**Search Criteria**	**Search Results (1985-2020)**
Scopus	Title or Abstract: ("Intellectual Property" AND "Digital Twin" AND "Risk"); ("Legal" AND "Risk" AND "Digital Twin"); ("Intellectual Property" AND "Cyber-Physical System" AND "Risk")	8
IEEE Xplore		1 (duplicate Axelrod, 2013)
Emerald		0
	Unique papers IEEE Xplore plus SCOPUS plus Emerald	**8**
HeinOnline	Full Text: ("Intellectual Property" AND "Digital Twin" AND "Risk"); ("Legal" AND "Risk" AND "Digital Twin")	22
	Unique papers IEEE Xplore plus SCOPUS plus Emerald plus HeinOnline	30
	Unique papers after screening rules applied	**24**
	Papers that provided comment on the hypothesis	**12**

Table 2: Search Results for Literature Review Related to H1

There were 17 papers in HeinOnline from a full text search of ("Intellectual Property" AND "Cyber-Physical System" AND "Risk"), however initial inspection of available papers suggested they were not closely aligned with the hypothesis, with the few most relevant articles discussing broader issues such as ethical considerations of cyber-physical systems and liability issues and adding to issues already identified such as ownership of IP that involved AI in its generation (Ghosh, 2020).

The analysis of relevant literature against the hypothesis is summarised in Table 3. Articles were considered to infer that the hypothesis was true if they mentioned or discussed risks and their potential causes or consequences that could reasonably be expected to impact multi-

stakeholder collaboration. This included criminal activity such as theft as well as breach of contract and disputes and withholding access to information or services. At this stage it was not necessary for the article to explicitly express that such a risk could impact multi-stakeholder collaboration provided the risk or concern was expressed. A false result was inferred either through explicit statement that Intellectual Property is not an issue with Digital Twins or cyber-physical systems or discussion that inferred this. There weren't any such discussions identified.

Test of Hypothesis	**Count**	**References and example Risks Identified**
True	12	**Intellectual Property Theft**: Dong *et al.* (2020); Settanni *et al.* (2017); Axelrod (2013); Palachuk (2020) mention IP theft risk from decentralised servers and Cyber-Physical Systems and issues of ownership and obligations related to data. Axelrod (2013) discussed the direct and indirect loss that can occur from a breach such as costs from compensation and adverse impact on reputation. **Intellectual Property Ownership, Access, Use and License Dispute**: Cole (2018); O'Leary and Armfield (2020); Mauritz (2020) discusses database rights and legal personhood relating to Digital Twin AI; Druetta (2018) discusses clarity risk relating to data rights during predictive analytics applications; Guttieres *et al,* 2019 discuss vulnerabilities from dependence on proprietary Intellectual Property.) **Mention of collaboration challenges with IP**: Stein (2020 **Broad legal risks of Artificial Intelligence in Digital Twins and potential identification of individuals**: Kartskhiya A.& Makarenko (2019), Culnane (2019).
False	0	No paper identified
Not Applicable	12	

Table 3: Summary of Hypothesis Testing of H1

Of the twelve articles that were considered to support the hypothesis, the majority expressed concern about potential intellectual property theft and ambiguities and potential misunderstandings relating to ownership and licence obligations. Although most articles only commented on the potential risks some articles cited actual crimes in support, for example Guttieres *et al.* (2019) cites several targeted cyber-security hacks in the biotechnology sector. The vulnerabilities of hardware, through malicious third party designers and providers of AI chips was highlighted by Dong *et al.* (2020) with the potential to cause information leakage in cyber-physical systems. Further system risks with third party decentralised servers were highlighted by Palachuk (2020), who, in relation to the construction sector cautioned for the need for clear contract terms and risk review of companies with access to the networks. Legal practitioners O'Leary and Armfield (2020) used an example of AI in an autonomous vehicle to highlight the risk of not communicating related IP and ownership rights through contract, to include data gathered by the AI programme in operation.

Given the concern expressed relating to IP and risks to Digital Twin Systems, services and associated technologies the hypothesis was considered true. This then enabled a literature review of prior work to understand the risks and mitigations and frameworks for managing them. Further literature supporting the hypothesis was revealed during the review of prior work such as Sinclair *et al.* (2018) and Madni *et al.* (2019).

2.3 Prior Work

2.3.1 Approach to Identifying Prior Work

According to Munn *et al.* (2018) a scoping review approach is appropriate for identifying gaps in knowledge, scoping a body of literature and clarifying concepts. As such this approach was adopted to identify prior work to understand how intellectual property concerns can impact collaboration to achieve a Digital Twin purpose and identify what work has been done to mitigate such risks. Searches were established to answer the following questions:

Question 1	What are the prior studies of legal issues with adoption of digital technologies for decision support? Which of these studies specifically relates to intellectual property issues? Which of these studies specifically relates to Digital Twin?
Question 2	What are the prior studies to understand risks to multi-stakeholder collaboration of complex systems? Which of these studies specifically

	relates to intellectual property issues? Which of these studies specifically relates to Digital Twin?
Question 3	What are the prior studies to develop Risk Management and Systems Assurance related to complex systems and Digital Twins? Which of these studies specifically relates to intellectual property issues?

For each question the prior work relating to each of legal, technical and business perspectives was sought initially through a search of title, abstract and keywords using broad search terms relevant to the question. The abstracts were read through for relevance to the question and full papers were then downloaded for more thorough review. The full paper review also sought out the subset of information relating to the specifics of IP and Digital Twin. Example search criteria and results of screening papers for relevance are captured in Appendix 1. The search for relevant papers was repeated periodically throughout the period of research study to ensure any emerging, relevant studies were identified and reviewed in relation to the current study. Emerging work is discussed in section 2.6.

2.3.2 Prior Studies of Legal Issues with the Adoption of Digital Technologies

The literature related to Question 1 revealed that IP issues were a key component of Digital Twin solutions (Wang *et al.,* 2020).

Prior to the current research study there were very few peer reviewed studies focussed specifically on legal issues with the adoption of digital technologies for decision support with significant studies emerging during the current study as discussed in section 2.6. By the end of 2020 several studies reported in journals and conference papers were concerned with ambiguities and uncertainties of increased connectivity and digitisation in supply chains and services and especially given the high rate of change of digital transformation and the early stages of adoption of technologies such as Digital Twin and IIoT. As such many studies broadly discussed and commented on the potential challenges or anticipated potential risks and issues. For example, Liu *et al.* 2019 analysed the 'cyber-physical-social thinking context' of smart systems and identified legal issues as one of several areas of focus. Cinque *et al*, 2018 focussed on issues with cloud computing specifically and commented on exposure to potential reputation and financial impact through an inability to meet Service Level Agreements (SLAs) if there were reliability issues with the cloud services. Risks identified included data ownership and retention issues and transfer of sensitive data. Risk relating to

the cloud specifically was further considered by Alkhabbas *et al.* 2020 exploring factors for optimal deployment models for IoT systems. They used a survey of IoT architects to identify the factors that influenced deployment. This identified a reliance on Cloud rather that Edge for software deployment and reliability, performance, security and cost influencing deployment decisions.

Ambiguities and uncertainties including related regulatory issues were also explored from the perspective of application in specific sectors. For example, legal academic Shaydullina (2018) carried out a critical analysis of the integration of technology in financial services (FINTECH) to identify best practice as the basis for proposing a system of institutional and legal methods for further development of the sector. Legal academics Anugerah and Indriani, 2018 further commented on the requirements for a legal framework in FINTECH also highlighting the increased data protection risks due to the rise of communication technologies and system connectivity. The uncertainties were studied in the context of mental health practice by socio-legal academic, Piers Gooding. Gooding (2019) mapped the technologies, including communication and information sharing technologies, in the mental health context, to identify cross-cutting legal, ethical and social issues.

Several academic authors commented on the proliferation of 3D printing and digital manufacturing and were also concerned about the increased connectivity and ease of moving digital records quickly across national borders. There was research and comment on the implications for IP law in relation to Additive Manufacturing and the digitisation of the physical component design, in the form of text books such as Daly (2016) and Murray (2016) and a research paper by Mendis *et al.* (2020) related the impact of EU IP legislation on Additive Manufacturing for industrial applications, interpreting how current laws applied to digital files and anticipating potential risks which may subsequently drive changes to the law.

Several specific legal issues were explored by academics by relating application cases to the digital systems. Such issues were discussed from a legal perspective with examples as follows:

Data protection and GDPR issues - Stefanouli and Economou (2019) analysed the relationship between smart cities and data protection from the perspective of new EU GDPR legislation.

Obligations and liabilities including AI - Madni *et al.* (2019) explored product and system safety, including from risk of accidental or malicious tampering with digital records and instructions and reliability of the data and information derived from the data, which leads to issues of liability for automated decisions that have unintended consequences. Although there were mentions of potential mitigations of these risks needing to come from a combination of legal protections, standards and system architecture the main academic focus of these research studies was technology and architecture research including technical security solutions such as blockchain, applied to an additive manufacturing case study (Mandolla *et al.,* 2019) and to a furniture manufacturing supply chain case study (Jaeger *et al.*, 2019). Liability issues associated with Artificial Intelligence (AI) decision making were analysed by legal academics Kartskhiya and Makarenko (2019) and Mauritz (2020) in relation to a broad range of digital technologies to include Digital Twins. They identified the need for a legal framework for use and application of artificial intelligence technologies, including standards. IP and commercial risk to data owners from 3rd party AI training service providers was explored by O'Leary and Armfield (2020) and Druetta (2018).

Protection of trade secrets - Soares and Kauffmann (2018) commented on the risks and opportunities with implementation of the new technologies of Industry 4.0 on the protection of trade secrets and concluded that Intellectual Property Law and contract law solutions needed to be underpinned by the business strategy and business model but did not go further.

Proprietary and open data and sharing - Legal research studies considered the implications of data ownership and sharing and the degree to which current laws support proprietary data protection and sharing centred on the EU Database Directive ('Council Directive 96/9/EC', (1996)) and copyright laws. Database protection in relation to Open Data Licences was discussed by De Filippi and Maurel (2015) and concluded that the complexity of the relationship may paradoxically act to discourage data sharing and re-use.

The body of prior work on IP relating to data and issues of ownership and agreed terms of use, could be considered a potential risk with Digital Twins for decision support although the discussions applied more generally and not specifically to Digital Twins.

Further technical academic articles which did not mention legal, law or Intellectual Property in the title, abstract and keywords were identified during the research study. In particular, Rasheed *et al.* (2020) reviewed methodologies and techniques for modelling and constructing

Digital Twins to identify current challenges and enabling technologies. As part of their mapping of common challenges and enabling technologies they identified data management, data privacy and data security as a challenge mapped to the enabling technologies of digital platforms, cryptography, blockchain and big data technologies. There was an anecdotal mention of IP as an issue within the main body of the report in so far as it could restrict access to specific mathematical models necessary to support the decision support purpose.

Systems engineering academics, Sinclair *et al.* (2018) produced a knowledge map from seventy two deliverables of the EU Horizon programmes relating to cyber-physical systems to identify knowledge gaps. Within the detail of the discussion they identified that progress with cyber-physical systems was hindered by data sharing, access rights, IP rights and regulations which they suggested were best addressed by the EU. They also mentioned that there are technical challenges related to IP rights without discussing further. Systems academics Madni *et al*, 2019, in review of Digital Twin applicability to Model Based Systems Engineering (MBSE), also expressed anecdotal concerns about IP in their concluding section, questioning whether operators would want to report operational data to a manufacturer and that extensive data sharing between manufacturers and potential customers could be disconcerting for them.

Legal practitioners, Bird & Bird LLP examined the legal issues relating to access to and re-use of big data in the transport sector as part of the Horizon 2020 funded LeMo project (Debussche, *et al.*, 2018). They identified several issues to include IP, open data, sharing agreements and obligations and data ownership as well as liability, competition, data protection and security issues and discussed challenges and opportunities. They concluded that the current legal framework does not encourage use of big data in the transport sector and that needed improvements ranged from avoiding restrictive court interpretations, and need for guidelines and codes of conduct to EU regulatory interventions. However they did not provide any specific suggestions for improvements in IP management at the time of the study only suggesting that protection may incentivise stakeholders to engage in data sharing. More specifically on data sharing they suggested that this could be stimulated through data sharing obligations in public tenders and recognised a need for legislative intervention to support data sharing agreements.

The National Digital Twin (NDT) project, launched by the UK government in 2018 and delivered in partnership with the Centre for Digital Built Britain (cdbb), sought to enable the

interoperability of a system of connected Digital Twins in the built environment. Such a system of Digital Twins would require multiple stakeholders to collaborate and so would need to consider potential challenges and barriers. Although the cdbb published a road map for implementation of the National Digital Twin (Enzer *et al.,* 2019), which included a legal and regulatory thread, there was no specific guidance at the Digital Twin user or implementer level prior to the research study. The National Digital Twin team had however developed principles called the Gemini Principles (The Centre for Digital Built Britain, 2018) to guide the National Digital Twin and its enabling information management framework to provide a focus for Digital Twin projects on the public good. There were three stated underpinning principles relating to Purpose, Trust and Function. Such principles would be expected to underpin stakeholder collaborations in achieving outcomes, which could be considered to include outcomes relating to operational decision support, which in turn comply with the principle of Purpose. The work acknowledged that the principles would continue to evolve over time.

In summary, the prior work on legal issues associated with digital technologies for decision support was not extensive, and although included IP risk to Digital Twin was generally at the early stages of identification, mapping and discussion of potential legal issues. Legal discussions were discussed from the viewpoint of legal academics with some limited technical discussions exploring application of blockchain to mitigate IP risks. Many of the issues were discussed in relation to specific regulated sectors such as medical, financial services and manufacture. There was further academic comment on data ownership and supplier obligations through specific application of Digital Twin and use of BIM in the built environment.

2.3.3 Prior Studies to understand risks to multi-stakeholder collaboration of complex systems

There is significant prior research relating to risks to stakeholder collaboration across fields from disaster management through to urban planning. The initial search criteria for Question 2 was focussed to identify titles, abstract and key words relating to multi-stakeholder or multi-partner collaboration with complex systems with the abstracts reviewed for relevance to decision support and collaboration risk. The initial research criteria identified prior work where multi-stakeholder collaboration was presented as part of complex system decision making solutions to managing societal risk rather than from the perspective of risk to maintaining the multi-stakeholder dependent systems once they were established. However

such papers, although context and system specific, provided insight into the inter-relationships that could infer sources of risk to collaboration.

Such problem-solution focussed papers included, Binot *et al.* (2015) who proposed a conceptual framework for multi-stakeholder collaboration to managing cross sector health and well being in South East Asia. They aimed to promote systems thinking and involve social science in implementation of the framework. The study concluded that the approach could reveal tensions between stakeholders. D'Agostino *et al.* (2020) investigated challenges of agricultural water management in Malta and used qualitative research approaches such as interviews and questionnaires to improve understanding of the collaboration barriers highlighting context specific issues such as water governance and policy gaps impacting decisions and need to promote shared opportunities for water infrastructure investment through multi-stakeholder collaboration. Djalante *et al.* (2013) developed a conceptual framework to improve integration of disaster reduction and climate change adaptation strategies, dependent on multi-stakeholder collaboration. Their application to a case study in Indonesia concluded a need to strengthen local multi-stakeholder collaborations. The framework included seven pathways covering integrated strategies, polycentric governance, sectoral integration, information management, learning, self-organisation, and finances and risk.

Building Information Modelling (BIM) is intended to facilitate multi-stakeholder collaboration in construction projects including decisions relating to change management and implementation options and uses some similar technologies to those used in Digital Twin, such as graphical, technical and commercial data relating to artefacts and use of communication technologies. As such the search terms of "risk", "stakeholder", "collaboration" and "BIM" were used to identify prior work related to Question 2.

Almarri *et al.* (2019) explored emerging contractual and legal risks from using BIM, due to the reliance on information technology. They identified risks from literature and carried out a questionnaire survey to understand the importance of these risks to stakeholders involved in BIM projects. Their findings confirmed that emerging risks were likely to be related to BIM documentation, IPR and liability, missing data and stakeholder assumptions. A later study by Almarri *et al.* (2020), explored the perceptions of users of BIM to potential management risks and identified nine most likely risks that may emerge which could be inferred to potentially impact collaboration. Such risks included lack of experience and skills, conflict due to

dissimilar expectations and maturity of processes and standards. Jo *et al.* (2018) compared BIM contract terms from two common standard forms used in Malaysian construction contracts and concluded that ownership of the BIM model and IPR were among potential legal issues that could arise and that there was a lack of a framework effectively addressing legal and contractual issues.

Previously, Hsu *et al.* (2015) had identified several legal issues from the application of BIM in Taiwan which included IPR issues, particularly potential disputes over copyright ownership when models modified by various stakeholders during a project are then used in future projects or required for operational and maintenance purposes relating to the original project. They identified that continuing to use BIM after the transfer of ownership, or right to appropriate, is a challenge for BIM applications and discussed potential mitigations through interpretations and application of Copyright Law.

Fan *et al.* (2018) carried out a systematic literature review of fifty-five journal articles and conference papers published between 2007 and 2017 to identify legal issues associated with BIM. They then related these issues to mitigations adopted by the construction industry. The issues included 'Model Ownership and IPRs, 'Infringement of another's IPRs', 'Protection of Business Knowledge', 'Protection for a creation that requires hard work' and 'Security Access and Control.' They identified that most issues were sought to be mitigated through use of contracts, although identified risks and issues with current clauses and lack of clarity for specific issues such as where a model contributor proposes to repurpose a model and data. A need for the technical mitigation of coding data was proposed for 'Protection for a creation that requires hard work".

The application of contracts to align stakeholder objectives, risk and reward in large contracts was explored by several academics. A more recent study by Galvin *et al.* (2021) explored Alliance Contracts and found they were not sufficient on their own for controlling opportunism risk. They used a single case study approach to explore the interlink between governance, trust and culture and how attention to these aspects impacts collaborative rather than opportunistic behaviour. They didn't, however, specifically explore any potential risk of opportunism in relation to IP.

Ahmed *et al.* (2020) focussed on the risk to collaboration from use of cloud computing in construction projects, particularly the risk of project failure related to the ability of the cloud

provider to support multiple collaborating stakeholders and the dependence on ongoing trust between stakeholders and the cloud providers. They proposed a trust based Cooperation Value Estimation (CoVE) approach intended to enable and sustain collaboration among disciplines in construction projects with a focus on data privacy, security and performance. They demonstrated the approach through a highway bridge construction case study and suggest the approach can be applied to other domains.

Overall, the main focus was during the design and construction and handover phase of a project with gaps in understanding implications during the operational life of the physical system. Most of the studies were qualitative and context specific, either relating to construction through application of BIM or applied to a specific social challenge that requires multi-stakeholder collaboration such as climate change or healthcare.

2.3.4 Prior Studies to Develop Risk Management and Systems Assurance Frameworks

Literature relating to Question 3 included studies developing and proposing systems assurance frameworks for complex systems documented in the later twentieth and early twenty-first century and tended to focus on specific emergent behaviours, typically each or a combination of safety, security or sustainability which as Hessami and Karcanias (2009), points out are the properties generally subject to a regulatory framework in most societies with other properties such as cost, reliability and quality left for stakeholders to define for particular purposes. Hessami and Karcanias (2009) proposed an assurance framework that considered safety, security and sustainability together in a Surety framework, recognising the pace of change and inherent uncertainties in cyber-physical systems.

Legislation and standards underpin the processes, governance and presentation of assurance that risks are identified and mitigated. Assurance Cases tend to focus on system Safety and Security and for complex systems tools such as the graphical notations, Goal Structuring Notation (GSN) (Kelly and Weaver, 2004) and Structured Assurance Case Metamodel (SACM) (OMG, 2020 and Wei *et al.*, 2019) are used to support linking the arguments to demonstrate the case and compliance with relevant risk management standards. Such approaches were evident in transport, oil and nuclear sector safety cases (Bishop and Bloomfield, 1998) but not applied to Digital Twins nor considering risks from an IP perspective. More recent work relates to automation of assurance and the development of ontologies to facilitate structure and automation.

Some industry practitioners and academics have explored application of Systems Engineering methodologies such as Model Based Systems Engineering (MBSE) to the development of Digital Twins and complex data driven systems to provide clarity of data threads and value chains and development of graphical assurance notations. In an early conference paper (Hart, 2015) identified the benefits of MBSE in providing traceability through a system lifecycle and (Madni *et al.*, 2019) proposed integrating Digital Twins with MBSE through the digital thread to facilitate a range of lifecycle development and performance assurance activities although cautioned about the perceived, and not well understood, legal and IP risks from sharing data with suppliers and customers. Bickford *et al.* (2020) went further to propose an approach to applying MBSE to scope and develop Digital Twins and integrate Digital Twin and physical system development and although cautioned about risks with applying the approach these focussed on the maturity of the approach and Digital Twin requirements and competency of the system engineering practitioners in applications such as risk-based decision making and PHM.

Chien *et al*. (2014) suggested that insufficient risk management knowledge and techniques were barriers to risk management and established a research study to identify risk factors and assessment methods for BIM construction projects specifically. They reviewed literature to identify risks from construction, software and BIM projects. They then applied DEMATEL to determine critical risk factors in BIM projects and applied to a case study to propose allocation of risk among collaborating partners. They identified legal risk due to breach of contract and IP protection in relation to general construction projects. This resulted in 'Legal Risk' as an identified risk factor dimension with 'Lack of BIM Standards' and 'Unclear Legal Liability' as the risk factors.

Overall, increased use of systems modelling related to complex systems and integration of assurance of multiple emergent properties is becoming more evident. Case studies of collaboration using complex digital technologies are increasing for BIM in the built environment in particular but there is still limited case study material for other sectors.

2.4 Initial Context

2.4.1 Approach to Identifying Initial Context

The context for using Digital Twins for decision support was explored and characterised to provide a frame for developing the research design for the risk framework. A purposive

approach was used to provide sufficient understanding of the context to enable the research design for Stage 2 to be developed. The characterisation of context also provided a frame for reflection on the scope and applicability of the risk framework and was revisited regularly during the research project. Initially the context was explored from three perspectives:

- Digital Twin decision support purpose and use cases.
- Types of IP Risk associated with Digital Twins.
- Frameworks, standards and industry practices for mitigating life-cycle risk.

The exploration of Digital Twin decision support purpose and use cases informed the definition of Digital Twin adopted for relating types of IP Risk and later for the development of the risk framework. A broad definition of Digital Twin was adopted in the initial stage of the project and then refined during Stage 2. This is discussed in section 2.4.3.

The analysis of literature resulted in an initial characterisation of context in relation to Digital Twin decision support services purpose and use cases as illustrated in Figure 2.

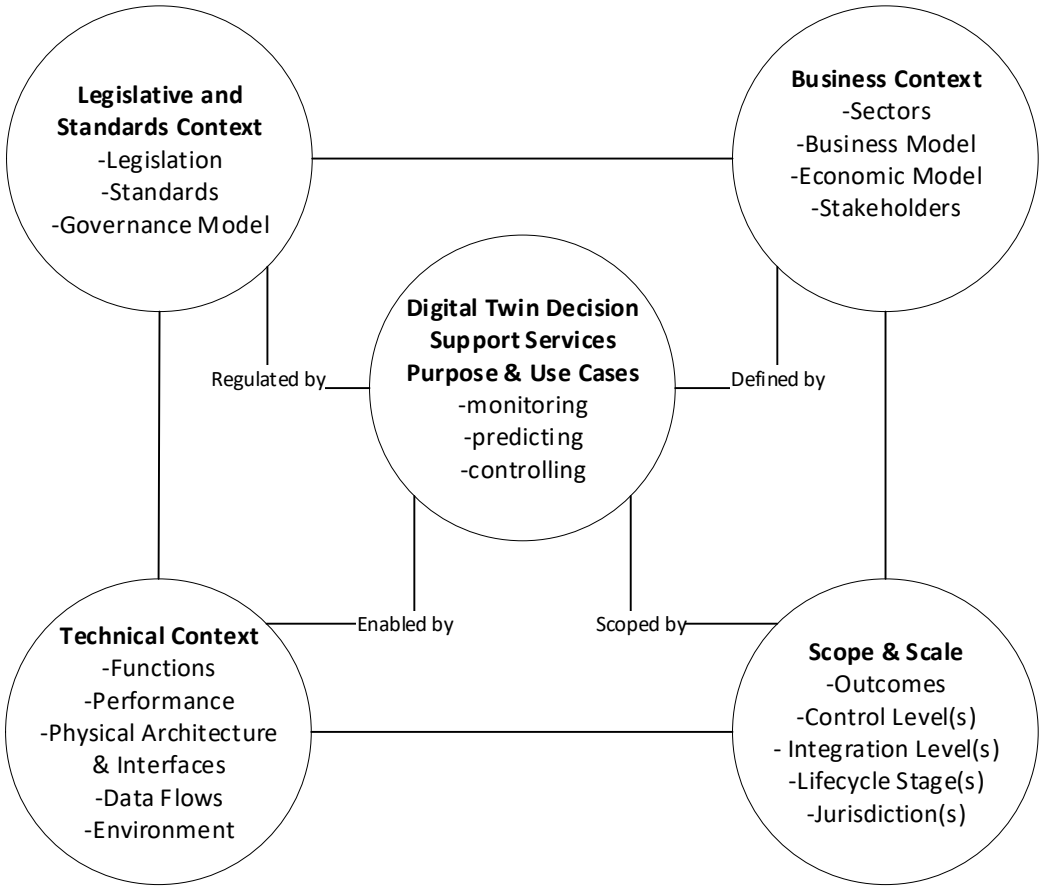


Figure 2 - Characterisation of context for Digital Twin System based Decision Support Services

Social and political factors are considered to be part of the business context. The following sections discuss the literature that contributed to the characterisation. The literature informing the context was also reassessed as part of implementation of Stage 2 of the research to code factors of importance for risk management.

2.4.2 Digital Twin Decision Support Purpose and Use Cases

A research objective to support scoping the research study was to review literature to define and characterise Digital Twin decision support purpose and use cases requiring multi-stakeholder collaborations in selected regulated sectors through a Physical Entity's life-cycle. This was then used to focus the scope of the study.

A search of the Scopus database for journal and conference proceedings with title, abstracts and keywords using criteria such as "Decision Support" AND "Digital Twin" AND ("Use Case" OR "Purpose") was initially used to reveal a sample of Digital Twin decision support purpose and uses, illustrative of the range and nature of applications across sectors. The search was periodically revisited during the study and revealed 39 out of 41 reviewed abstracts (to end 2023) with example decision support use cases. One article was excluded as it focused on automation rather than decision support and the remaining article, which emerged part-way through the research study in 2022, by Dos Santos *et al*, 2022, was a review paper documenting a systematic literature review of the use of simulation with Digital Twin to support decision making in production. Dos Santos *et al*, 2022 sought literature widely from Scopus, Web of Science, IEEE Xplore and Science Direct using the keywords "Simulation" AND "Digital Twin" and found that the main sectors of application were in manufacturing, service, logistics, construction and healthcare. A mapping of purpose and use cases with application sectors is illustrated in Table 4 with new sectors such as agriculture emerging from 2023.

Business Sectors (Examples)	**Decision Support Purpose and Use Case Examples**	**Example Article References**
Primary Sector – Raw Materials		
Agriculture	Intelligent Agriculture Managing carbon-water balance during food production for food security and sustainability. Flower bud thinning labour decision support.	Wang *et al.* (2023) Pickering *et al.* (2023(

Business Sectors (Examples)	Decision Support Purpose and Use Case Examples	Example Article References
Water	Dynamic demand assignment - Real-time operational management of water infrastructure systems	Shafiee *et al.* (2020)
Secondary Sector – Utilities, Mining and Quarrying, Manufacturing and Construction		
Manufacturing	Optimised integration of human operators in a manufacturing workflow (Industry 5.0); Precision manufacturing tolerance control and defect avoidance; materials handling; production performance monitoring.	Cutrona *et al.* (2024) Becue *et al.* (2020) Teicher *et al.* (2023) Watkins *et al.* (2021) Papacharalampopoulos *et al*. (2020)
Construction	Construction 4.0 (building design-planning-construction) Construction Process Optimisation	Yitmen *et al.* (2021) Altan and Isik (2023)
	Optimisation of asset lifecycle management e.g. condition monitoring and health assessment.	Macchi *et al.* (2018)
Utilities	Electricity Distribution Grid Operations and Management	Ruhe *et al.* (2022)
Tertiary Sector - Services		
Retail	Customer Service Design	Yan *et al.* (2022)
Healthcare	Clinical Decision Support e.g. Personalised patient journey for cancer treatment; remote patient-doctor interaction: constant patient monitoring, remote care; ventricular tachycardia prediction.	Keller *et al.* (2023) Zanitti *et al.* (2023)
Transport & Logistics	Supply Chain Management e.g. Drug supply and delivery chain optimisation, automotive industry distribution optimisation, real-time management of logistics systems.	Schenk and Clausen (2020), Korth *et al.* (2018)

Business Sectors (Examples)	Decision Support Purpose and Use Case Examples	Example Article References
	Warehouse Management e.g. Scenario comparisons and performance prediction	Sahlab *et al.* (2022), Baruffaldi *et al.* (2019)
	Transport Management e.g. Circular Economic management for sustainable vehicle life-cycle; maintenance scheduling - ship systems monitoring to manage manoeuvrability	Mugge *et al.* (2023), Uehara Sasaki *et al.* (2022)
	Eco-routing in cities to improve mobility sustainability	Aguiar *et al.* (2022), Belfadel *et al*. (2023)
Facilities Management	Industrial facility monitoring; industrial facility carbon footprint optimisation	Sun *et al.* (2022)
	Strategic facility management. Urban facility management: planning, scheduling maintenance operations and interventions	Mbabu *et al.* (2023)
	Offshore floating and subsea facilities operation	Hansen and Jaiswal (2023) Eriksson and Markussen (2023)
	Smart infrastructure management for sustainability and resilience	Phoon *et al.* (2022)
Quaternary Sector		
Public - Civic	Crisis Management e.g. Metro station crisis prediction and preparedness	Conges *et al.* (2020)

Table 4 Sample of Decision Support and Purpose of Digital Twin Cases to end 2023 (Scopus)

Decision Support purpose related to outcomes of 'Optimised System & Process' and 'Managed Resources' across a range of business sectors. This relates to common objectives for Digital Twin use indicated by Kritzinger *et al.* (2018) such as increased competitiveness, productivity and efficiency, with additional objectives such as sustainability and safety identified in Table 4. Within the 'Scope & Scale' characterisation, a series of 'Outcomes' can be identified with an example: 'optimised system productivity'.

The main decision making use cases reported by dos Santos *et al.* (2022) were classified as production planning, process evaluation, process control, resource allocation and routing. This classification, chosen by the authors in relation to simulation related to production was published after 2020 when the current research design was developed. Although planning, evaluation, control, resource allocation and routing was evident in the examples a more useful classification for the current research study was considered to relate to a broad grouping of management focus which could be related to strategic, tactical or operational management and considered relative to one or more performance objectives, 'Outcomes'. This was reflected as 'Scope & Scale'-'Control Levels'.

Macchi *et al.* (2018) had previously categorised five use cases which used Digital Twin for Asset Management into a matrix of asset lifecycle phases (beginning of life, middle of life, and end of life) versus asset control levels (strategic level, tactical level and operational level). Four out of the five case studies were mapped to the middle of life stage. Table 4 also identified that while some use cases focussed on a life-cycle stage such as operations, others were focussed on multiple lifecycle stages and full life-cycle optimisation. As such categorisation of 'Scope & Scale' by 'lifecycle stage(s)': design through manufacture, operations and disposal related to the 'Outcomes' was considered. For example, 'Purpose' of "predictive maintenance" may have a 'Scope & Scale' related to 'optimised safety, efficiency and effectiveness' for 'operational and tactical management' from 'operation through to disposal'.

The 'Scope & Scale'- 'integration level' was considered to reflect whether the decision support services related to an asset, system or process, or System-of-Systems.

After it was established that Digital Twin is utilised for decision support across sectors the 'Scope & Scale' focus for the research study was defined.

Web based literature relating to the UK's National Digital Twin programme (Enzer *et al*, 2019) was reviewed as a case study source for illustrating decision support purpose and use cases driven by a national strategy. The programme was established with the purpose of connecting an ecosystem of asset and enterprise Digital Twins for managing better outcomes for the built environment. This is considered to include energy management, traffic and transport as well as city planning, construction and services such as healthcare. Rail project High Speed 2 (HS2, 2022) had a vision for using life-cycle Digital Twins for increasing

productivity and reducing operational risk. The National Digital Twin programme identified principles called the Gemini Principles (The Centre for Digital Built Britain, 2018), to provide values to focus Digital Twin applications. The three main principles of Purpose, Trust and Function are each subdivided into three sub-values. The principle of Purpose identifies the need for a clear Purpose which must deliver genuine public benefit, enable value creation and improve performance and provide insight into the built environment. Mapping this to the elicited Outcomes from the literature review and this could extend the description to examples such as 'System & Process Optimisation for Improved Performance and Value Creation' and 'Resource Management for Public Benefit'.

Given that there is broad interest in Digital Twin applications for life-cycle management purposes optimised against performance objectives this was considered as the focus for the current research study. Considering example life-cycle management purposes, the Scopus search criteria was refined with "maintenance" as an example application life-cycle focus in the search term instead of ("Use Case" OR "Purpose") and a particular interest in this topic was noted with 58 pre-filtered Conference Papers and Articles in English. Of particular interest was a literature review by Errandonea *et al.*, 2020 that characterised Digital Twin maintenance papers by industrial sector. This identified maintenance purpose in the literature across several sectors, particularly manufacturing, the energy industry and construction with transport also represented as aerospace, naval engineering, railway and logistic services.

In order to manage the scope of the research project early stages of the project considered the context of the transport and gas supply sectors more broadly, as the researcher had access to stakeholders through established links to industry trade organisations for data collection. The context was later narrowed to the rail sector, within the broader transport sector, during research Stage 2 given the stakeholder interest from this sector such as the Digital Twin services vision from the High Speed 2 project in 2022 (HS2, 2022). The use cases of focus were considered consistent with the context of the Department for Transport (UK) Transport Data Strategy (Department for Transport, 2023) and the EU Data Strategy (European Commission, 2023) that emerged during the research study as there is a focus on using sensors and data to 'improve user experience', which can relate to the Gemini Principle Purpose of Public Benefit and creating a data platform to integrate with the National Digital Twin (The Centre for Digital Built Britain, 2018). The focus for the research study was identified as:

- Rolling Stock Digital Twins for purposes of asset lifecycle management e.g. predictive maintenance (asset level) and fleet availability (System-of-Systems level)
- Subsystem Digital Twins e.g. HVAC, within Rolling Stock for the purposes of asset lifecycle management e.g. predictive maintenance (asset level)

During the research project the Department for Transport website was monitored for emerging use cases. In 2023 they issued a report documenting the steps towards a Digital Twin for urban transport based on a project initiated in the autumn of 2021 (Department for Transport, 2023). This initially considered use cases for forecasting using real-time data, identifying low traffic areas and monitoring decarbonisation. The initial stages focussed on technical facilitation of data sharing and mapped out steps towards full urban Digital Twin and further use cases. They identified a future need to build a City Scale Digital Twin and resolve issues such as responsibilities for data ownership, maintenance, curation and storage. Such case studies would provide cross sector collaboration.

In 2023, the Transport Research and Innovation Board (TRIB) produced a 'Digital Twin Roadmap 2035' (TRIB, 2023) comprising four workstreams. The 'Enabling Environment' workstream contained a component 'Legal and compliance' with a target output end in the period 2026-2030. This aims to provide a legal framework to include IP and certification requirements and for data sharing, access and authorisation. This further demonstrates a need for the current research study and supports a focus on rail.

2.4.3 Definition of Digital Twin

The concept of the Digital Twin is considered by many academics, such as Madni *et al*. (2019), to have originated with Grieves in the early twenty first century. Despite this there have been various discussions in the literature relating to definitions with Grieves & Vickers (2017) commenting on the different understandings of the concept across fields. They illustrated this in their discussion of the Digital Twin application differences between discrete and process manufacturing that arise from a view of the lifecycle, scale and precision requirements. The concept has been defined in recent standards such as BS ISO/IEC 30173:2023 (British Standards Institution, 2023b) but there is still a diversity of definition in both the academic and practitioner literature and no "universally accepted definition" (Abdelrahman et al., 2025).

However, there are common features within definitions which have endured and clarified during the period of this research study and these features have informed the definition adopted. The definitions in the Reference section include Digital Entity, Digital Object, Digital Model (also referred to as Virtual Model) and Digital Twin (also referred to as Virtual Twin), and the definition of a Digital Twin System which comprises the Digital Twin, linked Physical Entity and the data connections, Digital Entities, Digital Models, data and interfaces which provides the functionality for the Digital Twin based decision support system. These definitions were related to the definition in BS ISO/IEC 30173:2023 (British Standards Institution, 2023b) which was published during this research study. The Digital Model relates to a Physical Entity and contains the metadata about its properties, content, behaviour, interfaces and relationships with other entities, but it may not be continuously linked to the Physical Entity through time. It can provide a representation at an instance in time or possible representations from simulation. The Digital Twin is the digital representation of a Physical Entity with data connections to that Physical Entity enabling convergence between the physical and digital states at the required synchronisation rate and provides an integrated view through a Physical Entity lifecycle. As such the Digital Twin comprises Digital Models but the particular link and synchronised relationship with the Physical Entity is important.

Qi *et al*. (2021) introduced the 5 dimension Digital Twin model, which was used during the early stages of this research study, as it provided clarity on the enabling technologies that could attract IP within the Digital Twin System. The 5 dimensions are connected to each other and comprise: Physical Entities, related Virtual Models defined as "faithful replicas of Physical Entities" (Qi *et al*., 2021), Digital Twin Data, Services and the connections between them. Services included application services for users such as simulation, monitoring and health management and third party services such as algorithm services and data management services. Qi *et al*. (2021) then identified a framework of enabling technologies linked to each dimension through a defined connection type.

Within literature the nature of connection between the Physical Entity and Digital Twin through the lifecycle has emerged as a consideration for the Digital Twin definition, with a two way connection with data flow from sensors from the Physical Entity to the Digital Twin and control instructions from the virtual (or digital) to the physical. Where there is a one-way data connection, usually from the physical to digital, this is often referred to as a Digital Shadow (Kritzinger *et al*., 2018).

For application to the rail sector, definitions, arising from research projects to develop rail specific Digital Twin Systems, such as Europe's In2Smart2 (Dambra *et al*., 2021) derive from Grieves definition and application in the manufacturing sector, such as Issa *et al.* (2023), although there are less precise definitions prevalent such as the In2Smart2 project referring to, and permitting, a broad range of definitions (Dambra *et al.*, 2021). More recently, relevant to the rail scope of the current study, Adeagbo *et al.* (2024) discussed the clarity of definition of Digital Twins in relation to health monitoring rail transit systems seeking to clarify terms. Their schematic of a Digital Twin included the two-way data connection between the physical and digital and identified the data management, storage, modelling and analytics elements consistent with the definition adopted in the current research study.

For the purposes of the current study, Digital Shadows are included as both Digital Shadows and Digital Twin Systems are relevant to a range of purposes for decision support for which collaboration risk is important.

For participants to the study during the initial data collection it was acknowledged that the definition of Digital Twin varied to some extent based on sector and application, but broadly applied to use cases which closely relate virtual/digital and physical assets with data, and which include increasing levels of sophistication in the relationship between the digital and physical, from exchange of sensor data, to applying data analytics to predict physical behaviour, to real-time control interactions. The briefing did not distinguish between Digital Twin or Digital Shadow. For the online questionnaires in particular the definition needed to be succinct, as shown in Appendix 4, immediately prior to Question 16.

During the development of the research project the definition was refined and presented to evaluators verbally with the support of a visual representation based on Figure 3, showing the Physical Entity in its physical and operational environment, Digital Twin System comprising the representative Digital Twin in its representative virtual environment, data storage of historic model instances through time and the services and user interfaces. The connections were identified from physical sensors to the Digital Twin System and in the opposite direction to controlling actuators. The terminology of Digital Shadow and Digital Twin was

introduced although it was verbally clarified that both were in scope for the framework.

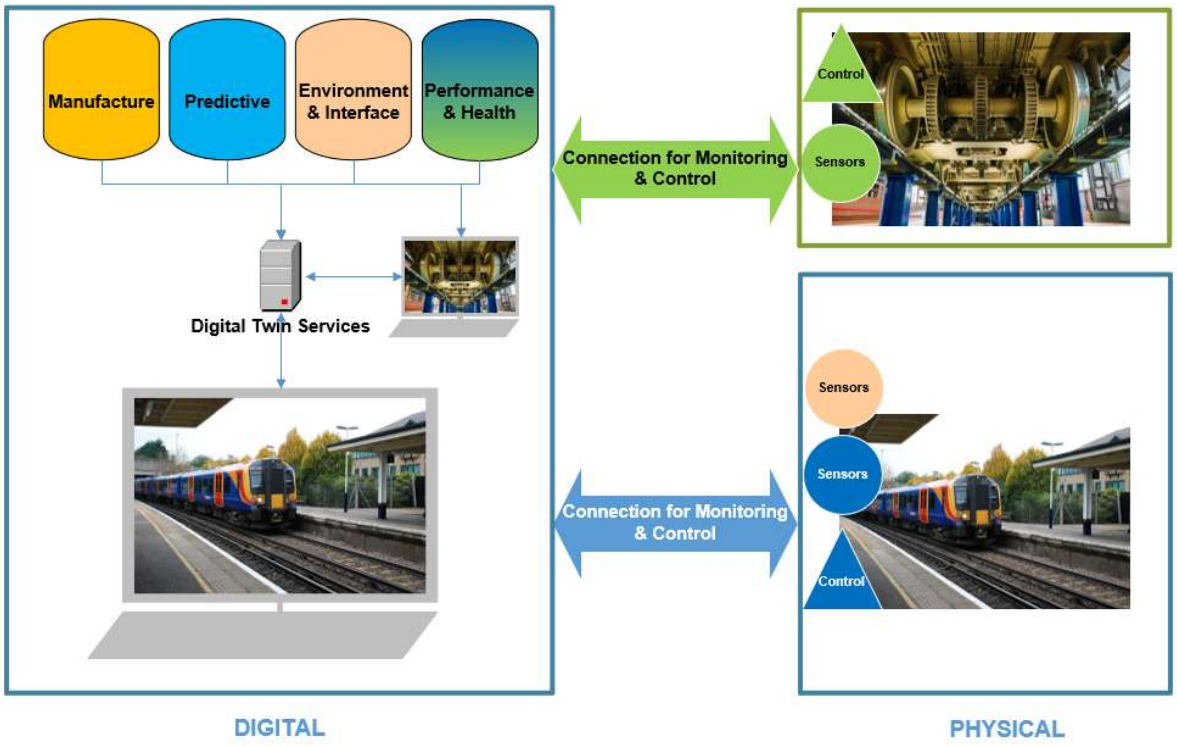


Figure 3 - Digital Twin Based Decision Support – Rolling Stock Maintenance Example

Note that the photographs in Figure 3 were accessed via Microsoft PowerPoint which identified them as by unknown authors licensed under CC-BY-NC-ND. The train is a Class 450 (Unknown Author, nd a) with a photograph of a train undergoing maintenance to represent maintenance processes (Unknown Author, nd b).

2.4.4 Types of Intellectual Property Risk Associated with Digital Twin

A research objective to support scoping the research study was to clarify the types of IP risk through literature review and relate these with the Digital Twin Decision Support Services context.

A purposive approach to the literature review started with identifying potential legal issues from socio-legal text books such as Murray (2016) and Daly (2016) and academic articles relating Industry 4.0 and IP, particularly considering issues for additive manufacture reported in Clementson *et al.* (2021a) as part of the current research study. This was supplemented with online sources specifically referring to IP issues with digitisation and mention of legal concerns in more technical journal papers. These technical papers were required to reveal the Digital Twin architecture related to particular legal issues. The initial coding of legal issues

in literature is documented in Appendix 4 (A4.2) which identified IP and other legal risks as important for Digital Twin systems as follows:

- Intellectual Property: Digital Twin System parts (Data, Services, Models, Connections, Digital Twin infrastructure) and Physical Entity
- Legal Compliance: Data Protection, Security and Information Governance
- Liabilities: From the impacts of decisions made using Digital Twins and the relationship with decision capability, data quality, artificial intelligence, service failures and sharing and segregation of liabilities.
- International Legal Issues, particularly as services and infrastructure can cross national borders; internet governance.

Specific commentary on legal issues with Digital Twin systems started to emerge from the professional legal sector in the early stages of the research study. For example, Bird & Bird LLP (2020) wrote an article on legal implications of Digital Twin system applications in the supply chain. This identified that there were many challenging legal issues, made particularly challenging due to the lack of a regulated legal framework and standards. Legal issues identified included IP with technology contributing to Digital Twin systems, dataset rights and the need to regulate the trade secrets and IP contained and used through the Digital Twin through contract, as well as technical approaches such as cyber security to protect the Physical Entity information. Other legal rights included data protection and liabilities relating to the use of the Digital Twin system, such as monitoring or controlling a safety-critical system. Wang *et al*. (2020) published a review of Digital Twin technology patents concluding that they mainly appear in the manufacturing sector but covered a range of technologies and applications. Mendis *et al*. (2020) provided specific commentary on the law with respect to CAD files, design data and materials and hardware relating to 3D printing.

The review was then extended to Digital Twin for rail decision support and reported in Clementson *et al.* (2021b) which identified the IP risks in relation to Digital Twin System architectures using a rolling stock example to illustrate. This revealed the following example mapping of IPR to generic Digital Twin System architecture. Trademarks, although also an IPR, were less visible as an issue in the literature in the early stages of study and so excluded from the table:

Components of Digital Twin with associated technologies	Copyright	Database Right	Patents	Industrial Designs	Trade Secrets	Example Stakeholder Ownership
Physical Twin: Including sensing technology, material technology and process technology	√		√	√	√	Designer Manufacturer Physical Twin Owner
Virtual Twin: Including simulation technology, visualisation technology, model evolution etc	√		√	√	√	Designer Manufacturer Physical Twin Owner Operator
Data Communications: Including communications technology, interfaces technology, interaction technology, collaboration technology, security technology etc			√	√	√	Manufacturer Physical Twin Owner Contractor
Services Including Architecture technology, algorithm technology, software platform technology (e.g. XaaS, Pay as you go service model)			√		√	Manufacturer Contractor
Data Including collection technology, storage technology (e.g. Public Cloud, Hybrid Cloud, Private Cloud etc), Processing Technology etc	√	√			√	Designer Manufacturer Physical Twin Owner User, Operator Maintainer

Table 5: Clementson *et al.* (2021b) Table 1 – Example IP Rights

Clementson *et al.* (2021b) observed that there could be several IP owners associated with the Digital Twin and life-cycle stages and progression was important for risk consideration in the current research study as over the Physical Twin life-cycle there may be changes in perceived IP value and the business context and characteristics of specific stakeholders involved.

The IP Management processes comprise identifying, evaluating, protecting, defending/enforcing and exploiting IP. Delivery of the purpose of the Digital Twin can be impacted through breakdown of the relations between collaborating stakeholders due to a deliberate or accidental IP Breach and financial implications associated with protection strategies and for recovering damages during a breach. Financial impact from IP theft can arise from reduced sales and competitive advantage and legal costs. IP value can be lost if protection is found to be invalid.

The context of the rail sector business environment considered by Clementson *et al.* (2021b) identified potentially complex contractual relationships between train manufacturer, train owner and financier and train operator as well as third parties in the provision of services, and raised questions of clarity, illustrating potential risks.

At the start of the research study, the legal environment relating to complex digital systems was not mature. Although there is a World Intellectual Property Organisation (WIPO) seeking to harmonise practices, the laws and application of law varies from region to region. For example, within the European Union the contents of a database could potentially be protected by sui generis database rights through application of 'Council Directive 96/9/EC' (1996) if it can be demonstrated that there has been substantial investment in the obtaining, verification or contents of the database. However, this protection is not available outside the European Union. Digital Twin implementations also need to consider protection of digitised information that contains Trade Secrets as laws such as coded in 'Council Directive 2016/943' (2016) require measures to be in place to keep such information secret and do not directly protect against reverse engineering. (Clause 16 and 17 'Council Directive 2016/943' (2016)).

The legal context for rail and transport mobility evolved during the study. For example, the Data Governance Act (Council Regulation 2022/868, 2022) was adopted in the EU in May 2022 to encourage trust in data sharing mechanisms related to protected data, to include that protected by IP rights, held by public sector bodies. It introduces regulated 'data intermediaries' for managing the data. Emerging context provided opportunity for reflection and support for the constructed framework.

2.4.5 Frameworks, Standards and Industry Practices for Mitigating Life-cycle Risk

A research objective to support scoping the research study was to identify existing frameworks, standards and industry practices for mitigating and managing life-cycle risk related to the decision support purposes in one or more regulated sectors, through literature review, to explore how they relate to the identified IP risks. A purposive approach was adopted using a range of initial search criteria applied to academic journals and practitioner sources such as standards databases and websites.

Although WIPO provides an overall international frame for IP, there are specific national rules, implementations and interpretations such as the EU Database Directive ('Council Directive 96/9/EC' (1996)). TRIB (2023) identifies that a legal framework for Digital Twins is not mature and presents a roadmap to develop one by 2030. However, the application of Digital Twins operates within an overall legislative and business context, and standards to frame Digital Twin developments have emerged over the timeframe of the research study such as BS ISO/IEC 30173:2023 (British Standards Institution, 2023b).

Risk management for all sectors and businesses is covered by the BS ISO 31000:2018 (British Standards Institution, 2018) series of standards with focus on information security risk in BS ISO /IEC 27001:2023 (British Standards Institution, 2023a)

The risk management context for life-cycle Physical Entity decision support, was explored for rail as an example sector.

In Europe the legal framework for the rail sector is underpinned by legislation such as the Interoperability Directive ('Council Directive 2016/797' (2016)) and the Railway Safety Directive ('Council Directive (EU) 2016/798' (2016)) which require demonstration of compliance with Essential Requirements ('Council Directive 2016/797' (2016)). Each Essential Requirement is itself underpinned by more detailed regulatory requirements such as the Common Safety Method (CSM) (Commission Regulation No 1078/2012 (2012)). There are then country specific legislative requirements implemented such as the UK's ROGS (2006) and the *Health and Safety at Work Act 1974.* The key features from these regulations are summarised in bold and illustrated using the safety requirement as an example:

- **Stakeholder regulatory duties** – Duties placed on specific sector stakeholders to develop management systems that meet certain criteria. For example, in the UK ROGS (2006) Regulations 3 and 4 require a rail operator to secure a Safety Certificate and the infrastructure manager, to secure a Safety Authorisation to confirm their Safety Management Systems are assessed as effective.
- **Management Systems** – Describes the processes for how the rail operator and infrastructure manager will safely manage their operations. Describes the risk assessment and tools and demonstrates compliance with legislation and standards such as the risk assessment methodology prescribed in the CSM ('Council Directive (EU) 2016/798' (2016), Article 6(3)(a)). For risk management,
    - **Risk Management** – Identifies risks and mitigations implemented for safe and secure operations. Plans, organises, monitors and adjusts performance as required to maintain safety.
- **Change Procedures** – Procedures to demonstrate safe introduction of new or altered assets and systems.
- **Governance and Assurance** – Defines roles and responsibilities. For safety, a National Safety Authority and independent Assessment Bodies assess and audit

Safety Management Systems in support of the issue of Safety Certificates and Safety Authorisations.

- **Collaboration** – Requires stakeholders to work together to operate a safe system (ROGS Regulation 22).
- **Guidance** – Provides approaches and required records for establishing Management System details for achieving outputs such as Safety Certificates and Safety Authorisations. National organisation such as RSSB further publishes management resources such as risk assessment templates and generic hazards lists.
- **Standards** – Sector specific standards are used to support safety and interoperability and support stakeholders to achieve their legal obligations.

Comparing rail with another sector, the Gas Distribution Sector, IGEM publishes standards which demonstrate similar approaches to the rail sector. For example, standard IGEM/GL/4 (Institution of Gas Engineers and Managers, 2018) provides the requirements for a safety management system relevant to gas system assets.

Governance and assurance are supported by specific standards such as the rail sector standard for supplier assurance Section G 2.2.1.4 RIS-2750-RST (Rail Industry Standard (2021)) of which covers a broad set of risks, to include contractual, reputational and financial risks. However, governance and assurance are also related to regulatory requirements for the presentation and assessment of Assurance Cases, such as Safety Cases (*The Railways (Safety Case) Regulations 2000*)

An Assurance Case is used, "*to demonstrate confidence in system properties of interest (e.g. safety and/or security)*" (Wei R *et al.,* 2019)

Piovesan *et al.* (2017) defines an Assurance Case as: "*a structured argument, supported by evidence intended to justify that a system is acceptably assured relative to a concern (such as safety or security) in the intended operating environment*."

An Assurance Case would be applicable to the implementation of a life-cycle Digital Twin based decision support system in that the use of the Digital Twin can have an influence, either directly or indirectly on the safety, security or performance of a Physical Entity, for example where decisions, automated or manual, based on the information from the Digital Twin or communicated to the Physical Entity, influence operations and maintenance

performance. Legal risks can relate to the duties of stakeholders involved directly or that indirectly impact the assurance of a concern. For example, where IP is allowed to be used for an unlicensed purpose or a contract is breached this could lead to unavailability of the Digital Twin service which could impact the safe operation of the Physical Entity.

Nair *et al,* 2014 carried out a systematic literature review on the provision of evidence for safety certification. They found that the techniques used for structuring evidence to show compliance with safety standards was "argumentation-induced evidence structure" in 92% of cases. The arguments could be expressed graphically or textually. Graphical methods such as GSN (Kelly and Weaver, 2004) and CAE (Bishop and Bloomfield, 1998) present a top level claim asserted within an argument, a description of the arguments to support the claim and reference to the evidence that is presented to support the claim. Model based evidence includes sector-specific UML meta models for standards such as BS EN 61508 (British Standards Institution, 2010), data modelling using entity-relationship diagrams to structure the data content of large safety cases and process models for capturing the activities in processes that produce the artefacts and present them in a tree based structure. Such model based assurance approaches were evident in assurance of complex systems such as train control systems with a recent example for autonomous trains (Chelouati *et al.*, 2023).

Wei *et al.* (2019) identify that the Object Management Group (OMG) has specified a standard called The Structured Assurance Case Metamodel (SACM) to provide a wider set of features than existing system assurance languages and approaches. SACM provides the foundation of model-based systems assurance, and it was shown that GSN can be written to be SACM compliant.

Introducing or using a Digital Twin for a decision support purpose, would, in many cases, require a change impact assessment to ensure operational safety and security are assured and this could be extended to an impact on other system properties such as cost and reputation. Within the context of digital assurance approaches for assuring system properties, factors and goals related to the effective management of IP, would potentially provide an input to other assurance cases such as safety cases. This context informs the research questions.

For the purposes of initial 'Scope & Scale' the 'Jurisdiction' and 'sector' relating to the specific application will identify the specifics of the Legislative and Standards context. However the specific context is located within a national and international context which

have broadly consistent elements and are based on international principles such as ISO 31000:2018 (British Standards Institution, 2018) for risk and WIPO (World Intellectual Property Organisation, 2010) for legal frame.

2.4.6 Context Summary

The review of Digital Twin Decision Support context was intended to provide an initial understanding of the risk context to support the research study design and provide a means to focus the scope and scale of the research project. Figure 2 was developed to provide a means of characterising the application scope of the study and to enable a frame for review of broader and general applicability. New literature related to context that emerged during the study was reviewed for impact. In particular, the need to manage IP risk to Digital Twin collaboration and develop a legislative framework to support is increasingly articulated such as through the TRIB Roadmap (TRIB, 2023) and Digital Twin specific standards are starting to emerge. As such this research project was considered to be timely.

2.5 Rationale for the Research Questions and Aims

The potential for IP considerations to contribute to collaboration risk using Digital Twins was confirmed therefore underpinning the need to understand those risks. The literature review of prior work and context suggested that while it was acknowledged that there were risks and there was discussion about some specific issues or a particular technical solution, overall risks and how to mitigate them were not well understood due to separate presentation of business, technical and legal viewpoints and there was a need to combine these. This led to the Research Questions 1 and 2.

Research Question 1 - What factors are important for describing how IP can influence multi-stakeholder collaboration risk using Digital Twin Systems for decision support?

Research Question 2 - How do these factors relate to describe overall risk and provide the basis for collaborating stakeholders to manage and assure that risks are mitigated?

Answering these Research Questions enables the Aims 1 and 2 to be met.

Aim 1 – To explore and describe a framework for understanding how IP can influence multi-stakeholder collaboration risk using Digital Twin Systems for decision support through the Physical Entity life-cycle.

Aim 2 – To explore how this framework could be applied to assure that life-cycle IP Risks to Digital Twin Collaborations are effectively managed.

Meeting the Aims, contributes to the goal of guidance assumed to be needed at the start of the research project as stated in section 2.2.

This guidance is identified as a described framework. A framework provides the supporting structure which is the first step for developing specific guidance. The framework provides the components, ideas, principles and the relationships between them justified in relation to its scope and purpose. As such, the framework for Aim 1 will identify and justify the legal, technical and business factors important for understanding collaboration risk and how they relate to influence risk.

As discussed in section 2.4.5, frameworks related to risk management enable risks to be identified and mitigated through planning, implementing and monitoring activities and through lifecycle stages and changes. This permits adjustments, as required, to maintain the required performance. As such the structure of the risk framework is expected to build on the structure of business risk management frameworks, that are embodied in standards for risk management purposes, while applying the components and ideas relevant to the specifics of Aim 1. The risk management standards to inform the framework structure are identified in Chapter 6.

For Aim 2, the framework will provide the basis for constructing risk models for specific applications. However, while the framework focus in this current research project is descriptive and illustrative of typical risks and applications, future research could introduce modelling steps to build on the justified descriptive relationships between framework components, potentially building mathematical models to evaluate and simulate context specific risk scenarios. Risk is an exposure to harm or loss, so risk to multi-stakeholder collaboration relates to harm to or loss of that collaboration. The consequences and impact of such risks are related to the required characteristics of the collaboration, such as performance obligations. For example, with a loss of collaboration the decision support purpose may fail. The research then focusses on IP issues that contribute to the consequences and impact of such risks and the causes that lead to the risks.

2.6 Emerging Work

The study of Digital Twin and legal issues is a topic that has received particular academic interest during the period of this research study highlighting the importance for regular review of emerging work after the initial review. For example Figure 4 below shows the increase in Articles and Conference Papers within Scopus to the end of 2023 with title, abstract or key words containing “Intellectual Property” AND “Digital Twin” or “Legal Issues” AND “Digital Technologies” and where the abstract is relevant to Question 1.

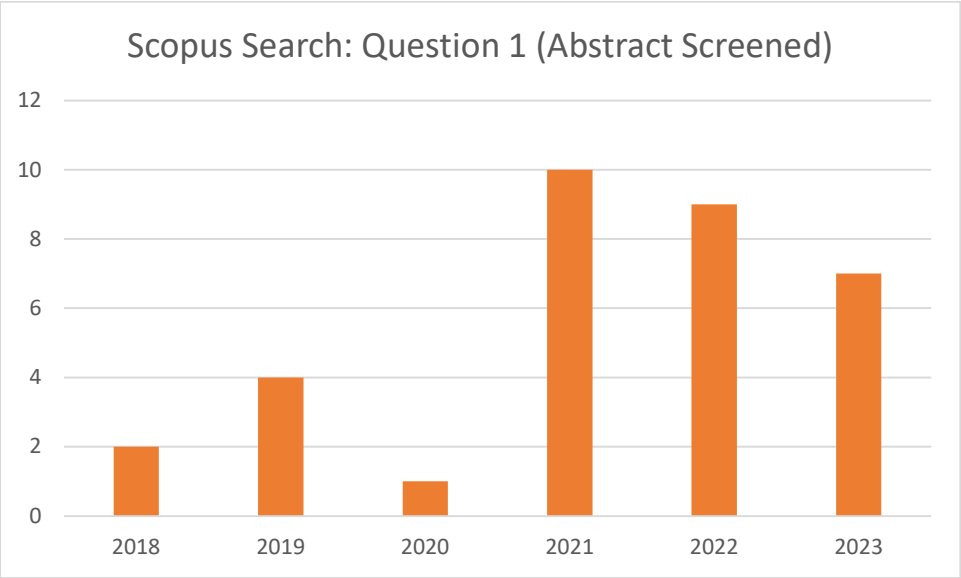


Figure 4 - Scopus Search relating to Question 1 after Abstract Screening (2023)

During 2022 and 2023 there was an increase in technical academic research exploring systems architecture solutions to mitigate security risks. Blakley *et al.* (2022) explicitly identified that multi-partner collaborators sought assurance that IP remains protected, including from disclosure to competitors, and how ECCA systems enable secure collaboration and models to remain isolated and maintained on the owner’s cloud with access control supported by access agreements and secure gRPC. As well as applications considered in the defence sector, there were case studies exploring technical solutions in the health sector, oil and gas and built environment.

A summary of the key emerging studies relevant to the prior work questions, following screening, are summarised below:

Study	Question	Summary and impact on current research study
Yadykin *et al*. (2021)	Question 1	An ontological analysis of the Digital Object in Cyber-Physical Systems and Digital Twins to consider the economic viewpoint. This viewpoint considers ownership, derivation of economic benefits from owning and using the object and transfer of ownership such as through sale. This adds to the technical viewpoint and potentially enables the economics of IP to be considered in the Digital Object properties. The authors future research interests are in developing an analytical framework to integrate the Digital Object into economic activities. Impact: Included as source material for exploring the coverage of and relationship between risk and mitigation factors, confirming the need to link technical and business factors.
Horvath and Rudas. (2022)	Question 1	The authors develop a Lifecycle Representation of Contexts (LRC), for an engineering model system which they define as behaving as a Digital Twin of the physical, with active connection to its contextual world. They state that LRC serves the integration of relevant system IP. Impact: Included as source material for analysis but given the technical focus did not impact the overall framework.
Galvin *et al.* (2021)	Question 2	Qualitative case study exploring collaborative and opportunistic behaviours in alliance contracts and how governance, trust and culture interact.

Study	Question	Summary and impact on current research study
		Impact: Included as source material for exploring identified risk and mitigation factors and their relationships.
Celoza *et al*. (2023)	Question 2	Qualitative study using semi-structured interviews and systematic and iterative qualitative coding to explore how contracts influence information management and to develop strategies to improve this in AEC projects. Impact: Included as source material for confirming identified risk and mitigation factors.
Wei *et al* (2024)	Question 3	Identifies a need for assurance cases to support the operational life of Physical Entities and proposes a model-based systems assurance framework for this purpose applied to a case study of an autonomous vehicle. Impact: Provides support for using model-based assurance cases linked to a Physical Entity lifecycle. This in turn informs the potential benefit identified in the current study of integrating an IP risk framework with model-based assurance approaches (section 8.3).
Burr *et al*. (2023)	Question 3	Considers using model-based assurance methods such as GSN for assuring ethical application of AI and suggests calling this Ethical Assurance. Impact: Further supports potential application of model-based assurance broader than safety and security outcomes with the IP risk framework potentially contributing to system assurance

Study	Question	Summary and impact on current research study
		cases to include a future Ethical Assurance framework.

Table 6: Key Emerging Studies

There were several studies which did not add new understanding to the current study, but reinforced issues already identified such as application of blockchain to protecting IP such as Qiao *et al.* (2022), Celik *et al.* (2023).

Various literature review studies to categorise or summarise current research landscape for Digital Twins emerged during the current project. Omrany *et al*. (2023), although focussed on the construction industry, was particularly useful for reflecting on the areas of DT implementation which included Physical Entity management and maintenance and underpinned the need for the current study. This highlighted challenges hindering implementation, to include privacy and security, and recommended a need for data protection and access controls as well as governance frameworks for industry collaboration.

The research methodology adopted in Stage 2, with purposive review of literature, revealed further emerging studies of interest. For example, in the context of Additive Manufacturing supply chains Adu-Amankwa *et al.* (2023) explored criteria for deciding how, when and why to secure and manage IP. This type of study could inform future research, linked to application of the risk framework (see Section 8.6). Legal practitioner discussions of IP issues with collaborations became more prevalent on the Internet from 2023, such as the blog by Ertle (2023) which highlighted risks such a misaligned interests, theft and control loss and generic mitigations such as licensing agreement and IP assignment considerations.

Part-way through the research study cdbb published a Legal Roundtable Outcomes Report (Rock *et al.*, 2021) documenting the outcome from a series of four workshops with legal experts which discussed the legal difficulties of secure data sharing, dependencies and common sector themes such as data ethics, regulation and finance. The workshops debated IP, data and access issues but concluded the area needed further consideration, highlighting a need for governance of the National Digital Twin to clearly set-out where IP resides. The report is considered to support the hypothesis underpinning the research study while identifying that the issues relating to potential barriers to collaboration with Digital Twins from IP issues require further understanding.

More recent scoping studies of Digital Twin research specifically, such as Wang *et al.* (2024) identify that although Digital Twin research is increasing, the research fields are “scattered” (Wang *et al.*, 2024) and limited.

Chapter 3 Research Design, Philosophy and Methodology

3.1 Introduction

The initial literature review, exploring the basis for the research study, prior work and context, resulted in the confirmed statement of research questions, aims and objectives for the research study. These are presented in Chapter 1. Chapter 3 outlines the research design considerations and underlying philosophical position and theoretical perspective arising from these aims, which resulted in the specifics of the research design. This chapter then outlines the considerations for the selection of methods, tools and techniques considered to implement the research design. The specific implementation features of the research design are then discussed in Chapter 4.

3.2 Research Design Considerations

3.2.1 Character of the Research Questions and Aims

Research Question 1, stated in section 1.4, sought to identify factors important for exploring and describing how IP can influence the risk to multi-stakeholder collaboration using Digital Twins for decision support. Based on the literature review it was anticipated that the research would be conducted in a period of emerging development of Digital Twin System applications for this purpose with potentially challenging and uncertain access to case study data.

Research Question 2, stated in section 1.4, sought to describe and explain how the factors relate to each other to contribute to risk, providing the understanding and basis for stakeholder guidance by providing a functional explanation to enable them to determine how two or more factors combine to influence collaboration risk. As this requires understanding of the identified factors it is sequential to the explorative step associated with Research Question 1 although can progress iteratively and in parallel with it, supporting reflection on the explorative step. Development of understanding of the relationship between factors also suggests a purposive data collection approach, refining information gathering and analysis to improve understanding where there are gaps.

Answering the research questions enables the overall aims of constructing a risk framework which can be used for understanding IP influences to collaboration risk using Digital Twins for decision support.

3.2.2 Character of Digital Twin Systems for Decision Support

Digital Twin Systems are considered complex systems as they combine an arrangement of physical parts, software, data and human interaction and can potentially represent socio-technical systems such as a transport system. Digital Twins can also represent the full life-cycle of a Physical Entity from design through to disposal or a specific life-cycle stage. As the scope of the research study is decision support and at the start anticipated a focus on one or more life-cycle stages, a systems engineering research methodology was considered. Researchers such as Muller (2013), recognising the challenge that systems tend to include a combination of hard engineering and softer human factors (social, psychological, political and cultural), have defined more pragmatic systems engineering research approaches generally applied to study the effectiveness of systems engineering methods and techniques in practice. These tend to start with a statement of an industrial problem linked to an industrial goal with sequential stages leading to a validated hypothesis. However, the current study although having the goal or aim of a framework for understanding risks to collaboration with Digital Twins for decision support, focusses on understanding risk factors rather than studying the effectiveness of methods in practice.

3.3 Philosophical Position

The philosophical position considers both the character of the Research Questions in seeking factors that relate to explore, describe and explain risk, which can have both objective fact and subjective value elements, and the character of Digital Twin Systems, interacting with collaborating humans in organisations and political and cultural contexts, and identifying the importance of value as well as fact based considerations in a systems engineering context.

Saunders *et al.*, 2016 discuss research methods and philosophical assumptions and positions for business student consideration. As risk management is important in the business context to achieve a business outcome, the approaches were reviewed for a fit with the systems engineering view and research questions. For identifying risk factors the ontological assumption is largely objective as whether IP risk can potentially impact collaboration and identification of the risk factors of importance and their causal mechanisms are assumed to be largely universal and relevant across Digital Twin applications. However, there is a degree of subjectivity assumed in the significance of a factor or group of related factors in their potential risk as this could potentially depend on the context of a specific application. It was considered that the level of subjectivity could potentially be reduced by narrowing the

context of focus but comparing a limited number of specific contexts may enable the generalisability and sensitivity to factors to be explored too. However, as the research seeks to focus on identification of the factors and understanding their relationships then the assumption overall is towards ontological objectivity.

As Digital Twin Systems for Decision Support are not yet well established the epistemological assumption is between the objective and subjective continua and includes a mix of experiential and expert viewpoints in defined contexts as well as objective observable phenomena, related to digital technology adoption, with the balance depending on what is available for this project.

The axiological assumption is towards subjectivism as the values and views of stakeholders in relation to IP risk and how they perceive their importance could potentially have an impact on collaboration. The views of those involved in managing risks is therefore considered to be important. However, the research ought to ensure factors that are logically and objectively important are revealed to provide understanding of risk detached from the current perceptions of stakeholders, as it is known that implementation experience with Digital Twin Systems is still maturing and objective considerations ought to reveal insight that may challenge and be missed by reliance on values alone.

The overall philosophical assumptions that have informed the research study design are reflected in Table 7.

	Objective	Subjective
Ontology		
Epistemology		
Axiology		

Table 7: Philosophical Position of the Research Project

The extreme objective, Positivist and subjective Interpretivist philosophies were therefore not considered appropriate to the research questions. As such Critical Realist and Pragmatist philosophies were further considered.

A Pragmatist, multi-philosophical approach, fits with systems engineering research that seeks an industrial, practical solution to meet an industrial goal (Muller, 2013). In the case of the current research study this would be the goal of practical risk management guidance for

Digital Twin System collaborators. However, there are several steps needed to achieve practical guidance and the first steps of understanding the risks is a current research gap, reflected in the Research Question 1 and so the current research study needs to focus on this initial understanding. In particular it aims to identify and understand the risk factors and their relationships as the basis for future practical guidance before exploring how this understanding could be applied to assure risks are managed. These aims required understanding that the real risk factors, even if not all observed through empirical observation, would need to be identified and this focus on description of factors in the context of structures of reality that influence observable events favoured a Critical Realism philosophy. As such this required the research study to consider mitigation of bias through reflection, and data collection approaches and explanation of causal mechanisms.

3.4 Theoretical Perspective

Stage 1 of the research study tested the hypothesis and premise for the research study through literature review and so was deductive. However, Stage 1 revealed that there may not be significant empirical data from Digital Twin research and implementations although such would increase during the period of the research. Even studies published during the research period such as Jeschke and Grassmann (2021) were highlighting insufficient available empirical research data on Digital Twin Systems.

The next stage of the research study, with a focus on exploration and description, required an inductive theoretical drive to generate and build theory and present this in the form of a framework. However, this stage also required retroductive theorizing, that is iterative evidence-informed and theory-driven analytical steps, to reflect on the completeness of the factors identified and describe and understand the relationship between them.

Fitting within a systems research frame, a final verification and validation stage was required to ensure the constructed theory answered the research questions. This required a deductive evaluation of the final framework and so the main part of the research study is abductive overall.

3.5 The Chosen Research Methodology

Based on the Research Design considerations (section 3.2) a Systems Engineering Research Method (Muller, 2013) was applied to frame the research. This was developed with consideration of the structure of a Design Science Research Methodology (Gregor and

Hevner, 2013, Peffers *et al.*, 2007, Offermann *et al*, 2009) which provides progressive stages to the research design. The consolidated stages are identified as:

- **Stage 1: Problem identification and definition** – literature analysis to identify the problem through an initial hypothesis, working assumption and context and then to describe and justify the research aims, objectives and research design;
- **Stage 2: Analysis and Risk Framework Design** – implementation of the data collection and analysis part of the research design to achieve the aim of a risk framework which answers Research Questions 1 and 2 and concludes with hypotheses that these are answered;
- **Stage 3: Evaluation** – evaluation and testing of the declared hypotheses relating to the framework solution, through expert evaluation and application of case studies from publicly available sources. Includes a review of the evaluation scope to comment on general applicability of the framework in relation to the original research questions.

Consideration of the philosophical position and theoretical drive (sections 3.3 and 3.4) informed the approach within each stage and the progression through the stages.

The overall approach is illustrated in Figure 5.

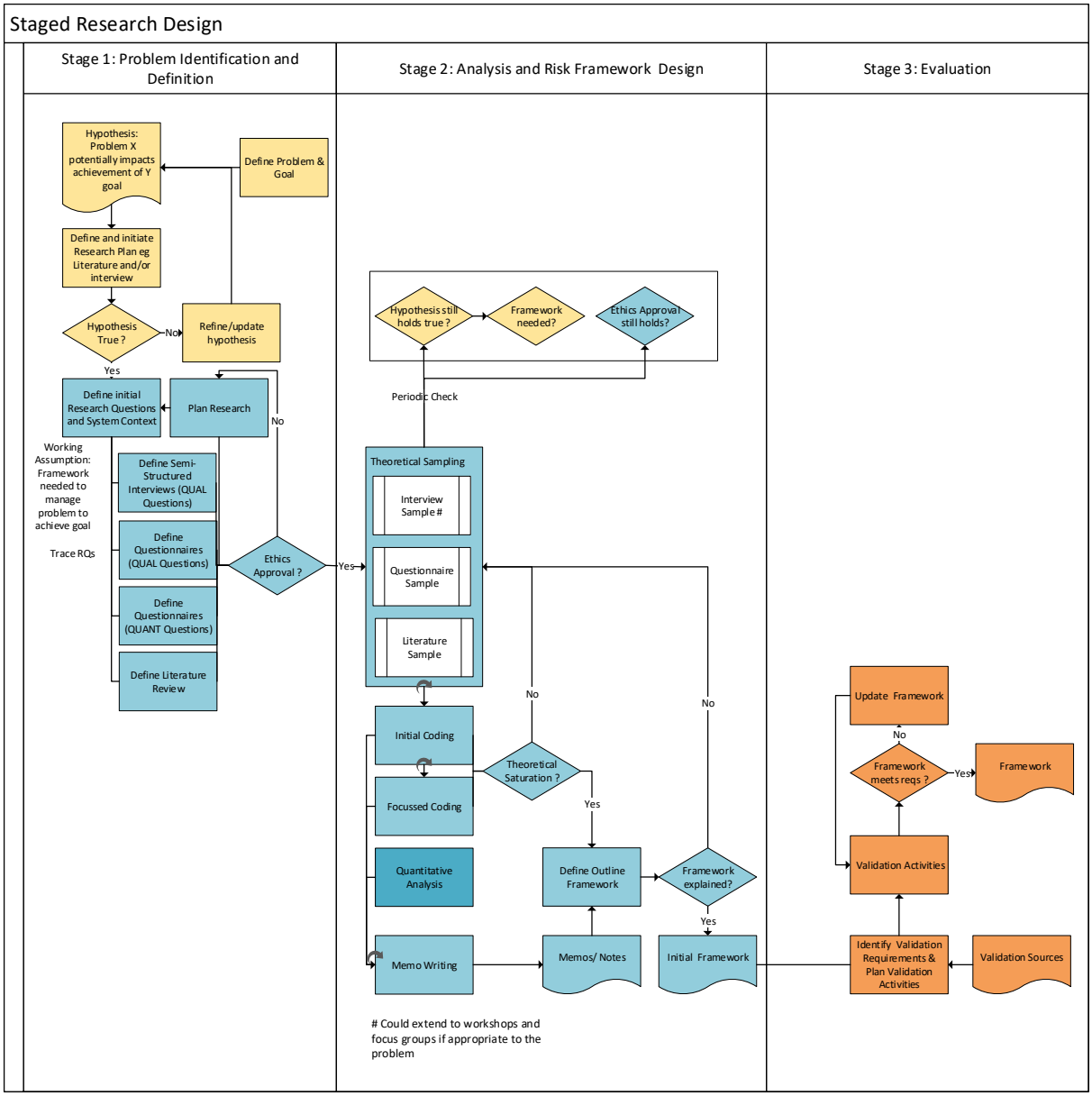


Figure 5 - Staged Research Design Adopted

Stage 1 used a targeted systematic literature review to test the initial hypothesis H1(section 2.2). Literature review (sections 2.3 to 2.5) was then used to develop the research questions and aims and enable research design for Stage 2 (section 2.5).

The Stage 2 research design considered the explorative and descriptive nature of the research questions (sections 2.5 and 3.2) and aims together with the philosophical position (section 3.3) and theoretical perspective (section 3.4). Although the overall Research Design was a complex design with sequential and concurrent elements through the Stages 1 to 3, the basis of the final research design adopted in Stage 2 was a Mixed Methods Approach: Concurrent

Embedded Design (Cresswell, 2009) dominated by qualitative analysis as the core component to explore and describe a constructed risk framework. It is evident that other systems engineering researchers were exploring qualitative approaches in systems engineering around this time too (Ramdas *et al.*, 2020). Some elements of quantitative analysis were maintained to strengthen the study, to corroborate observations, support explanation and clarify the scope.

Schoonenboom and Johnson (2017) provided further guidance on points of data integration through the results and analysis steps. The quantitative data analysis was integrated with the qualitative analysis as illustrated in Figure 6.

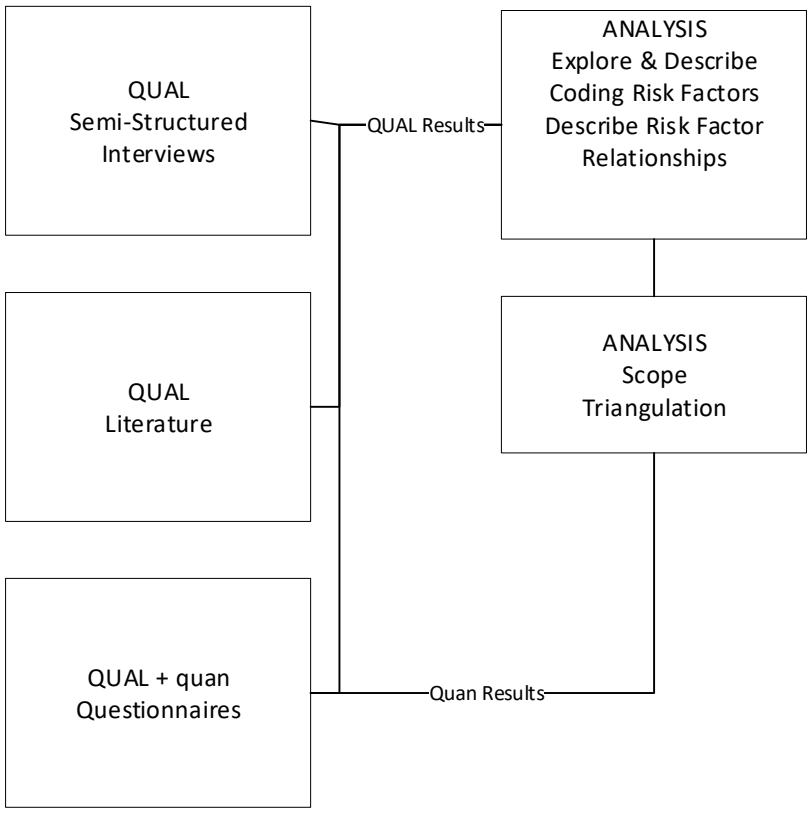


Figure 6 - Integration of qualitative and quantitative data

A Grounded Theory methodology was selected for eliciting factors from qualitative sources and revealing theory underpinning their relationships to contribute to the methods for answering Research Questions 1 and 2.

Although initially inductive to reveal factors important for the framework and the relationships between them, the approach overall is abductive with data collated and analysed

simultaneously as it is collected in a process called theoretical sampling, updating and recoding the initial factors list until no new factors are identified and the relationships between them are clarified. Data was derived from literature review (qualitative), semi-structured interviews (qualitative) and questionnaires (qualitative and quantitative) to provide a diversity of sources and to mitigate bias from any single data collection method. The interviews and questionnaires supported until no new coded factors were identified from that source and sampling of academic and professional literature became more important over time to build understanding and explanation of the relationships between them.

The collation of data continued until theoretical saturation (section 3.7) of coded factors was considered to be reached. This is when no new factors are identified and the relationships between them have been defined.

The risk framework was then documented and hypotheses stated to assert that Research Questions 1 and 2 were answered. This formed the input to Stage 3.

In Stage 3, evaluation and testing of the risk framework was carried out through a mix of expert reviews and application of cases available in the public domain.

3.6 Grounded Theory Method

According to (Sato, 2019) Grounded Theory provides a "*methodological validity to qualitative theory-building studies*" and is appropriate where little is known about a phenomenon (Tie *et al.*, 2019). By applying Polacsek *et al's.* (2018) decision flow chart, the Charmez (2014) approach was considered most appropriate as it tends to construct rather than discover theory, more in keeping with the Design Science approach, and allows flexible coding guidelines recognising the interpretive role of the researcher and participants. This was considered necessary given the infancy of Digital Twins, implemented in specific contexts and is consistent with the axiological position discussed in section 3.3. The Grounded Theory approach adopted is illustrated as follows:

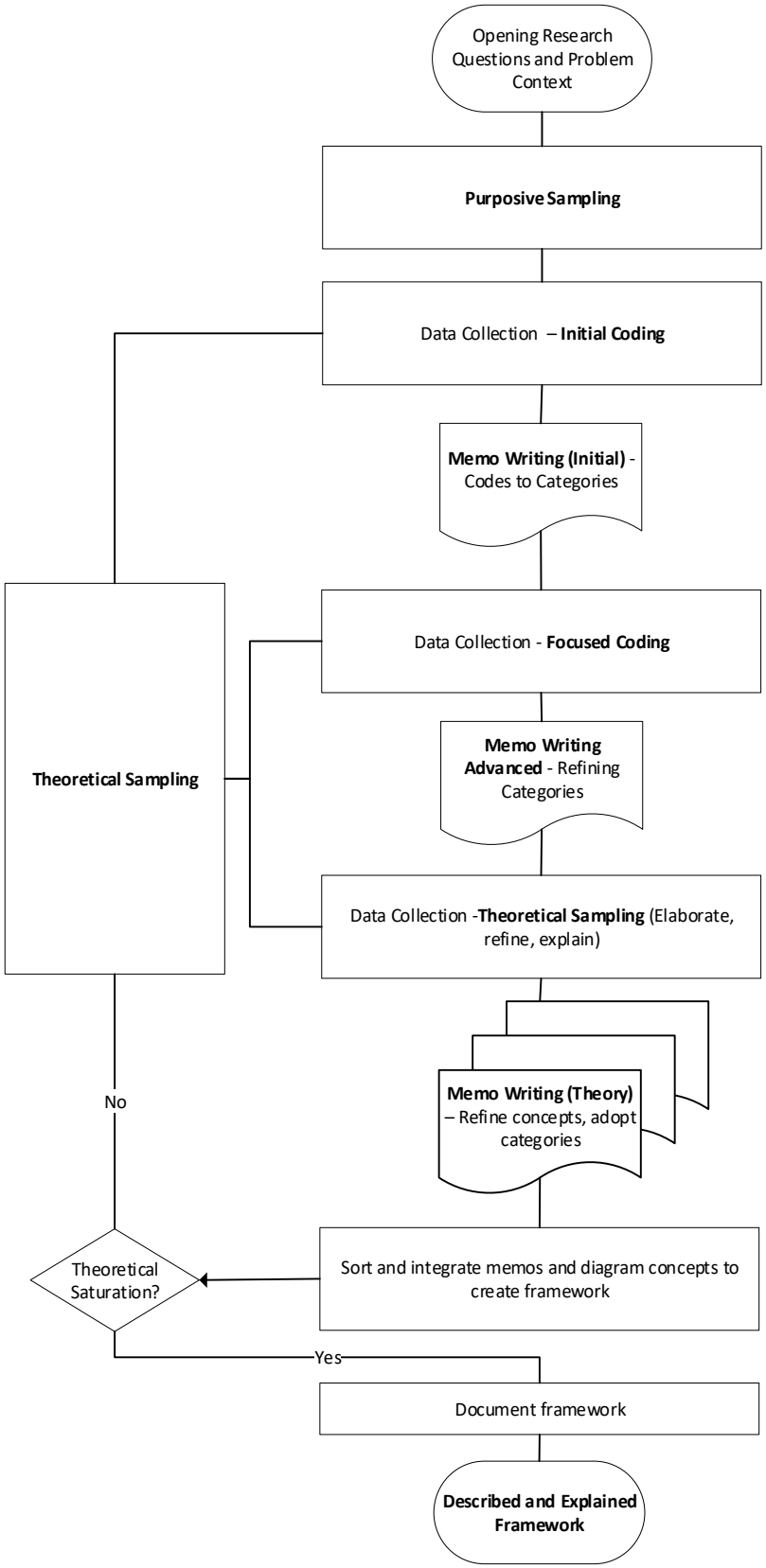


Figure 7 - Grounded Theory Approach to Qualitative Analysis Adopted by the Research Study

The aspects of the approach are summarised below with examples of implementation of each aspect in Appendix 2.

3.6.1 Sampling

An iterative and flexible sampling approach was considered appropriate for the qualitative analysis given the evolving and increasing availability of empirical data over the period of the research project. Purposive Sampling directs the initial collection of data and forms the design of initial questionnaires and semi-structured interviews and identifies the participants to be targeted. Theoretical sampling progresses from the initial codes and categories developed from the initial sampling and can be used to fill gaps, clarify uncertainties and assess interpretations as the research progresses. The main purpose is to elaborate and refine categories relating to the theory. Theoretical sampling continued until no new properties emerged. This theoretical sampling included re-examination of earlier data collected.

3.6.2 Coding

Initial Coding identifies and labels segments of text from semi-structured interview notes, qualitative question responses in questionnaires and literature that have analytic importance to the research questions. The labels for initial coding are close in description to the original text.

Focussed Coding starts with the initial codes that make the most analytic sense and tests them against a range of data.

3.6.3 Memo-Writing

Memo-writing is used to support analysis of the data and codes. Early memos record observations and predicted relationships in data in emerging categories. Advanced memos describe how the category emerges and changes and how the topic is seen from various viewpoints and makes comparisons. Clustering is used to relate codes.

3.6.4 Theoretical Saturation

Categories are saturated when gathering more data doesn't provide new theoretical insight, nor new properties. For this research study the mature categories were related back to the participant responses from interviews and questionnaires in chronological order to justify that sufficient participants had contributed and no new categories were revealing from that collection method as time progressed. Certainly this suggested that the specifics of the data collection method would not likely contribute further categories.

3.7 Quality and Rigour

Data was sourced from a mix of literature, interviews and questionnaires to ensure viewpoints from a range of business, technical and legal academics and industry managers with responsibility for digital systems and decision support and that this covered a range of manufacturers, asset owners, operators and maintainers. The final codes and categories that formed the basis of the constructed risk framework were retested against this initial dataset of interviews and questionnaires in chronological order to confirm theoretical saturation of the codes and justify that there were sufficient participants to generalise the theory. (Appendix 2 – Theoretical Saturation).

In the early stages of the research study, the basis of the research and early observations were presented at conferences to both academic and systems engineering audiences to explore reactions to the study and initial findings. (Clementson *et al.*, 2021a, Clementson *et al.,* 2021b)

Stage 3 provided further diverse checks of the constructed framework through review with further participants, from legal (practitioner and academic) and industrial asset supply and management perspectives and reflective review of application to case studies in the public domain. The number of participants at this review stage was justified through review of literature of consensus type studies which showed that although there was no set standard for sample size (Santaguida, 2018), between 3 and 80 participants is possible, depending on the application (Ogbeifun *et al.*, 2016) with a minimum of 8 suggested. In depth interviews typically of 10 to 30 participants with an aim of at least 5 interviews for each audience sub-group was recommended by Royal Academy of Engineering (nd). Each participant was shown aspects of the framework independently and asked a likert or yes/no question and then asked to explain their choice. This enabled the thinking underpinning the response to be understood and related to other participants. Application of the evaluation is discussed further in Chapter 4.

3.8 Ethics

Data collection and analysis followed ethical approval from the University of Derby, College of Science and Engineering Ethics Committee (Appendix 3). Ethical considerations included participant consent for interviews, questionnaires and related follow-up, as well as the storage and scope of use of the collated data.

3.9 Reflexivity in the Research Process

During the research process memos were reflected against the original research questions and as understanding increased literature and notes were revisited for further insight. As the questionnaires and interviews progressed there was also reflection on the scope and type of participants and range of viewpoints. The legal participants were perceived to be more aligned with their perspectives whereas the business participants had a broader perspective and more varying views of the risks, although common threads could be identified.

3.10 Summary

The research design reflects the complex socio-technical systems nature of Digital Twin Systems for decision support and the maturity of application and availability of empirical data in a rapidly evolving area. As such a structured, staged approach is justified to allow reflection at each step. Use of mixed methods with Charmez Grounded Theory to construct theory and understanding of risk factors, presented in a framework, is justified as appropriate to the research aims and questions. By involving a mix of data collection approaches and participants this is intended to provide a more complete view of risk factors, reduce bias and further provide points for reflection. A quantitative data collection was included to provide potential for triangulating findings and reflecting on scope.

Chapter 4 Research Methods

4.1 Introduction

Chapter 3 identified and justified the overall Research Design adopted to answer the Research Questions and meet the Research Aims. Chapter 4 provides details of the Research Methods adopted within the Research Design in Stages 2 and 3, in particular specifics of data; collection, sampling, analysis and integration, and evaluation. Stage 1 methods are discussed in the literature review section, Chapter 2. Ethics approval for the data collection and evaluation is documented in Appendix 3.

The specific implementation of the research methods is described in the following sections.

4.2 Data Collection

4.2.1 Data Collection Methods

The data collection methods selected for Stage 2 reflected the research design considerations discussed in section 3.2 and philosophical position discussed in section 3.3. The three methods selected were Literature, Questionnaires and Semi-Structured Interviews. The design of data collection using each method was developed to achieve objectives related to the Research Questions and Aims as well as further explore the context related to the data collection methods and, in order to minimise bias, multiple data collection methods considered similar objectives. Table 8 summarises the mapping of data collection objectives to the data collection method.

Data Collection Objective	**Mixed Methods Data Collection**
Data Collection Context: Identify the characteristics of Physical Entity life-cycle decision support use cases, application sectors and role of the data source in Physical Entity management for confirming the research study scope and potentially exploring the context sensitivity in RQ1 and 2.	Questionnaires Interviews Literature
Data Collection Context: Identify the perceived maturity of implementation of Digital Twins and digitised processes for Physical Entity decision support for reflecting on the quality of data relating to RQ1 and 2.	Questionnaires Interviews Literature

Data Collection Objective	Mixed Methods Data Collection
Explore the challenges, risks and barriers to Physical Entity management to inform identification of the legal, technical and business factors that are important for exploring and describing the relationship between IP and multi-stakeholder collaboration risk in life-cycle Physical Entity decision support using digital systems such as Digital Twins (RQ1) and the relationship between them (RQ2).	Questionnaires Interviews Literature
Explore existing frameworks, standards and industry practices used for managing risks to assess their coverage of IP related risk management. (RQ2, Aim 1)	Questionnaires Interviews Literature
Identify industry cases for using the constructed framework. (Aim 2)	Literature

Table 8: Stage 2 Mixed Methods Data Collection Related to Data Collection Objectives

4.2.2 Data Collection Questionnaire

The initial Purposive Literature review was used to design an online questionnaire (Appendix 4) that was sent to participants through a link in an email. The questionnaire provided an introductory explanation of the research purpose, which was to understand perceptions of risk, the nature of these risks and how they were impacting on the take-up of opportunities for managing Physical Entities in a digital context, including using Digital Twin applications. The scope included similar questions relating to each of Physical Entity management, in a digital context, described as Asset Management, and more specifically Digital Twin, to explore if there were similarities or differences that could provide insight on the maturity with Digital Twin applications. The questionnaire also included questions to add to and reflect on the context objectives that were part of the literature review in Stage 1. The questionnaire was divided into the following seven sections with justification as identified below:

Section	Title	Justification
1	Consent	Consent for responses to be used as described, consent for follow-up and related contact details.
2	Industry Sectors and involvement in Asset Management	Questions 4 to 8 collated data about the sector, type of assets their organisation has responsibility for, asset lifecycle management stages of their organisation's focus and the timeframe over which the asset is in their responsibility. This information was to support observing any differences in perceptions of risk based on asset involvement.
3	Processes used in Asset Management	Questions 9 to 12 included questions to explore perceptions of the maturity of digital processes and techniques adopted within the organisation, digital asset management use cases of importance and their benefits. This information was to support observing any differences in perceptions of risk based on digital maturity.
4	Challenges, Risks and Barriers	Questions 13 to 15 explored challenges and risks to effective adoption of digitised asset management solutions. There were a mix of qualitative and quantitative questions, with the quantitative questions seeking relative importance of challenges. Within the list there were legal risks, data gathering risks to relate to risk culture and skills. This section both explored

Section	Title	Justification
		the perceived significance of legal risks relative to other business risks while allowing the respondent to provide commentary on challenges and barriers of particular concern.
5	Digital Twin	Questions 16 to 20 explored the maturity of the adoption of Digital Twin in the participant sectors and organisations before asking about risks of concern and how these risks are managed by existing frameworks. These questions were qualitative.
6	Managing Risk with Digital Twin Adoption	Questions 21 to 24 explored existing approaches for managing risks and perceptions of their applicability to Digital Twin.
7	Information About Your Organisation	Questions 25 to 27 captured more specific information about an organisation which provided the potential for comparison between respondents from similar organisations and within a supply chain.

Table 9: Initial Questionnaire

As the questionnaires were designed at an early stage of the Research Design they were framed to elicit perceptions of legal risk to Digital Twin collaboration without putting IP risks specifically in the mind of the participant. This was to ensure that if IP issues were identified and discussed by the participant that they had not been led by the questionnaire. It also enabled further review and reflection of the initial hypothesis, H1, that IP issues potentially impact collaboration and how these issues relate to other barriers to Digital Twin adoption.

4.2.3 Data Collection Semi-Structured Interviews

The Semi-Structured Interviews were designed to elicit details about the sector structure, example Digital Twin use cases of importance and the context of the risk and legislative

frameworks already in place in the sector. They also elicited views about the perception of risk and priorities associated with Digital Twin adoption and whether there had been any legal challenges associated with implementation and use of digital technologies. There were broad guiding questions to facilitate the interview (Appendix 4), one of which sought if the participants had concerns about legal risks such as IP, security or contractual issues such as data sharing and protection and whether the organisation had been exposed to such risks. The interviews therefore provided the potential example of IP and data sharing issues to enable further discussion on this topic if relevant. This is in contrast to the questionnaires which were less likely to suggest a particular risk to the participant.

4.2.4 Data Collection Literature

Initial purposive literature identified in Stage 1 provided input to the Grounded Theory process design for coding factors relevant to Intellectual Property risks and management of those risks. During the Theoretical Sampling stage the literature review search terms were refined as discussed in section 4.3.1. As part of this stage the University of Derby library database was used rather than a specific database and terms were initially sought in any field and the titles and abstracts then reviewed for relevant focus. For the identification of cases for evaluation, in particular, the Internet was used to search more broadly for business and media literature sources.

4.3 Sampling Strategy

4.3.1 Literature

Purposive Sampling during Stage 1 which directed the research design and formed the design of initial questionnaires and semi-structured interviews and identification of the initial participants to be targeted is described in Chapter 2. Theoretical sampling progressed from the initial codes and categories developed and was mainly used to fill gaps, clarifications and to explore interpretations of relationships between codes and categories as the research progressed. The main purpose was to elaborate and refine the categories relating to the theory. Theoretical sampling was continued until no new properties for the framework emerged.

4.3.2 Participants

For the initial data collection using questionnaires and interviews, sector industry organisations were approached to assist advertise enrolment of participants to their members who represented the range of companies involved in Physical Entity decision support,

specifically the Rail Forum UK and Institution of Gas Engineers (IGEM). There were not as many volunteer participants as intended and so direct contact to Physical Entity owner, maintenance and operation businesses was required to secure participants. The semi-structured interviews were carried out between May 2020 and February 2021. The questionnaire was available between May 2020 and April 2022.

Overall, there were 19 respondents to the initial questionnaire and 6 semi-structured interviews providing 25 data-sets for the initial qualitative assessment before literature was used to fill gaps and provide explanation.

All 25 participants identified as representing the 'Rail, airline and pipeline transportation' sector with one participant from the questionnaires additionally self-identifying as representing the 'Electric power and transmission' sector. They represented a range of organisations from large organisations with ownership and life-cycle responsibility for assets over several decades to smaller organisations predominantly involved in an aspect of the Physical Entity life-cycle such as operation or maintenance. The Physical Entities were in the respondent organisation's care for a range of time, 52.6% under 10 years and 47.4% over 10 years which included 15.7% where the Physical Entity was in the organisation's care for more than 30 years.

There were sixteen unique organisations represented by the questionnaire respondents. This demonstrated good representation from both large companies (62.5%) and SMEs (37.5%). The interviews were predominantly large organisations with one SME represented.

The roles of questionnaire respondents were predominantly Directors and Senior Managers (79%) with Managers and Consultants representing the rest as illustrated in Figure 8. The semi-structured interview participants were Directors or Senior Managers with a technology capability background.

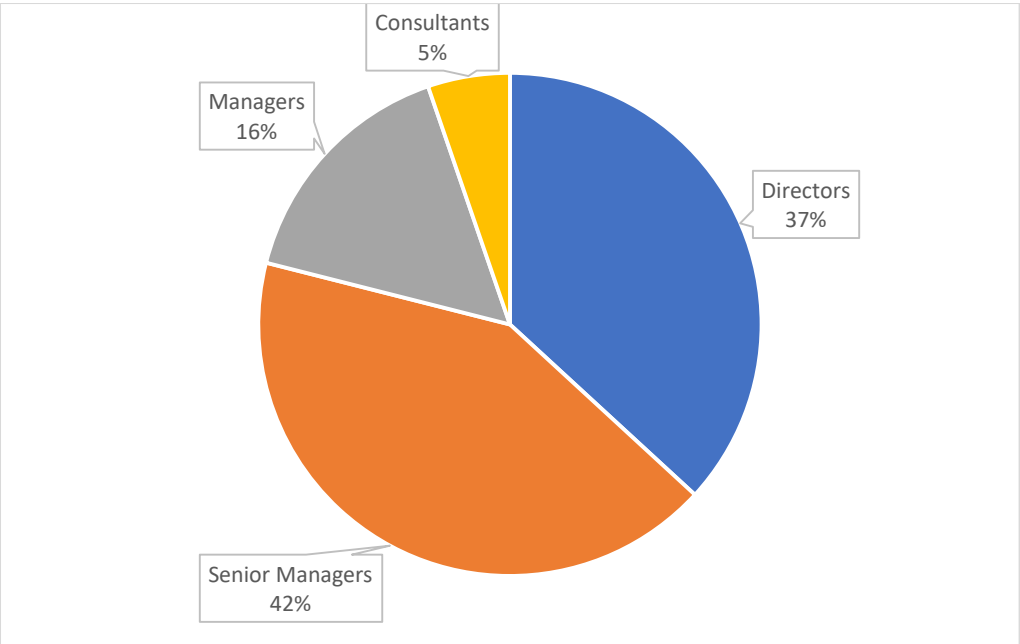


Figure 8 - Self-identified Roles of Questionnaire Participants

With all participants identifying as representing 'rail, airline and pipeline transportation' it needs to be considered that the perceptions of risk could be relevant to those sectors only and a future study could seek to explore this. Additionally, in anticipation of a larger number of questionnaire returns, there were questions within the questionnaire that sought to further differentiate participants and their organisations, such as Physical Entity characteristics and where in the Physical Entity lifecycle the organisation was focussed on managing it, however these were not taken forward into the analysis. Several participant organisations had Physical Entity management responsibility in multiple stages of the lifecycle with most involved in maintenance (84%) and a high proportion (63%) involved in design, build and operation stages.

From a rail sector perspective, the major UK Physical Entity owners of rolling stock and track were represented and a sample of international manufacturers including system integrators. Both passenger and freight operators were represented. The consultants worked across the supply chain and reflected experience across stakeholders. Overall it was considered that the participants were representative of the rail sector, and it was considered that the evaluation stage would seek to include new participants from different organisations to provide independent critical review to mitigate challenges with initial absolute participant numbers.

4.3.3 Tool Selection

Tools considered for documenting and organising codes and categories included NVivo and Microsoft Office applications, especially Excel, Word and Visio. Microsoft Office was consistently available during the study and the questionnaire output was initially exported into Excel where it was found that worksheets could be added for analysis linked to the source data. Initial literature coding was captured in tables in Microsoft Word.

4.4 Data Analysis and Integration

The qualitative data from the questionnaires and semi-structured interviews was coded as the data was collected to identify IP Risks related to digital decision support collaborations, factors that influence and manage these risks, and the relationship between them, thereby meeting the initial Stage 2 Research Objectives.

Literature was then sampled and analysed to improve understanding of the codes and over time the codes were grouped into categories and eventually a set of categories and codes that related to the Research Objectives were ascertained. This set of codes was then related back to the dataset in chronological order to confirm data saturation from the initial set of questionnaires and semi-structured interviews.

The quantitative data from the questionnaires was analysed once this saturation was confirmed and when it was clear that no more questionnaires would be easily forthcoming. This enabled reflection on scope of applicability of the findings: industry sector and nature of businesses and provided both a means to triangulate that legal issues are a concern within the context of other business concerns and to provide the potential to explore sensitivity to asset responsibility, Digital Twin application maturity, and types of risk management methodologies used.

4.5 Evaluation

4.5.1 Overall Approach to Evaluation

The construction of the risk framework in Stage 2 resulted in stated hypotheses that claimed the framework met the original Research Questions. Stage 3 used Expert Review and selected Rail Cases available in the public domain to test these hypotheses. Applying the conclusions from a secondary study relating legal issues with “big data” in transport operations to the framework was also used to further evaluate against the stated hypotheses. The relationship between these Evaluation Methods and the hypotheses are as follows:

Hypothesis	Evaluation Method Applied
H2: The described Framework explains how Intellectual Property Risks potentially impact multi-stakeholder collaboration using Digital Twins for life-cycle decision support.	Expert Review by legal experts and Intellectual Property owners and users. Applying conclusions from a secondary study relating legal issues with "big data" for managing transport operations.
H3: Application of the framework could mitigate risks to achievement of multi-stakeholder collaboration using Digital Twins for life-cycle decision support.	Expert Review by legal experts and Intellectual Property owners and users. Applying the framework to publicly available Rail Cases.

Table 9: Stage 3 Evaluation Methods Related to Test Hypotheses

Both the expert evaluation and cases focussed on the rail sector although the legal professional and academic experts did not represent a specific sector but were intellectual property specialists. The approach is described in the following sections.

4.5.2 Expert Review

The expert review involved ten participants, five of whom were legal professionals or academics and five of whom were in industry with responsibility for aspects of Physical Entity or system life-cycle decision support. Although all participants were located in the United Kingdom, over half of the participants had an international outlook based on their organisational focus, for example two European Patent Attorneys and an international legal academic and three out of the five industry participants represented internationally owned and operating suppliers. The total of ten participants, with five in each of two type groupings is within the accepted range of participant numbers for review studies as discussed in section 3.7.

A presentation format was used for presenting aspects of the framework, capturing questions about the framework and the participant responses. The questions were a mix of yes/no, likert and reasons for each response were captured as free text. The researcher presented the aspects of the framework to each participant individually. This was intended to enable each

participant's views to be explored equally to mitigate potential bias from a dominant participant in a group environment.

The process allowed for presenting an updated framework to participants if material changes needed to be made following the feedback. Given there was consensus of views from the initial review this step was not needed. Neither was it considered necessary to extend the number of participants based on the initial feedback.

The review pack is captured in Appendix 6.

4.5.3 Case Studies and Comparative Studies

The framework was applied to case studies in the public domain to evaluate the framework claims. This was achieved by relating the characteristics of the case studies to the framework categories to explore qualitative risks and compare relative risk between case studies.

Rail rolling stock was a target for the case studies as they are complex systems, with only a few manufacturers and system integrators operating within the EU, sharing a supply chain. The lifecycle stages of procurement, operation and mid-life changes tend to be relatively well documented with the operating life typically comparable between applications at around thirty to forty years. This enabled a comparative focus on differences in sector structure across jurisdictions and within a jurisdiction with a few case examples. The case studies were identified in 2022 from a search of publicly available reports on the Internet relating to European rolling stock and within the context of digitisation initiatives within the European rail industry such as DSD (Germany). This included two cases within the context of the UK with echoes of the complexities of industry structure and culture outlined in the McNulty Report, 2011 such as fragmentation, 'weak capability' of partnerships, and the subsequent implementation of its recommendations between 2011 and 2019. The case studies selected contribute to a rolling stock maintenance support purpose. Some cases were not explicitly identified as Digital Twin Systems within the case study literature but were considered relevant if there was use a Digital Twin comprising a Digital Entity for decision support relating to the Physical Entity and so two way communication, from sensors to the Digital Entity and then control action from the Digital Entity impacting the Physical Entity, even if the maturity stage used a human in the loop, such as a maintainer, to implement the control action. The three cases considered are identified in Table 11.

Ref.	Case Study	Purpose
Case 1	HVAC Maintenance-as-a-Service within upgraded Class 444/450 for South Western Railway, UK (Ebert, 2021, Rail Business UK, 2021)	Knorr-Bremse HVAC system condition monitoring (Maintenance-as-a-Service) integrated into Siemens Mobility's Railigent platform for Desiro Class 444/450 fleet maintenance optimisation.
Case 2	Class 345 trains for Crossrail (Elizabeth Line), UK (Rail Engineer, 2018)	Alstom (formerly Bombardier) Aventra Class 345 fleet maintenance optimisation.
Case3	Digitale Schiene Deutschland (part of Deutsche Bahn) Digital Twin in Germany using NVIDIA Omniverse™ Geyer,2022	Prevent incidents and detect and optimise response to operating issues using automation. This is intended to improve network efficiency, capacity and quality. Involves Stadler Digital Twin trains.

Table 11: Rolling Stock Digital Twin for Maintenance Decision Support Case Studies

The cases involved three manufacturers and system integrators, Stadler, Siemens and Bombardier (now Alstom) to ensure a range of perspectives. Case 1 and Case 2 allowed comparison of two system integrator approaches with contracts in the same geographical area. Case 1 also allowed the issue of a sub-system supplier collaborating with a system integrator to be explored. Case 3 was an application in an alternative geographical area (Germany) with a different, and simpler, rail sector structure compared to the UK.

More information was available for Case 1 compared to the other two case studies as Siemen's Railigent platform, which forms part of the case, was a case study in the Horizon Legal Issues for Big Data in Transport (LeMo) programme (Debussche *et al.*, 2018) and so provided an additional perspective with broad legal focus. As part of the evaluation, the big data legal issues identified in this report were reviewed for coverage and consideration in the constructed framework.

4.6 Summary

This chapter provided details of the implementation of the Research Design, in particular specifics of data collection sources, sampling, analysis and integration and evaluation at points within Stages 2 and 3. The different data collection methods are intended to mitigate bias and increase discoverability of the main risk factors and their relationships. Participants in both Stages 2 and the evaluation in Stage 3 were dominated by the rail sector and so the research study identifies scope of application to rail. However, generalisability was explored from a legal perspective by the legal expert evaluation participants, and the understanding of the risk categories has derived from a broad perspective, through international and cross-sector literature. Generalisability is further discussed in Chapter 8.

Chapter 5 Construction of the Risk Framework

5.1 Introduction

The Research Design (Chapters 3 and 4) was followed in Stage 2 to identify the IP risk factors to collaboration with Digital Twins and how they relate to describe and construct a risk management framework (Aim 1). The process of evolution of findings from the data collection and analysis is discussed (Section 5.2) with quantitative question observations discussed in relation to the qualitative analysis (Section 5.3). The process resulted in the framework presented in Chapter 6.

5.2 Development of Factors and Categories

Interview notes and free text responses to questions in the questionnaires were coded relating to risk factors and their relationships. Example initial codes are illustrated in Appendix 2. Similar codes were then brought together with the context of their originating text and given a reference. This formed early memos, an example of which is in Appendix 2. An early body of academic literature relating to Digital Twins was also separately coded for risk factors relating to Digital Twins. Examples of these literature coded factors are provided in Appendix 5.

The coded factors from the interviews and questionnaires were brought together with the coded factors from the initial review of a body of literature (examples in Appendix 2) and various visual diagrams of these factors were used to support analysis, bringing together similar factors and identifying the relationships between them. An example of one of these diagrams is illustrated in Figure 9 with further examples illustrated in the memo section of Appendix 2 (A2.4).

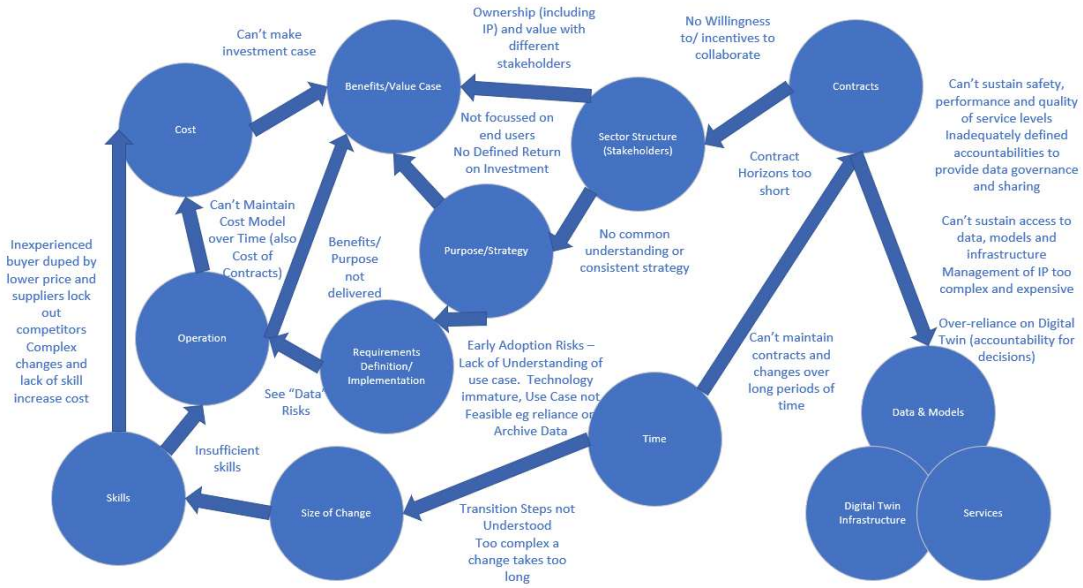


Figure 9 - An example of relating codes visually

At the end of April 2022, the set of coded factors was checked against the batches of interviews and questionnaires that had been received in chronological order to test for saturation. The saturation assessment result is summarised in Appendix 2. The batches of questionnaires were grouped in four chronological batches, to the end of 2020, literature and interviews to the end of March 2021, questionnaires to end of December 2021 and questionnaires to the end of April 2022. No new risk factors emerged from the interviews and questionnaires after March 2021. While academics such as Hennink and Kaiser, 2022 conclude that saturation could generally be achieved for 9 to 17 interviews, others such as Sim *et al.*, 2018 point out that where sampling is guided by saturation and an ongoing iterative process of interpretation, such as grounded theory, the sample size cannot be pre-determined. It was considered that no new factors would emerge from the target sector participants and literature and that the main factors of concern to the sectors had been revealed.

The quantitative questions in the questionnaire were then assessed and related to the qualitative analysis (section 5.3).

The focus of data collection was then more theoretical sampling and analysis (section 3.6.1, Appendix 2), categorising the factors into a risk framework and in understanding the relationships between risk factors. This included review of context literature (section 2.4)

such as frameworks, standards and industry practices to support presentation of the related risk factors in the constructed risk framework.

5.3 Quantitative Analysis

5.3.1 Introduction

There were 19 respondents to the questionnaires and so only simple analysis of quantitative questions was carried out for the purpose, as outlined in section 3.5, of forming a view on the scope related to participants (section 5.3.2) and to provide a means of triangulating their perspective on the relative importance of legal concerns compared to other business risks (section 5.3.4) within the perceived digital maturity context (section 5.3.3), with observations and codes from the qualitative analysis. The questions also assisted identify the type of risk management methodologies currently used and considered important (section 5.3.5).

5.3.2 Scope

Table 9 in Section 4.2.1 summarises the structure of the questionnaire. Related to scope, the mix of multi-criteria selection and yes/no questions in Questions 4-8 ascertained the types of regulated sector the respondents represented and the nature of their involvement in asset management. Question 26 further clarified whether they worked for an SME or larger organisation and Question 28 captured their role within the organisation.

All respondents identified as representing the 'rail, airline and pipeline transportation' sector, and so this was considered the sector scope for perceptions of risk and issues given that there were no respondents selecting other sectors, to include oil, gas and water. Only one respondent additionally selected 'electric power and transmission'.

SMEs and non-SMEs were considered to be broadly equally represented: 9 SMEs and 10 non-SMEs. The respondents identified as Directors, Senior Managers and Managers with one Consultant identifying 'Other' as opposed to Engineer or Technician for which there were no respondents. As such the views are considered to generally represent Senior Management and Leadership.

Excluding all consultants, of those self-identifying as having direct responsibility for assets for part of their life, 64% were responsible for vehicles and subsystems and 45% for linear infrastructure. Design, build, manufacture, and use, operation and maintenance represented the main asset lifecycle stages where respondents were involved. The assets were only identified as being in the care of respondent organisations for over 20 years in 32% of cases.

By aggregating the categories into under 10 years and 10 and over years, there were 53% in the shorter timeframe and 47% in the longer timeframe. It is concluded that there is representation for a broad range of asset care periodicity, lifecycle stage and system types within the represented sector. However, it is also concluded that there is insufficient data to look at how these characteristics influence relative responses to questions on risk perception.

5.3.3 Perceived Digital Maturity

Question 9 explored respondents' perception of the maturity of digital systems within the representative organisations. There were five levels of maturity for respondents to select against each Physical Entity lifecycle management stage and overall lifecycle management and an option to identify 'not applicable' if they couldn't respond. For analysis, the levels were coded as integers 0 to 4. The mean was between 1.86 and 2.23 across the stages suggesting perceived maturity was at a 'Pilots and Trials' stage rather than 'widespread digital processes with some gaps' (coded as 3). However the standard deviations were also high, between 1.0 and 1.3. Looking at the individual datasets there were 7 respondents who scored an average of 3 or more across categories of which 4 were large organisations and 3 SMEs. There were 4 respondents who scored a mix of the two lowest categories, 0 ('Manual and Paper Processes') or 1 (Partial Digital) for all stages. Three of these respondents were notably from companies relating to rail freight operations as opposed to rail infrastructure, passenger operations or the manufacturing supply chain.

Question 11 further explored the perceived degree to which organisations were adopting Industry 4.0 technologies to support effective asset management. For this, "Not adopting and no clear need" was coded as 0 with "not adopting and missing opportunities (not OK)" as -1 and "Adopting" to varying degrees coded 1 to 3 where 3 was "Adopting and Industry Leader". There was more variation in the perceived adoption of some technologies compared to others with the mean for adoption of 'Virtual/Augmented/Immersive Reality' given the lowest mean of 0.05 with the highest mean of 1.3, indicative of perceived most adopted technologies, for 'Cloud Computing' and 'Data Analytics'. This compared with a mean score of 0.1 for 'Digital Twin' and 0.6 for 'Cyber-Physical Systems'. Respondents were able to not provide a response if they felt they were unable to score a technology. The highest number of respondents not providing a response in a category was 3 for Cyber-Physical Systems. The distribution of responses across technologies is illustrated in Figure 10:

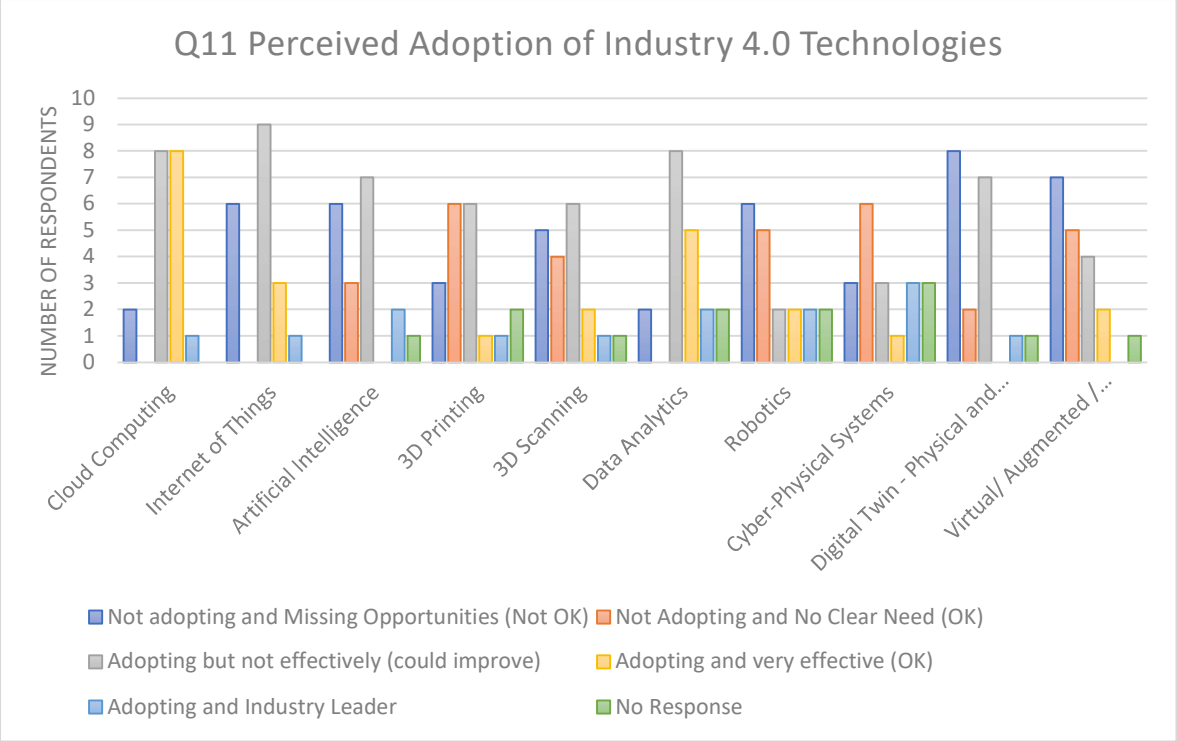


Figure 10 - Perceptions of Adoption of Digital Technologies including Digital Twin

The mix of views across Questions 9 and 11 is indicative of a mixed perception of digital maturity within the represented organisations. However, taken together with 8 respondents perceiving that Digital Twin was 'Not Adopting and Missing Opportunities (Not OK)' and a further 7 suggesting they were 'Adopting but not Effectively' this suggests a perception of basic, low level adoption and maturity of Digital Twins (79% of respondents) specifically.

The extent of adoption of Digital Twin was further explored through Question 16 which sought perception of the level of adoption with 5 options from Basic Adoption with connected physical and digital assets connected through real-time data e.g. from sensors, through to Using Predictive Analytics to Influence Decisions in the representative sectors. There was an option for the respondent to select if none of the presented options applied. Selection of this option required an explanatory comment. Only one respondent (5%) selected this stating that adoption was very limited at this time. All the others indicated a degree of adoption with the highest proportion of respondents indicating the lowest category of basic adoption (63%) for their sector.

Relating perceptions of sector adoption (Question 16) with organisation adoption (Question 11), low perception of Digital Twin maturity was evident in both questions. Basic, low level

or no adoption: 15 (79%) for organisation increasing to 17 (89%) if 'not adopting and no clear need' included, compared to 12 (63%) for sector (basic adoption). Although the results suggest that participants perceived their organisations were less mature than their sectors the questions were posed slightly differently and so are not directly comparable.

Overall perceived digital maturity was considered low at the time of the survey with a perception of further potential opportunities and increasing maturity in the future, potentially driving change. This context for the exploration of risk factors may suggest that participant experience of risk factors may be based more on perception of risk based on past experiences of technology changes and early experience with Digital Twin rather than mature, actual experience with Digital Twins for decision support. However, all respondents were involved in Physical Entity decision support with influence of adopted solutions and so their perceptions were an important view of the current situation.

5.3.4 Challenges, Risks and Barriers

Question 14 provided a list of potential challenges to adoption of digital asset management solutions and asked respondents to select either that this wasn't a concern at present, they didn't know whether it was a concern, or that they believed it to be a current challenge, ranked as moderate, significant or most important. The intent of this question was to explore whether legislative issues, to include IP, were perceived to be challenges and potential barriers at all within the context of a broad list of business challenges and to relate the observations to the qualitative question responses. Initially all responses indicating concern with a potential challenge (sum of moderate, significant or most important) were compared to responses suggesting no challenge or that they didn't know whether it was a challenge or not.

Over 90% of respondents identified concern over the following challenges:

- Organisation Structure
- Culture e.g. Risk Averse or not digitally aware
- Size of the required organisational change
- Limited Resources
- Lack of Digital Skills
- Inadequate knowledge management as a starting point

Over 80% of respondents identified concern for legal and ethical issues, of which IP was a part, expressed as:

- Lack of understanding of exposure to legal risks and consequences (Cloud/IoT, security, data protection, data access, Intellectual Property, Contracts with multiple stakeholders, AI decision responsibility) (84%)
- Ethics e.g. extent of data gathering, monitoring and control (84%)
- Demonstrating compliance with relevant legislation and regulations (89%)

Uncertainty in implemented legal protections from careless or malicious activity was only considered to be a concern by 68% of respondents with 3 stating it wasn't a concern and 3 stating that they didn't know. Out of step regulation and standards and lack of current technical solutions were also concerns for over 70% of respondents although three respondents in each case, conversely, didn't think it was a concern. The remaining challenge was industry sector structure which while considered a concern by 79% of respondents, had the greatest number of respondents at 4, selecting that they didn't know whether it was a concern or not.

Overall this was considered to confirm that concern over exposure to legal risks, including IP risk, is of concern as a potential risk and barrier, as there was not a strong response to suggest it wasn't a concern but, as anticipated, such concerns are within a context of other significant business concerns. As such it was reflected that respondents may find it challenging to isolate concerns for IP or other legal risks from the broader concern context when responding to qualitative questions and that it may be important to reflect on the inter-relationship between IP and other business concerns.

Question 23 asked if respondents were aware of any legal activity with IP infringement or data security breaches. All answered that they weren't which, given the seniority of the participants within their organisations, suggested there hadn't been any high profile incidents in these sectors at this time. It was not clear whether this was due to the early stages of implementation where legal incidents are yet to emerge. This did identify a need to search for legal incidents more widely in literature, which revealed commentary on issues such as risks from data analytics service providers exploiting data (Druetta, 2018), and service risks from with-holding data share (Yaqing, 2017). Novarty (2021) commented on the

misappropriation of IP in supply chains and the potential consequences and provided an example of a single IP theft costing a company over $3.2billion.

5.3.5 Managing Risks

Question 21 asked respondents to identify the approaches they use to manage risks associated with Digital Twin applications. The permitted responses were Yes, No and Not Applicable.

For each of the approaches presented there were between 2 (11%) and 4 (21%) of respondents who identified the approach was not used. Each suggested approach was widely used with each claimed to be used by between 10 (53%) and 14 (74%) of respondents. Contracts with stakeholders for data access/use/sharing and IP was identified by the highest proportion of respondents 14 (74%) with Standards Compliance and Risk Management Tools each identified by 13 (68%).

Two respondents suggested all identified approaches were not applicable. When these two responses were related to the qualitative Question 22, which sought views on gaps in guidance and methodologies, it was revealed that one respondent felt they did not have adequate knowledge to answer the question and another suggested that approaches would develop slowly over time as they have done with safety critical systems and in the aviation sector.

This question in isolation did not provide further insight to the qualitative analysis but did indicate that a range of approaches to risk management may be appropriate and accepted by respondents.

5.3.6 Quantitative Analysis Summary

The analysis of data from the quantitative questions in the questionnaire concluded the following:

- **Scope** – All questionnaire participants represented the rail, airline, and linear infrastructure sectors.
- **Relative Importance of Legal Concerns** - Concern for legal risks with Digital Twin use in the context of other significant business risks relating to change and the adoption of new digital technologies for decision support. This supports the identification of factors grounded in the qualitative analysis which relate IP risk with broader, business issues.

- **Perceived Digital Maturity** – Support for qualitative and early literature review perspectives that Digital Twin adoption is not yet mature particularly through a diversity of views of Digital Twin and Industry 4.0 technology adoption and a mix of views on the applicability of current risk management methodologies to Digital Twins.

5.4 Summary

Within the context of the rail, airline, and linear infrastructure sector participants and broader industrial contexts from literature the factors relating IP risk to collaboration with Digital Twins were derived and the relationship between them explored through implementation of the research design to construct a risk framework.

It was evident the relationships between IP and collaboration risk needed to be related to a broad range of business risks identified through analysis of the data as a perceived risk to collaboration. The relatively low maturity of experience with Digital Twins, given the temporal presence of the digitisation revolution, was evident from both literature and participant experience with perceptions and current experience informing the construction of the factors and their relationships within the framework. However, several common factors and relationships were identified through the data sources and literature assisted in filling gaps to understand these relationships in relation to IP risk to collaboration.

Chapter 6 Described Risk Framework

6.1 Introduction

The construction of the risk framework resulted in categories and factors which relate to enable understanding of how IP can influence the risk to multi-stakeholder collaboration using Digital Twins for decision support through the life-cycle of a physical system. The constructed risk framework is described in section 6.2. The theory of relationships between categories and factors is described in section 6.3. The framework is then related to existing risk management standards to identify whether there is new understanding not currently reflected in the existing standards. This is described in section 6.4. Application of the risk framework is discussed in section 6.5.

6.2 Described Framework, Factors and Categories

6.2.1 Overview of the Framework

The presentation of the specific factors of the IP risk framework required a visual frame. The starting point was the standards for risk management, such as the BS ISO 31000:2018 series (British Standards Institution, 2018) which represent a mature structure to apply. Risk management in these standards comprises iterative stages of identification of risk to achieve a purpose, analysis and evaluation of risks for tolerability, declaration of mitigating requirements and solutions, and assignment and implementation of stakeholder obligations. There is then an underpinning continuous risk monitoring and review cycle. BS ISO 44001:2017+A1:2024 (British Standards Institution, 2024b) provides more context for collaboration risk considerations. Within this risk management process frame there was a need to present the specifics of IP risks to collaboration. For an overview of the framework a bow-tie diagram (Ministry of Defence and Military Aviation Authority, 2018) was found to facilitate visually illustrating the flow from a Cause through, Escalators and Barriers to a Top Event in the presence of a Hazard, and then from this Top Event through Escalators and Barriers to a final Consequence.

When considering IP risk (harm or loss) to collaboration when using Digital Twin based decision support systems there is a Hazard if the Digital Twin System utilises valued IP which could potentially be infringed (Top Event), such as used without the IP Owner's permission or beyond the limitations of any granted licence. Such an infringement could result in a dispute between the IP owner and the stakeholder that committed the infringement. The stakeholders will seek to resolve the dispute, but this could impact the collaboration with

a potential consequence of failure of the Digital Twin System purpose, such as ability to deliver decision support services to the required performance. There could also be financial consequences in legal resolutions such as legal costs and damages and from any temporary or permanent impact on services. Trust between the disputing collaborators could also be impacted which could lead to damaged reputations which in turn could lead to a financial loss consequence.

There are several causes of infringement, and such could originate from accidental, negligent or deliberate intent. The framework identifies factors that could increase risk of infringement, such as ambiguity over ownership or ease with which protected IP can be accessed in digital form and these causes relate to the complexity of the systems, and clarity of the applicable law. Digital Twin Systems generate data that relates to the Physical Entity and its use. While some data may originate from a generic sensor such as a temperature sensor, other data may originate from a bespoke sensing system that has been designed and developed to provide the specific information required for a decision support purpose that is of particular interest to the Physical Entity designer to develop future products, but is also of interest to the user of the Physical Entity who may want to engage a third party to develop tools for predicting when maintenance should be due from the data. Literature has already identified potential IP infringement risk from third party AI developers (Druetta, 2018). IP law seeks to balance incentives for innovation with social benefits and public interest (World Intellectual Property Organisation, 2010) but while it builds application experience with Digital Twin Systems, sector governance approaches may develop to mitigate some causes and consequences.

An example Hazard related to IP and Digital Twin was “Valued IP or proprietary data essential for achieving the purpose of Predictive Maintenance using Digital Twin.” The Hazard could result in a Top Event such as “IP Infringement” or “Data Exploitation” or “Trade Secret Leakage”. Consequences could then be “Failure of Purpose”, “Reputation Loss”, “Financial/Business Case Failure”, all of which adversely impact collaboration to achieve a purpose using Digital Twins. Example Causes leading to the Top Event, revealed through the analysis of collated data, particularly the participant perceptions of risk, included “Owner of Proprietary Data Perceived Unacceptable Risk of Data Breach”, or “Proprietary Data Value Mismatch between Data Owner and Beneficiary of Digital Twin Service delivering the Purpose.”

The coded IP risk factors could then be related as an Input to the risk assessment comprising Goals, Context and Viewpoint; a Risk Influencer, either on the cause or consequence side of the bow-tie or both sides; or a Risk Mitigation Tool that could reduce the risk or consequences. The resulting risk framework is illustrated in Figure 11.

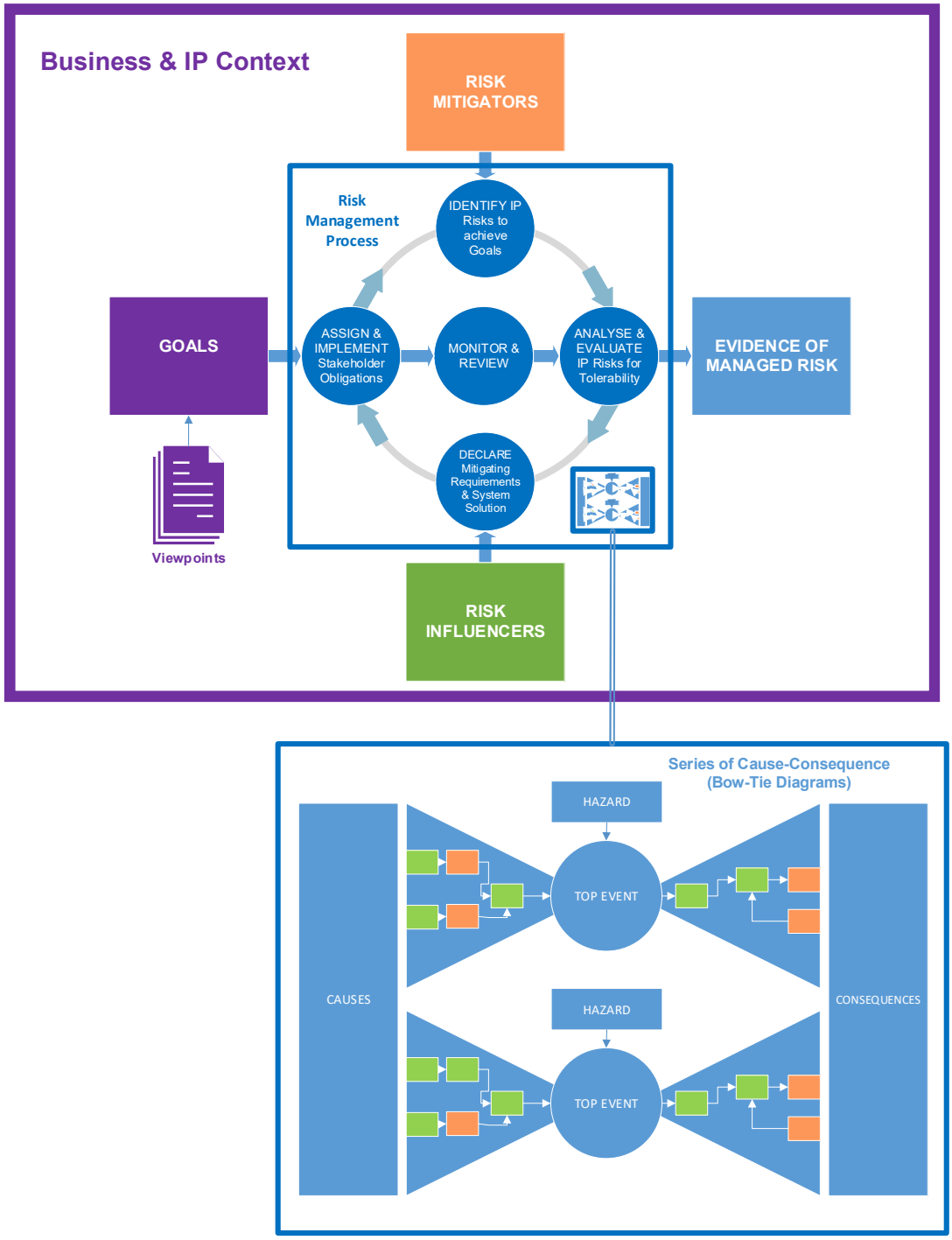


Figure 11 - Overview of the IP Risk Framework for Collaboration Using Digital Twins for Decision Support

6.2.2 Categories, Sub-Categories and Factors

The coded IP risk factors were consolidated and grouped into the following Categories and Sub-Categories:

Category	**Sub-Category**	**Factor**
Goals & Context	Goals	Digital Twin Purpose, Need, Requirements Value/Business Case Tolerable Risk
	IP Context	IP Inventory (Owned & Used) Existing IP Protection & Licensing Policies Legal, Financial & Insurance Stakeholders
	Business Context	Enabling Technology, Tools and Systems Application Sector(s) Geographic Scope
	Viewpoint	Lifecycle Stage(s) Contract(s) Stakeholder(s)
Risk Influencers	Maturity	Governance, Culture and Leadership Policy, Strategy and Management Trust, Competency and Capabilities
	Clarity	Accountabilities and Obligations Standards and Legal Environment

Category	Sub-Category	Factor
		Traceability (Value Case to System & Contracts)
	Complexity	System Complexity Stakeholders Map of IP Owners, Users and Governance Structure and Incentives
	Longevity	Life-Cycle Stage Contract Term Timeframe Entity Life Timeframe
Risk Mitigators	Legal	Model Contracts & Insurance IP Protection & Licence Model Regulatory Sandbox/Framework
	Technical	IP Tracking & Cyber Security Controls Systems Methodology (was MBSE prior to evaluation) Generic System Architecture & Interfaces
	Business	Defined Training & Qualifications Defined Stakeholder Types & Roles Generic Risk & Mitigation Options
	Governance & Policy	Generic Governance & Assurance Model Sector Audit and Accreditation Schemes Policies & Standards

Table 12: IP Risk Framework Categories, Sub-Categories and Factors

6.2.3 Goals & Context

The Goal sub-category together with the Viewpoint sub-category identifies the main inputs to the risk management process.

The Goal is to deliver the Purpose of the collaboration using Digital Twins, consistently with the Business Case which assumes a Tolerable Risk for IP risk. For example, if the Purpose is optimised maintenance of a fleet of vehicles, there will be an associated Business Case for the fleet maintenance which considers the costs of implementing and managing the maintenance service, including all costs to third parties for tools and services associated with the Digital Twin System, such as data management and algorithm development, sensor maintenance and costs and benefits associated with protection of any IP with costs for related insurance against business risk, including defending IP breaches. The Business Case benefits will relate to assumptions about the performance requirements to achieve the Purpose. These together then relate to the Tolerable Risk for IP risk to collaboration. The definition of the 'Digital Twin Purpose, Need, Requirements' can be related to the scope of the Concept Definition of BS ISO/IEC/IEEE 15288:2023 (British Standards Institute, 2023c) which includes Business Analysis and Stakeholder Needs and Requirements and traces to a Systems Definition, to include the System Architecture, and System Realisation, Deployment and Use (Figure 5 BS ISO/IEC/IEEE 15288:2023 (British Standards Institute, 2023c)).

The Goals can then be considered from a particular Viewpoint.

This Viewpoint could be the perspective of a particular Stakeholder, such as a manufacturer of the Physical Entity or user of the Digital Twin Services or a Regulator representing an outcome for Social Benefit, or it could be considered from the perspective of a Contract between stakeholders in relation to the Goal Purpose. The Viewpoint of Life-Cycle Stage allows the different Goals to be applied for different Physical Entity life-cycle stages. For example, the value of a Physical Entity IP may be different to a particular Stakeholder in the early stage of a Physical Entity's operation than when it is at mid-life or end of life. This is illustrated through the following participant response of an asset owner relating to sharing data for a maintenance application: "*There can be reluctance by OEMs to share design information due to the perceived level of commercial interest and potential future competition. It is more likely to share for older assets depending on the perceived commercial risk for the stakeholders involved*." There is potential to layer Viewpoints, for example specific Stakeholders, then Sectors then End Users/Society.

The Business Context and IP Context Sub-Categories provide the risk context for informing the risk analysis.

The IP and Business Contexts relate to each other, for example the IP Inventory (Owned and Used) will relate to the Enabling Technology, Tools & Systems used to achieve the Goal-Purpose. Existing IP Protection and Licensing Policies may impact the level of protection that is in place and this in turn should link to the ability to achieve the Goals, Business Case and Tolerable Risk. The specifics of the geographic scope of the Digital Twin infrastructure and services will inform the legislation that applies relating to the existing IP protection and licensing policies and how these are enforced as although WIPO seeks to administer an international framework of IP and facilitate international protection (World Intellectual Property Organisation, 2010) there are differences in laws and their implementation across the world. For example, although there is broad international copyright protection of original arrangement of data in databases in copyright, the sui generis database rights, that protect substantial investment in obtaining, verifying and presenting the content of a database, are unique to the EU through 'Council Directive 96/9/EC' (1996).

The context of Application Sectors, such as aerospace or healthcare will inform the policies, supply chain structures and specifics of risk and governance that apply.

Changes to Goal and Context may occur during the lifecycle and so should require a re-evaluation of risk as part of ongoing risk management.

Hypothesis: The Goals & Context sub-categories and factors provide the inputs to assess Intellectual Property risk to collaboration with Digital Twins.

6.2.4 IP Risk Influencers

The IP Risk Influencers identified have the potential to escalate progression from the Cause to a Top Event or from the Top Event to the Consequences. They exhibit characteristics that can be relatively riskier or less risky to the collaboration in specific contexts.

The IP Risk Influencers have been grouped into four sub-categories, each of which has factors potentially capable of illustrating relative risk such as high, medium or low, for example 'High Complexity Risk Influence' or 'Low Complexity Risk Influence'. Whether these risk influencers are perceived to be of concern for a particular 'Goal & Context – Viewpoint' will depend on application of the risk framework. The 'Goal & Context' will

also identify whether the risk environment is within (internal) or outside (external) control of the Viewpoint of a particular stakeholder or group of stakeholders. Where the external environment risk influence is particularly high, it may be challenging for individual stakeholders to manage their overall risk.

A summary description of the IP Risk Influencer sub-categories and factors are provided in Table 13.

IP Risk Influencer: Maturity
Description
A business and management environment that is mature in consideration and understanding of the specifics of managing IP risks to collaboration with Digital Twins for decision support is expected to be lower risk than one that is not. Risk Maturity Models in various contexts, for example Hoseini *et al.*, 2021(construction projects), Yeo and Ren (2009), (complex product systems) identify common categories for framing assessment of maturity risk and this provides the basis for exploring and describing maturity in relation to IP risks to collaboration. Such models also support definition of levels of maturity from low to high, such as from undocumented, ad-hoc risk management to documented, optimised risk management. The presence and characteristics of an IP Policy in the context of such decision support collaboration is considered to underpin the understanding of Maturity. A high Maturity IP Policy focusses on balancing reward for innovation and investment, with the interests of the wider collaborative Purpose, while avoiding and discouraging improper competitive activities which threaten both Purpose and innovative endeavour. Adoption of principles such as the GEMINI Principles (The Centre for Digital Built Britain, 2018) within the IP Policy, particularly for a societal Purpose, may also be indicative of higher Maturity. The implemented IP Policy should be understood across and through each collaborating stakeholder supported by indications of high Trust, Competency and Capabilities and underpinned by supporting Governance, Culture and Leadership. Trust in the technical ability of the Digital Twin to achieve its Goal & Context-Purpose is a significant issue and can be impacted by availability of appropriate data with impact particularly severe for a Safety Purpose. Such availability of data could arise from an IP

or contract dispute between stakeholders. IP risk to collaboration is therefore focussed on the Trust between employees within a stakeholder organisation and stakeholders external to the organisation involved in implementing the Digital Twin System and services. If trust is low between collaborating stakeholders there is more likely to be dispute which disrupts achievement of the Purpose. Perceived lack of trust could impact on sharing of data to deliver the Purpose and where there is poor trust there is more likely to be breach of IP licences or contract terms. This will also relate to how well supply chain management processes consider Trust with IP and data through the supply chain. Technology and system design capability will mature over time in terms of both function and ability to protect and manage IP while delivering Purpose to stakeholders. While some stakeholders can influence this risk through design choices there may be technical limitations that also impact risk which should improve over time as technologies better able to mitigate risks become available. This links to the "Longevity" risk influencer category.	
Governance, Culture and Leadership	
Example Indications of Lower Risk	• accountability for IP risk to achieve the Goal • established and implemented IP Policy • enabled Collaboration and Trust to achieve the Goal • encouraged ethical and systems thinking behaviours • identification of the right skills, knowledge and capabilities • established systems, organisational and governance structures and interfaces • clear identified roles and responsibilities • commitment to continual improvement • governance of protected and licenced IP
Internal Control Examples	• Evidence that the Leadership has implemented IP protection policies that are justified in relation to the "Goal & Context". • Leadership of IP risk management that ensures legal, technical and business controls are in place.

	• Leadership that ensures there is a governance structure for monitoring risk mitigation performance and implementing improvements. • Evidence that IP risk management processes to achieve "Goal & Context" are understood throughout the organisation. • Presence of Insurance against IP breaches and disputes. • The leadership has evaluated and assessed that the organisational structure and culture throughout it, is effective in supporting the "Goal & Context".
External Control Examples	• An implemented Sector IP Policy that balances incentive and reward for investment in innovations with Sector Purpose using Digital Twins for Decision Support. • Sector Leadership that recognises remedies for breach appropriate to each of malicious, reckless and accidental cause. • Regulatory governance structures, including audits, accreditations, licencing and training, to mitigate breaches. For example, licencing suppliers that manage others IP and data, and mandating the use of standards for technology and collaboration.
Policy, Strategy and Management	
Example Indications of Lower Risk	• clear cascade of responsibility for IP protection and management. • IP Policy, Strategy and Processes to achieve the Goal (Purpose & Business Case) • active IP risk management • implemented collaboration risk performance evaluation and improvement Evidence of mitigation of identified issues such as: "*Fragmented industry - ownership and value gained are within different organisations. OEM Build & Maintenance contracts maintain IPR within one organisation (train builder) even if they are not the train*

	owner." (Q13#5) "The short contract time horizons, misaligned incentives, multiple players, lack of consistent strategy" (Q13#3)
Internal Control Examples	Effective implementation of a management framework for managing risk based on ISO 31000:2018 (British Standards Institution, 2018) which considers IP risks to achievement of Goal & Context - Purpose.
External Control Examples	A sector relying on collaboration having policies for facilitating risk management through mandating standards and risk framework compliance and developing guidance for IP risk management.
Trust, Competency and Capabilities	
Example Indications of Lower Risk	• Defined IP, systems, collaboration and risk capabilities and knowledge required across and through collaborating organisations. • Active management of trust between internal and external stakeholders to include managing risks to the Purpose arising from related competency gaps. • Digital Twin System assessed as capable of protecting and managing IP to achieve and maintain the Purpose. • Checked validity of IP clauses. Evidence of mitigation of example issues such as: *"The sharing of data and models, and controlling who gets access to those is a big concern, along with unscrupulous players locking out competitors." (Q19#1) "The market does not fully understand the concept of Digital twins, cost of development of a twin and the related ROI" (Q19#6)*
Internal Control Examples	• An implemented, managed competency framework covering roles from legal, to technology and service management that considers the following competencies through the organisation, supporting the Physical Entity life-cycle: o **Systems thinking** – ability to see other stakeholder perspectives and link the role and value of IP used by and generated by the system to achievement of the Goal & Context-Purpose. Systems thinking should support

	effective evaluation of Digital Twin solution options and traceability. ○ **IP** – ability to ensure that the purpose and value of IP is understood through the organisation consistent with the IP Policy, to facilitate implementation of protection controls. This includes: ▪ ensuring technical and design roles understand how architecture choices (cloud/IoT, Security, Data) and geographic location of solutions impacts legal protection and remedies, and ▪ legal specialists understand Digital Twin System architectures to advise effectively. ○ **Risk Management** – supporting "Policy, Strategy & Management". This should be underpinned by breadth and depth of understanding of generic risks, system architectures in relation to the Goal & Context and related security and safety risk management frameworks. For example, Chandru and Kumar (2009) noted a need for IP Owners to be "more educated" in ways to manage IP transfer risks. ○ **Collaboration Management** – ability to recognise each stakeholder's objectives and seek to maximise their achievements as well as holding individuals to account for unacceptable behaviour. Example competencies are identified in Table C1, BS ISO 44001:2017+A1:2024 (British Standards Institution, 2024b) and include leadership, culture and governance. • Procurement processes that support confidence and trust in 3rd party services and clarify authorised architecture components.
External Control Examples	• Sector audit, incentives and guidance (Policy, Strategy and Management) to support "Governance, Culture and

	Leadership" in improving Trust for collaboration within sector Digital Twin applications.
	• Sector level competency frameworks and skills development to support collaborative partnerships and IP competency for mutual understanding. This includes:
	  ○ Defining the level of understanding of IP law purpose and application to Digital Twin solutions and services to achieve Purpose and balance stakeholders needs. This is influenced by the maturity of IP law applied to such complex socio-technical systems.
	  ○ Ensuring digital competency throughout the supply chain as Trust and Opportunism in Collaboration can be influenced by the balance and symmetry of digital competency between collaborators (Son *et al.,* 2021)

IP Risk Influencer: Clarity	
Description	
Effective management of IP risk to collaboration requires Clarity of Purpose, Digital Twin System Architecture, Stakeholder Obligations and a systematic process that links these together. If Clarity is high the overall likelihood of threats and potential escalation factors should be lower, and the effectiveness of barriers and recovery measures are likely to be higher than if Clarity is low. There is a close relationship between Maturity and Clarity. For example, if Maturity is low in the risk environment outside a particular Stakeholder's control it may be more likely that Clarity of Standards & Legal Environment will be lower and issues such as "Data Sovereignty" and "Value" less clear. The factors revealed as particularly important for IP risk management are: • Accountabilities and Obligations • Standards and Legal Environment • Traceability (Value Case to System & Contracts)	
Accountabilities and Obligations	

Example Indications of Lower Risk	Clarity indications include explicit and clear obligations for using Digital Twin Systems and services that protect know-how, trade secrets and IP and include: • Accountabilities and obligations for managing the Digital Twin models, data (ownership, collection and services during design, production and operation) and algorithms that respect the activities and endeavour involved in maintaining performance requirements and fidelity. • Obligations for storing, analysing and permitted use of the models and data. • Obligations for data security. • Data value chain and agreement of value benefit and risk ownership across all stakeholders. • Responsibilities for engaging 3rd party services. • Obligations for managing change, sale and transfer of data, models and AI rights including to third parties or to a new service provider. Such should consider: o mitigating IP and confidentiality risks such as restricting a third party's ability to use a stakeholder's proprietary data to ensure such data remains confidential and that competitor's do not benefit from it. o ensuring that any risk allocation obligations beyond express terms and conditions in the contract for sale are clear. For example, implied terms from common law and local legislation e.g. 'fitness for purpose' • Obligations for regulation and audits and accreditation of data service providers. • Obligations for use of applicable standards and architectures. • Data privacy obligations on a party gathering data must be considered. • Country/geography restrictions of use/operation

	To reduce risk the sector can clarify expected accountabilities and implement certification/licensing regimes. Linked to Trust, Competency and Capabilities the sector or government could provide clarity by creating an agency to oversee AI Regulation across national borders and set standards for AI development and use and perhaps offer certification of AI systems.
Internal Control Examples	The ownership and obligations through life-cycle changes need to be explicit in contracts to increase clarity. This is particularly important where the external legal environment is not yet mature and clear. In particular, Druetta, 2018 noted that the legal environment does not provide clarity of data ownership nor effective protections, providing the example of the EU sui generis database rights and stating that it is difficult to show a substantial investment to secure such protection. Almarri *et al.*, 2019 noted IP is a critical issue for adoption of BIM in the built environment with a survey identifying lack of clarity for BIM object ownership as a stakeholder concern.
External Control Examples	Sectors and government bodies may assist in clarification of Liabilities, Accountabilities and Obligations for collaborations underpinning Digital Twin services that are important for the Public Good (The GEMINI Principles (The Centre for Digital Built Britain, 2018) and interoperability. If levels of information access are clarified top down from government or sector bodies this will impact risk for a particular stakeholder. Sectors and governments can provide clarity where it may be challenging for individual stakeholders to resolve equitably. For example, stakeholders may place different value in data based on their involvement in the data value chain. O'Leary and Armfield (2020) noted that a stakeholder teaching the AI with data may want to acquire more secure rights than a licence in order to maintain the value of its "teaching" investment and the representative competitive advantage.
Standards and Legal Environment	

Example Indications of Lower Risk	The availability of generic application standards and legislation for mitigating IP risk to Collaboration with Digital Twins to include standard generic architectures. For example there are various functional and feature architectures for Digital Twins evolving which can form the basis for assisting with identification of the IP and ownership including a recent Standard for Digital Twin concepts and terminology, BS ISO/IEC 30173:2023, (British Standards Institution, 2023b) and a reference architecture for Digital Twins in manufacturing, BS ISO 23247-2:2021, (British Standards Institution, 2021a). This combined with systems engineering approaches can evaluate Digital Twin solution options against the Purpose to identify less complex and lower risk solutions. Reduced exposure to a range of legal jurisdictions and focus on those jurisdictions with high levels of harmonisation.
Internal Control Examples	Minimising geographic scope of the applicable legal environment through supply chain choices where possible (links to Complexity). Improving clarity by adopting available, including voluntary, standards. For example, an interviewed participant implementing Digital Twins was voluntarily adopting Collaboration Standard BS ISO 44001 (British Standards Institution, 2024b). This standard provides a risk management process for managing collaborations which includes clearly defining benefits from collaborations, determining the necessary competencies and behaviours and expectations for communication, monitoring activity and risk and disengaging from the collaboration. Stakeholder involvement in Standards development can also potentially mitigate Clarity and Complexity risk for that Stakeholder and contribute positively to the management and value of IP, provided there is external governance to control opportunism and manage competition (Lambert and Temple, 2015).
External Control Examples	Standards bodies, regulators and sector organisations identifying gaps in standards coverage and developing the Standards & Legal Environment. During the period of this research project the standards

	environment was rapidly evolving and so not yet clear. For example, ISO/IEC 30173:2023 (British Standards Institution, 2023b) – Digital Twin emerged in 2023 to provide clarity of cross-sectoral concepts and terminology and a draft standard ISO/IEC 30186 Digital Twin – Maturity Model and Guidance for a Maturity Assessment emerged in January 2024 for public consultation. So far, these emerging standards are focussed on the technical capability maturity and not business, legal and IP aspects. Sectors and Regulators can monitor Standards Development activities for balancing innovation for IP owners and maintaining Purpose for IP users, mitigating opportunism and encouraging early revealing of IP in standards development through use of FRAND Licences. (Lambert and Temple, 2015) A Sector can clarify: "Data Sovereignty", levels of access and key "Data Ownership" in standards and guidance notes and define "Data Categories" and "Standard Architectures". As the legal environment can vary across the world, risk for stakeholders based within a country can be mitigated if the country standards body is active in driving Digital Twin stakeholder needs through International Standards bodies. Regulators and policy makers need to consider the legislative environment for data sharing and ownership and reduce any asymmetric advantages for larger companies. Legislative experiments and legal sandboxes can provide cautious "wait and see" approach to new scenarios before formalising new legislation. (Gromova *et al.*, 2022) This would avoid premature rulings that may entrench a monopoly control of data by a stakeholder, and those that discourage market competition and growth of new market participants.

	Clarity of Risk Management would be improved through adoption of standards such as: • BS ISO 31000:2018 *Risk Management –Guidelines* (British Standards Institution, 2018) • BS ISO/IEC/IEEE 16085:2021 *Systems and software engineering (*British Standards Institution, 2021b*)* Linking to the next factor "Traceability", lower Clarity risk can be indicated through evidence of adoption of systems standards such as BS ISO/IEC/IEEE 15288:2023 (British Standards Institution, 2023c).
Traceability (Value Case to System & Contracts)	
Example Indications Lower Risk	• Use of traceability tools to provide visibility of the link between Goals, Purpose and Requirements through to the Digital Twin System solution (system and services), Obligations and Accountabilities and Contracts. • Collaborating parties share visibility and use of tools where this facilitates clarity of obligations.
Internal Control Examples	If there is clear traceability from the Value Case and Purpose and Requirements through to the solution; and the IP owned, generated and used is traced to this solution and underpins and traces to clear contract obligations the risk should be lower. Traceability provides clarity through visibility. Clarity of traceability from IP risk considerations through to the Digital Twin System solution options during the design stage should allow mitigations to be considered and built into the system solution. Technical solutions that provide traceability of digital information associated with Physical Entities should reduce risk and allow traceability during a breach to mitigate consequences.
External Control Examples	Clarity of traceability between Value Case and Obligations should support agreement of contracts that support collaboration. Sectors

	requiring processes which demonstrate traceability across collaborating stakeholders could potentially improve clarity and external risk.

IP Risk Influencer: Complexity

Description

Complexity and Clarity closely relate to impact overall risk. A highly complex Digital Twin System, range of stakeholders and Structure and Incentives can potentially increase the risk of low Clarity. Conversely, increasing Clarity where there is Complexity can support managing overall risk. However, Complexity is independently linked to the Goal & Context, for example the Physical Entity may be a complex system of systems across world regions, or a single system contained within a specific country. Complexity is considered from the perspective of the Digital Twin System (System Complexity), collaborating and interacting stakeholders (Stakeholders Map of IP Owners, Users and Governance), and the structural, legal and business environment within which the Digital Twin collaboration operates (Structure and Incentives). Each is described in turn.

System Complexity

A Physical Entity can be an asset, system, system-of systems and include processes and enterprises. As the Physical Entity complexity increases so does the complexity of the Digital Twin System solution providing the Purpose.

However, complexity will be further complicated if the Digital Twin System and its collaborating stakeholders and supply chain cover a broad geography with differing legal environments and a multiplicity of data storage, analysis and data integration tools. For example, several academics comment on the globalisation of the semiconductor supply chain and expansion of computing devices which has increased the risk of computing hardware used as an attack surface to steal IP (Hu *et al.,* 2021).

For Digital Twin architectures which are modular and manage complexity and where complexity is within the control of a particular stakeholder this may reduce their risk. Conversely increasing system complexity, within their scope of control, may be beneficial to some stakeholders. For example, Novarty, 2021 noted that increasing the Physical Entity complexity and by offering different value added services it would make it harder to imitate. This may be of particular interest to Manufacturers and IP Owners of complex

Physical Entities as by retaining control over the Physical Entity lifecycle and the operational data that relates to the Physical Entity through offering XaaS such as Maintenance-as-a-Service they will control their risk. A sector must however retain a view of the sector or societal Purpose to ensure the needs of other stakeholders such as Operators/End Users are not adversely affected and may therefore need to regulate to balance complexity risks to Purpose.

Stakeholders Map of IP Owners, Users and Governance

Almarri *et al.* (2019) commented on the "multiplicity of parties" in collaboration contributing to unclear IP rights. New standards such as ISO/IEC 30173:2023 (British Standards Institution, 2023b) identify the types of Stakeholder groups involved with Digital Twins but not from an IP perspective. For IP collaboration risks, there are not only the IP Owners and Users directly relating to the Purpose, but indirect stakeholders, such as Finance and Insurance stakeholders involved in IP value, protection and policy, Information Managers and Regulators, contributing to governance, and 3rd Parties providing services from data storage to communications and hardware maintenance. A high number of stakeholders engaging with IP is indicative of higher Complexity and potentially higher risk influence.

Identification of new types of Stakeholder role may also be indicative of lower risk, such as a Data Steward (Open Data Institute, 2023) which links to Accountabilities & Responsibilities to "redress structural inequalities" and providing a "systemic" view of the data in relation to the Purpose. The Systems Standard BS ISO 15288:2023 (British Standards Institution, 2023c) identifies the role of an Information Manager for defining the knowledge management strategy and designating the authorities and responsibilities for its management.

While the map of stakeholders could be particularly complex, this area also links with Clarity which seeks to ensure there is a clear view of the stakeholders, and their obligations traced from the Goals & Context, which includes owned and licenced IP.

Weak or complex Governance of IP risk to collaboration would also increase risk. Safety and Security Assurance may already be linked to the Purpose but the specific considerations for IP risk need to be integrated.

Structure and Incentives

Complex sector, governance and organisational structures can provide a barrier to managing IP risk to collaboration especially where there are a high number of contractual boundaries or layers of governance which may not be aligned. Such Complexity can potentially increase the risk of opportunism or provide a disincentive. Structural complexity was a particular concern of respondents to the initial questionnaires and interviews. A typical quote (#5), *"..cost/effort to entry is too high, especially given the fragmentation of the industry meaning IPR ownership, asset ownership, potential value to be gained, all lie with different organisations.*"

The risk influence of complexity of incentives and disincentives not aligned with the Purpose was also evident from respondents, for example (#8), "*Willingness for different organisations to work together to find a solution, the rail industry is not structured to have a system that finds the best solution for passengers. Company incentives are often elsewhere*."

Sub-Category: System Complexity	
Example Indications of Lower Risk	• Supply chain from limited jurisdictions with greater legal harmonisation. • Decision Support service model minimising contractual interfaces. • Modular Digital Twin system architecture
Internal Control Examples	The Physical Entity IP Owner, such as a manufacturer, maximising control over the Digital Twin architecture with use of Edge Computing, passing data through their own data storage and analytics before passing processed information through Digital Twin services and offering XaaS. (Note the balance with External Risk Controls)

	Use Standard System Architectures with Clarity of IP ownership and licence obligations. Engage with supply chains and collaborating stakeholders in countries that are members of international IP treaties and in accordance with their Security risk assessment and policies. Use Systems Engineering approaches to assess and evaluate options to reduce complexity risk to achieving the Purpose.
External Control Examples	Sectors requiring use of standard Digital Twin Architectures and data schema and value maps for Purposes relevant to their Sector. Sectors and jurisdictions promoting and joining international IP treaties and working towards improved harmonisation of laws, and remedies and perhaps identifying actors and jurisdictions of known risk.
Stakeholders Map of IP Owners, Users and Governance	
Example Indications of Lower Risk	• Minimised contractual boundaries, potentially using systems modelling to support identification of supporting stakeholder structures. • Use of national or sector governance systems and standards which identify and involve a range of stakeholders from end users to IP and financial experts with defined roles.
Internal Control Examples	Early involvement of IP and Financial experts in IP risk management and governance. (Rock *et al.*, 2021) Implement Digital Twin System solutions and supply chains that minimise stakeholder contract interfaces to achieve the Purpose. Integrate stakeholder map with adopted Security Risk Management processes to minimise internal and external accidental as well as deliberate breaches.
External Control Examples	Establish external facilitating stakeholder roles such as a Data Steward

	Sectors to define standard stakeholder roles and obligations associated with sector specific Digital Twin Systems.
Structure and Incentives	
Internal Control Examples	Organisational structure justified in relation to business risk to achieve the Purpose which includes IP, Safety and Security considerations.
External Control Examples	Implement Sector structures that reduce the number of contractual barriers between stakeholders collaborating to achieve the Purpose. A systematic modelling of concept solution architectures will assist evaluate the relative risk. Create Incentives for collaboration and trust such as: • accreditation and audit of suppliers (e.g. AI developers) (relates to Maturity) • sector standards which achieve increased visibility of the relationship between the data value chain and implementation of standard contracts and approaches. This could be developed with the support of trusted not-for-profit organisations such as the Open Data Institute (Open Data Institute, 2023).
IP Risk Influencer: Longevity	
Description	
Longevity risk influencers relate to time. The three related time factors are: • Life-Cycle Stage • Contract Length Timeframe • Physical Entity Life Timeframe The Life-Cycle Stage refers to the Life-Cycle of the Physical Entity, whether pre-Digital Twin through design to Manufacture or during the Operation and Maintenance stage. Within the Operation and Maintenance Stage this could be further subdivided into early Operation, mid-Operation or late-stage Operation. This may be important for Physical Entities with a relatively long operational life and that may undergo various upgrades and	

changes during this Life-Cycle Stage or encounter changes to the related Digital Twin technologies. As such Physical Entity Life Timeframe is an additional risk influencer independent of the Life-Cycle Stage. Participants to the interviews and questionnaires noted that the Physical Entity Life Timeframe related to IP Value with examples of rights-holders more reticent to provide access to design and data in the early stages of operational life but more willing to share data as the Physical Entity approached end of life and they had new innovations and products to offer.

Contract Length Timeframe refers to the length of a contract between stakeholders. Contract Length links to Clarity-Obligations, with a focus on those risks that relate to absolute contract length, such as business climate and priorities changing over time, or contract length relative to the Physical Entity Life Timeframe which may introduce risk relating to license transfer and data. As participants commented on how changes to a business over a contract period can change their attitude to particular risks this may also relate to a changing attitude to IP licence or contract breach over time.

A Physical Entity with a longer life will be exposed to given risks over a longer period which could impact the likelihood of those risks causing an IP risk to collaboration. Over a longer period there is also more likely to be change, such as changes of business ownership, Physical Entity and IP transfers and upgrades and changes to the Physical Entity itself. Participants to the initial interviews and questionnaires commented on the introduction of digital technologies and how existing Physical Entities and associated contracts had not envisaged the potential of Digital Twins and so it was higher risk to adopt Digital Twins for older, existing Physical Entities.

Example Indications of Lower Risk ***Life-Cycle Stage***	
Internal Control Examples	A Risk Management Process that considers risks and mitigations in all life-cycle stages and provisions for changes within a Life-Cycle Stage. Systems life-cycle processes that consider IP in contract obligations from Stage to Stage, particularly post-manufacture/construction with handover into Operation and Maintenance. (Almarri *et al*, 2019)

External Control Examples	Developing standards or guidance for managing IP rights through changes in Operations and Maintenance stages for Purposes of importance to the Sector End Users. For a sector, defining the data thread, ownership and required licences through each Life-Cycle Stage for a generic application, including defining monitoring and regulation. This should be carried out in consultation with stakeholders.
Contract Length Timeframe	
Internal Control Examples	For Physical Entity IP risk control a rights owner such as a designer that also manufactures may consider retaining ownership of the Physical Entity and moving to a Physical Entity service contract, XaaS, which aligns contract length with a Physical Entity life stage to retain control over the IP and the Digital Twin Supply Chain.
External Control Examples	Standard contracts linked to standard architectures for Purposes of importance to a Sector. Sector implementing accreditation and audit of Digital Twin services during a contract timeframe to monitor security, IP and confidentiality compliance and minimisation of opportunistic and monopolistic behaviours
Physical Entity Life Timeframe	
Internal Control Examples	If considering change to a Physical Entity Service XaaS contract, reflect on length of Physical Entity life in consultation with finance and insurer stakeholders and ensure modularity of architecture to provide flexibility to change and upgrade.
External Control Examples	Consider Sector Digital Twin Services Governance and Architecture that allows integration of Digital Twins and changes to Physical Components and Subsystems over time.

Table 13: IP Risk Influencers – Description Summary

The IP Risk Influencers can relate together to increase risk, such as a high complexity and low clarity scenario but the risk control examples contribute to the identification of categories of Risk Mitigation Tools that can support managing and reducing risk.

Hypothesis: The IP Risk Influencer sub-categories and factors identified can potentially influence IP risk to collaboration with Digital Twins.

6.2.5 Risk Mitigation Tools

The Risk Mitigation Tools are intended to mitigate the risks either from cause to top event or from top event to final consequence. The coded Tools identified relate to the potential control of Risk Influencers. The Tools were categorised into four sub-categories with three Factors within each Sub-Category. It is anticipated that Tools within each of these factor headings will develop and be tested in the next few years as Digital Twins mature.

It is expected that the Tools will be developed by governments and sector leadership groups for the use by stakeholders, particularly the Legal and Governance & Policy Tools which includes Generic Assurance Model, Sector Audit and Accreditation Schemes, Policies and Standards as well as Model Contracts and Insurance, IP Protection and Licence Model and a Regulatory Sandbox for exploring the effectiveness of approaches to balance IP benefits and achievement of End User Purpose before committing them in law.

Governments and sector leadership groups are also anticipated to drive forward Business and Technical Tools, particularly Generic System Architectures and Interfaces, which has started to emerge with recent standards such as BS ISO/IEC 30173:2023 (British Standards Institution, 2023b). However, other Tools can also be driven forward by individual stakeholders depending on their role. For example, Developers can build in Technical IP Tracking and Cyber Security Controls and adopt a Systems Methodology and MBSE model to provide Traceability from Purpose to Solution recognising that traceability management capabilities are still developing and an area for potential future research (Anda & Amyot, 2022). This MBSE model should remain live for the life of the Physical Entity, capturing changes and including a model layer to show the traceability of IP and data ownership and licences to contracts and stakeholder obligations. Issues of model ownership and ambiguity of IP and use and re-use of data in the operational stages has been discussed in the context of the built environment and application of BIM. Such scenarios can be modelled in the MBSE model and traced to contract terms to provide Clarity.

Generic Risk & Mitigation Options will relate to the Defined Stakeholder Types & Roles, IP Protection & Licence Model and Generic System Architecture and Interfaces.

Hypothesis: The Risk Mitigation Tools sub-categories and factors identify the considerations for mitigating Intellectual Property risk to collaboration with Digital Twins.

6.3 Relationship Between Factors and Categories

6.3.1 Introduction

Although section 6.2 has discussed the relationship between some factors, sub-categories and categories, this can be further illustrated through examples. Figure 12 considers managing IP Risk to achieving the Decision Support Purpose through collaboration, considering stakeholder viewpoints from the IP Owner and User perspectives. As this scenario is focussed on the viewpoint of specific stakeholder types the other potential viewpoints of Life-cycle and Contract and all other Stakeholders are reflected in the Business Context. The Application Sector stakeholders considered are collaborating stakeholders that may be IP Owners, Users, or both. The IP Context specifically relates to Legal, Financial and Insurance stakeholders. This diagram is then used to illustrate the relationship between Risk Influencers and Tools.

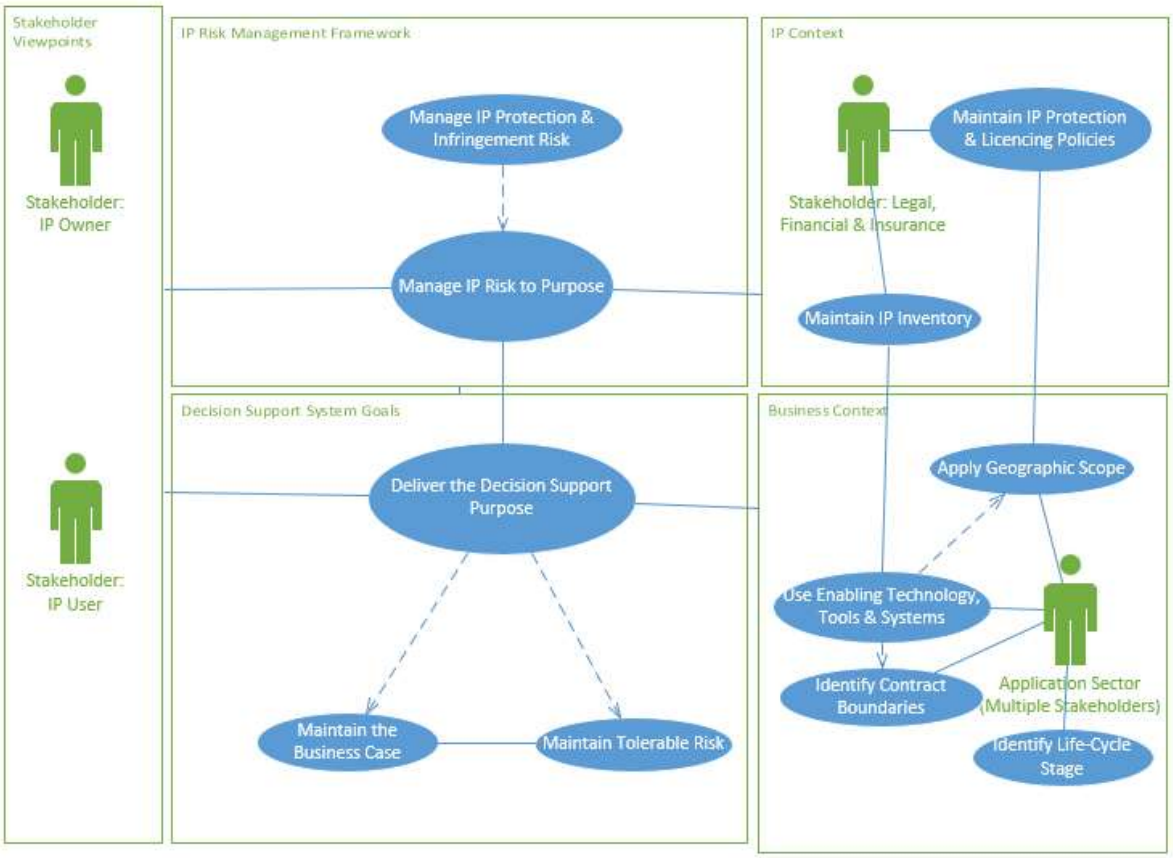


Figure 12 - Extract Use Case for Managing IP Risk to Deliver a Decision Support Purpose

Illustrations of the relationships between Risk Influencer and Risk Management Tool categories are identified in the following sections. The Risk Influencers are identified by orange diamonds and the Tools by green hexagons.

6.3.2 Example - Clarity of the Legal Environment Related to Policy

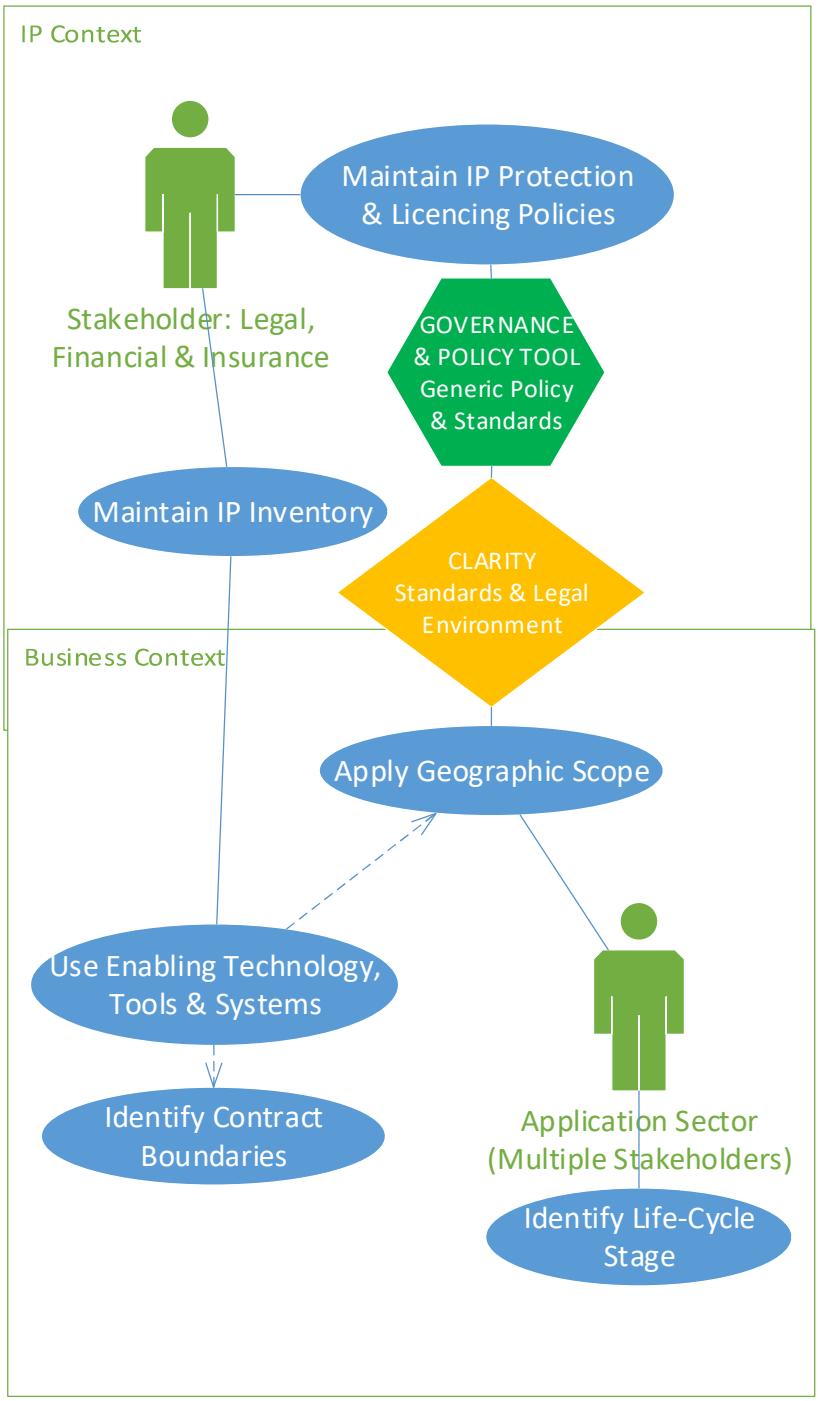


Figure 13 - Example Risk and Mitigation Tool Related to System Geography

From the perspective of geography, it has been identified that the legal rules and interpretations can change between jurisdictions, and this can impact the protection of IP and the remedies available and lead to ambiguity. A group of collaborating stakeholders, especially where this relates to a sector or public purpose, can mitigate through policies and standards. For example, specifications and procurement policies may state limits to the geographical areas for data storage and source of hardware and rules for the jurisdictions where IP protection is sought.

6.3.3 Example –Complexity and Clarity Related to Systems Methodology Tool

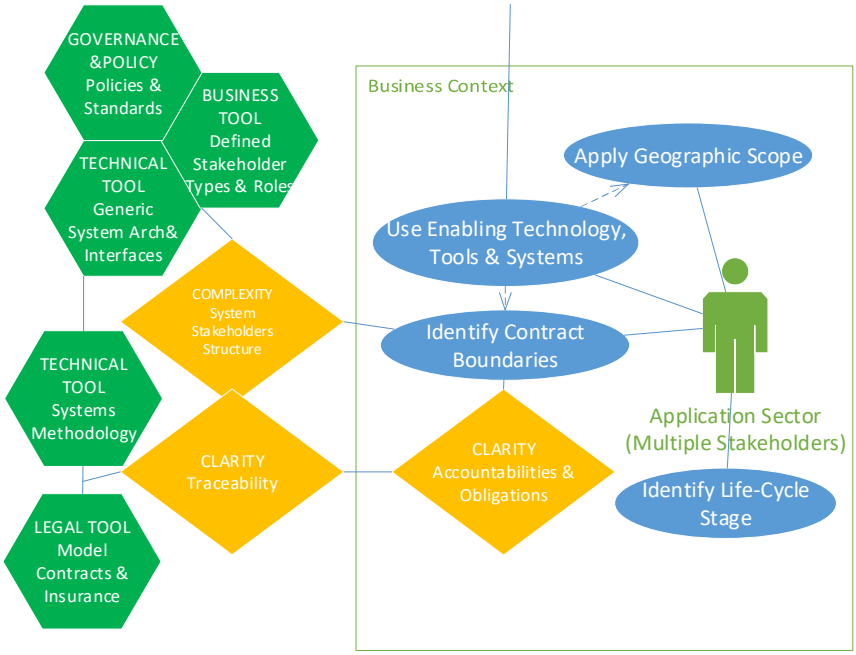


Figure 14 - Example Systems Methodology Tool Related to Complexity and Clarity

A lack of systematic traceability from Purpose through the decision support solution through to IP registers and accountabilities and obligations in contracts increases the risk that IP risks are not mitigated and any changes to IP ownership and licence structure over time cannot be effectively evaluated. A Systems Methodology such as MBSE, applied during system development could potentially be extended to cover an IP contract viewpoint to provide this traceability and clarity over a lifecycle. For classes of decision support, such as predictive maintenance for railway systems, generic system architecture and interfaces linked to defined stakeholder types and roles could be developed and traced to model contracts. If overseen by sector leadership this could potentially provide greater clarity while also allowing specific technologies and changes. A basis for approaches can build on the system of systems and service systems engineering knowledge areas of the SEBoK v 2.10 (SEBoK, 2024), released

06 May 2024, using methodologies such as SySML to provide the traceability between tools. The SEBoK Enabling Systems Engineering knowledge area provides the basis for identifying the systems roles, capabilities and business culture at business, team and individual level for enabling such systems approaches which can form the basis of the Governance & Policy Tools. This in turn could link to Business Tool – 'Defined Training and Qualifications' (not shown). Requiring a systems approach through standards such as ISO/IEC 15288:2023(British Standards Institution, 2023c) which include acquisition(clause 6.1.1), supply (clause 6.1.2) and knowledge management(clause 6.2.6) processes which link to the life-cycle stage, in addition to use of Collaboration Frameworks could in turn influence the specifics of the Technical Tools implemented. Model based Systems Methodology can also apply to other risk mitigation tools such as the Generic Assurance Model using standards such as the Object Management Group's Structured Assurance Case Metamodel (SACM, 2020).

6.3.4 Example – Maturity of Trust related to Governance and Policy Tool

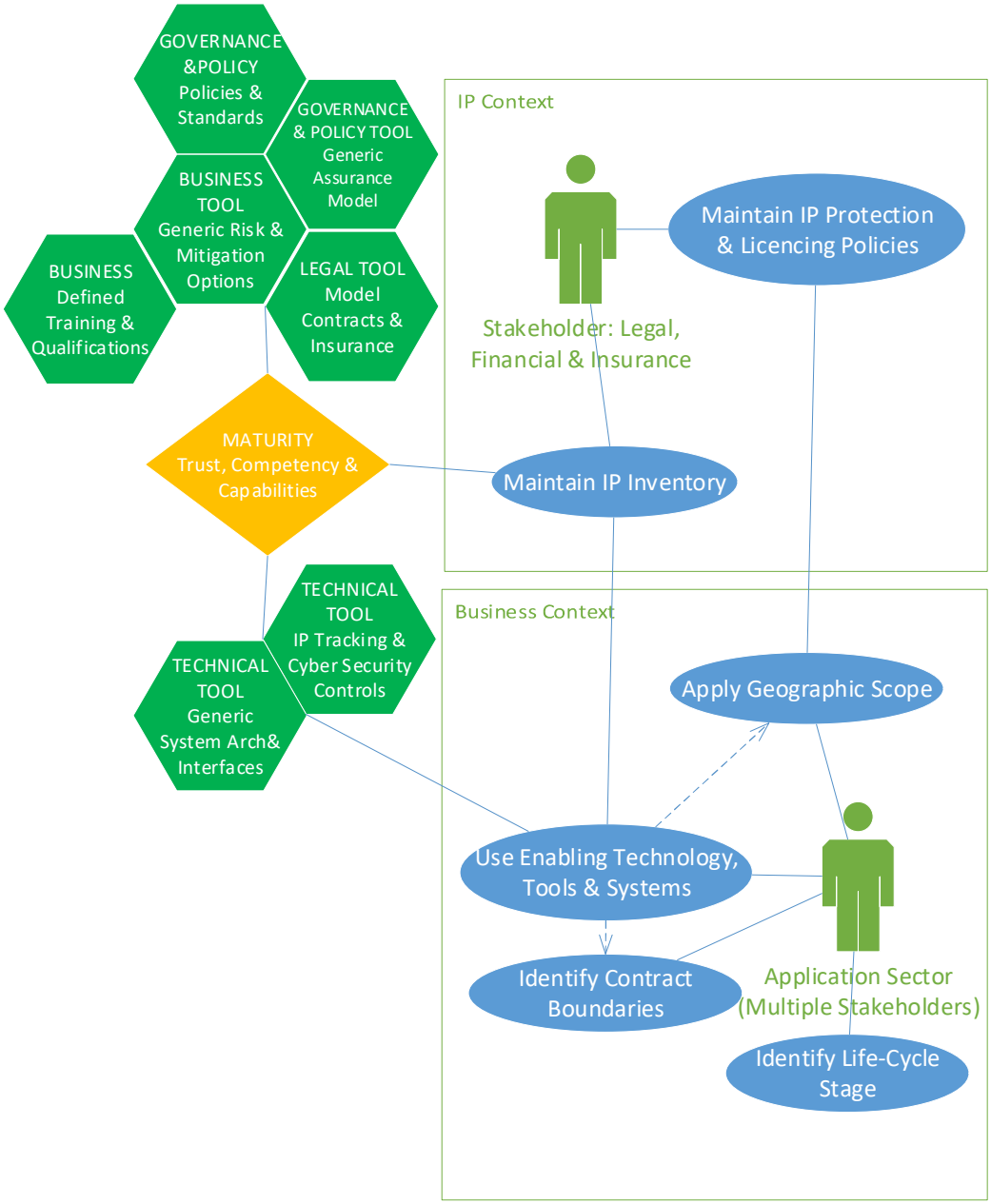


Figure 15 - Example Governance & Policy Tools Related to Maturity

Trust risk, relating to the appropriate handling of proprietary data and IP can be managed through a combination of technical, business and legal tools underpinned by governance and policy tools. Technical controls build trust through defined system architectures, to include data architectures, which track and control access to proprietary IP to minimise risk to the Purpose and individual stakeholders. This is then supported by legal controls, particularly model contracts to clarify ownership and obligations. However, it can be envisaged that the Technical Tools will have a level of maturity and the process of their design and control in

the business context will itself influence trust. As such Trust in collaboration requires the support of Business, and Governance & Policy tools. For example, Policies and Standards will support standardisation of the system architecture and the legal, risk, systems assurance and collaboration frameworks that need to be followed. This will identify the competencies required for collaboration and within each stakeholder, application of standards, leading to generic risk and mitigations which contribute specific competencies and requirements for procurement policies. Once a contract is awarded through use of Model Contracts, which require compliance with standards and specify obligations to mitigate risk to include at the end of a contract period, required training and qualifications and implementing Audit and Accreditation, monitoring will be initiated to ensure ongoing compliance.

As trust and business conditions can change over time multiple mitigations will be needed using the Generic Assurance Model in support and providing Insurance against breach from residual risk.

6.4 Relationship to Risk Management Standards

BS ISO 31000-2:2018 (British Standards Institution, 2018) is the principal risk management standard and includes parts for particular types of risk. BS ISO/IEC 15288:2023 clause 6.3.4.3 (British Standards Institution, 2023c) notes that specific systems risk standard BS ISO/IEC/IEEE 16085:2021 (British Standards Institution, 2021b) is aligned with BS ISO 31000 (British Standards Institution, 2018) and highlights the risk activities of risk management planning, maintaining the risk profile, risk analysis, risk treatment and monitoring. During the early stages of this research study related risk guidance BS ISO 31022:2020 (British Standards Institution, 2020) was published which provides guidelines for the management of legal risk.

Some risk standards relate to the Purpose, so for predictive maintenance of a safety critical system using Digital Twins Safety Risk standards apply and some are specific to a sector application. However for Physical Entity management, for the realisation of value, more generally, the asset management standard BS ISO 55001 (British Standards Institution, 2024c) applies. Safety then relates closely to Security which is evidently important for managing IP and protecting from accidental or deliberate breach. As such BS ISO 27001 (British Standards Institution, 2023a) applies.

The structure and coverage of these standards was reviewed against the emerging IP Risk Management Framework to identify where the IP Risk Framework related and whether there were new insights not currently contained within the existing standards. The ISO 31000 standards (British Standards Institution, 2018) cover approaches to Risk Identification, Analysis, Definition and Degree of Risk and Risk Treatment and this and the related standard parts for legal, security and safety cover Leadership, Planning, Support, Operation, Performance Evaluation and Improvement and the concept of 'internal' and 'external' factors where 'internal' factors are substantially within the control of a stakeholder. The legal, safety and security standards then provide more specific guidance relating to those particular risks.

The review concluded that the constructed IP risk framework, overlaps with the Security, Safety and Legal standards and guidance notes but there are Risk Mitigations and grouping of mitigations which are new and ought to be captured in a new guidance note. This is illustrated in Figure 16, where the Risk Mitigation Groupings of Privacy, Access Control, Physical Security and Human Resource Security in the Security Standard are related to the groupings of Legal Controls, Technical Controls, Business Controls and Governance and Policy in the emerged IP Risk Framework. The processes box identifies example management, primary and supporting processes from a particular railway asset web link. However, there are further relevant business standards such as the collaboration framework BS ISO 44001:2017+A1:2024 (British Standards Institution, 2024b) and technology standards relating to risk management such as those for systems and software, for example, BS ISO/IEC/IEEE 16085:2021 (British Standards Institution, 2021b) and BS ISO/IEC/IEEE 15288:2023 (British Standards Institution, 2023c).

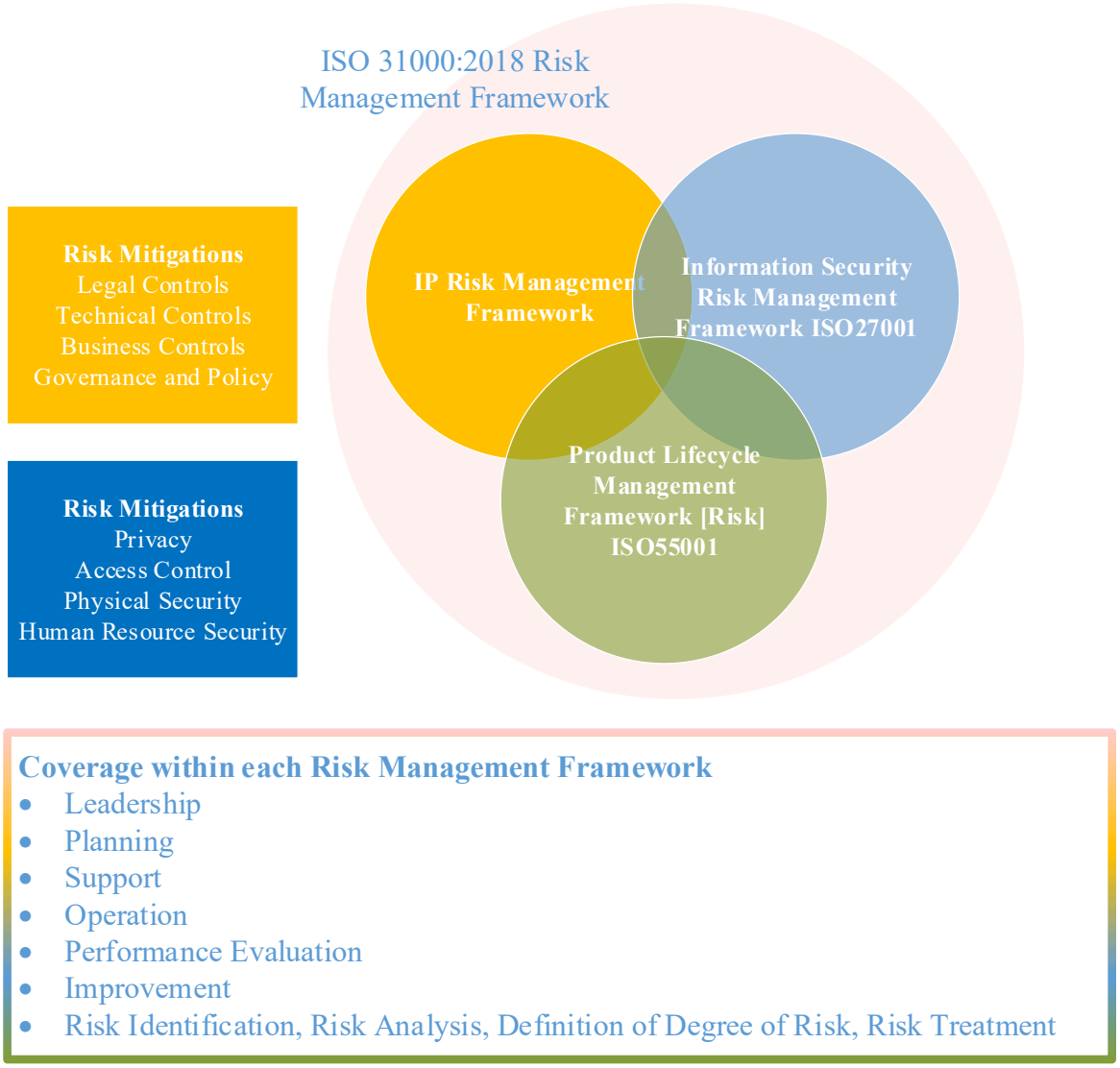


Figure 16 - Comparison of Risk Management Framework Standards with the Emerged IP Risk Management Framework

The constructed IP Risk Framework was compared with the legal risk guidance of ISO31022:2020 (British Standards Institution, 2020), where it references IP explicitly. Section 3.2 ISO31022:2020 (British Standards Institution, 2020) provides the standard's definition of legal risk which includes risks related to non-contractual rights such as IP and clarifies that this includes the risk of an organisation not asserting its rights as well as the risk from an organisation infringing third-party IPR. Both of these scenarios are covered by the IP Risk Framework. Section 5 ISO31022:2020 (British Standards Institution, 2020) relates to the Legal Risk Management Process and Section 6 relates to the Implementation of the Management of Legal Risk. There are then five informative Annexes, providing examples of risk identification, estimation of likelihood of events and consequences of events related to

legal risk with an example of a legal risk identification matrix and considerations for contracts. The clauses explicitly mentioning IP are related to the IP Risk Framework in Table 14.

ISO 31022:2020 Clause	**Mentions of IP**	**Coverage in constructed IP Risk Framework**
5.2	Clarifies the internal and external context of legal risk. Explicitly identifies that internal risk includes "assets that the organisation owns, such as intellectual property."	Considers internal and external Risk Influencers in relation to IP and goes further by recognising that these are identified through their impact on and traceability to the Purpose.
5.3	Identifies infringement of IPR as a source of information useful to the identification of legal risk.	Infringement of IPR, whether accidental, careless or deliberate is accommodated in the framework cause-consequence diagrams specifically for Digital Twin applications for decision support.
Annex A1 (Informative)	The example "Legal Risk Identification Matrix (LRIM)" identifies six categories of risk, Category 4 of which is "Infringement of rights" with the example that this could be an IP infringement by a third-party, without permission.	Infringement of IPR is included in the framework but links Goal & Context, especially Purpose to IP Risk Influencers and Tools to provide more understanding as to how such Infringement can be initiated and mitigated.
Annex D (Informative)	The example of estimating the consequences of events related to legal risk mentions examples of non-monetary consequence from "minor loss of reputation, corporate	Such consequences are included in the framework cause-consequence examples which also additionally facilitates consideration of relative

ISO 31022:2020 Clause	Mentions of IP	Coverage in constructed IP Risk Framework
	image or intellectual property." Other consequence considerations are geographical and intra-organisational.	likelihood through the Risk Influencers and the relationship between factors to enable comparison of relative risk.
Annex E (Informative)	Key issues to consider when reviewing contracts include, Disclaimer of Warranties that third party rights are not infringed and that Indemnities are identified to include covering infringement of IP rights and inappropriate disclosure or data breach. The standard notes that IP and data breach can be "extremely costly to defend and remedy." Although IP is not explicitly mentioned there are several other issues which have been identified as important in the current research for IP risk to include "Location of Data", "Ownership of Data" and "Insurance". For "Ownership of Data" such is recommended to be with the organisation that provides the data and recommends clarifying that the service provider does not acquire any rights or licences.	The listed issues form the basis for the 'Legal Tools – Model Contracts'. There are other issues revealed in the IP risk framework that should consider IP risks such as "assignment and subcontracting" in relation to the system solution and limiting or controlling these to trusted organisations subject to collaboration standards or those accredited e.g. for AI development. For Ownership of Data the IP Risk Framework does not presume an owner but requires consideration of ownership related to maintaining the Purpose for collaborating stakeholders through the life of the Physical Entity and maps to the Business Tools: Stakeholder Roles. This ensures that ownership is clarified and defined through

ISO 31022:2020 Clause	Mentions of IP	Coverage in constructed IP Risk Framework
		linking Purpose and Stakeholder Roles.

Table 14: Explicit consideration of Intellectual Property in ISO 31022:2020

Within ISO 27001:2023 (British Standards Institution, 2023a) there is only one explicit mention of IP. This is in Annex A, Table A1 which provides Information Security Controls aligned with ISO 27002:2022 (British Standards Institution, 2022). IPR is mentioned as an Organisational Control with the following requirement:

"The organization shall implement appropriate procedures to protect intellectual property rights." (British Standards Institution, 2023a, ISO 27001:2023 Table A1)

The controls in ISO 27002:2022 (British Standards Institution, 2022) are divided into Organisational Controls, People Controls, Physical Controls and Technological Controls. IP is predominantly contained within Organisational Controls (section 5.32 British Standards Institution, 2022, ISO 27002:2022) explicitly with a couple of mentions in People Controls relating to non-disclosure and managing employee changes. The Organisational and People considerations relating to IP protection risk are summarised in the standard as:

- Information Security Requirements
    - for complying with IP rights: terms in contracts with suppliers, including clarity as to how they will be met during the management of projects, especially during early stages. (5.8, 5.20 ISO 27002:2022)
    - preventing unauthorised copying of information by personnel especially during changes or during a notice period relating to termination of employment. (5.11, 6.5 ISO 27002:2022)
    - for the secure termination of supplier relationships to include, clarity of IP ownership developed during the engagement as well as other considerations such as return of assets and ongoing requirements for confidentiality. (5.19 ISO 27002:2022)
- Requirements to implement procedures for protection of IP and trade secrets (clause 5.32 ISO 27002:2022) to include:

    - defining and communicating policy on protection of IP rights
    - use of confidentiality and non-disclosure agreements (6.6 ISO 27002:2022)
    - publishing procedures for IP rights compliance that:
        - define compliant use of software and information products
        - do not duplicate or convert to other formats or extract information other than as permitted (Refers to data sharing agreements)
        - do not copy in full or part printed material to include standards
        - maintain appropriate licence conditions ensuring maximum number of users is not exceeded
        - acquire software from trusted suppliers
        - maintain asset registers and identify all assets with IP protection requirements and proof and evidence of ownership of licences etc
        - carry out reviews to ensure only authorised products are used
        - dispose of or transferring software to others
- Governance for complying with procedures for IP rights such as with terms and conditions for software and obtained information

Relating to the constructed IP risk framework, an absence of such requirements would be indicative of higher risk through the Clarity and Maturity Risk Influencers. For decision support systems based on Digital Twins the Tools provide a means of implementing these requirements and linking them to the overall Purpose to facilitate risk management.

IP is also mentioned under the standard's Technological Controls to include identifying the need for requirements for:

- procedures to protect end point devices (8.1 ISO 27002:2022) to mitigate IP dispute risk when using personal devices,
- read and write access to secure source code (8.4 ISO 27002:2022) and mitigate introduction of unauthorised, unintentional or malicious code that would impact confidentiality of IP.

These are considered within the IP Risk Framework Tools, IP Tracking & Cyber Security Controls and Generic System Architecture & Interfaces. The standard also identifies a Business and contract control, requiring information security requirements, to be communicated to suppliers when outsourcing development (8.30) to include consideration of

license agreements, IP rights and code ownership related to the outsourced content. Model Contracts within IP Risk Framework Tools can provide this linked to the Purpose.

The relationship between the constructed IP Risk Framework, Risk Mitigation Tools groupings for mitigating risk and the security standard ISO 27002:2022 (British Standards Institution, 2022) control groupings are compared in Table 15.

IP Risk Framework Risk Mitigation Tools Grouping	**Security Risk Control Grouping (ISO27002:2022)**	**Explicit Mention of IP in ISO27002:2022**	**Comment on Broader Relationship between IP Risk Framework Mitigation Tools Grouping and ISO27002:2022**
Technical	Technological	Protection of end point devices (8.1) Read and write access to secure source code (8.4) Outsourcing development (8.20)	The standard identifies some example considerations only which link to the IP Risk Framework topics of: • IP Tracking and Cyber-Security Controls • Generic System Architecture & Interfaces However, unlike the IP Risk Framework the standard does not integrate the considerations nor link the Systems Methodology.
	Physical	No explicit mention	Physical Security controls (ISO 27022:2022) include physical system architecture

IP Risk Framework Risk Mitigation Tools Grouping	Security Risk Control Grouping (ISO27002:2022)	Explicit Mention of IP in ISO27002:2022	Comment on Broader Relationship between IP Risk Framework Mitigation Tools Grouping and ISO27002:2022
			considerations such as storage media, cabling and equipment maintenance as well as physical location of equipment. This relates to 'Technical – Generic System Architecture & Interfaces" of the IP Risk Framework.
Business	People Organisational	Project lifecycle (5.8) Suppliers (5.19, 6.6) Employees (5.11, 6.5)	Supplier, Project and Employee considerations are considered under 'Defined Stakeholder Types and Roles' linked to 'Generic Risk & Mitigation Options.' Defined Training and Qualifications – only covers mention of technical and security capabilities within the standard and does not clarify legal capabilities.
Legal	Organisational	IP Rights (5.32)	Although there is mention in the standard to consider security obligations in relation to IP Rights there

IP Risk Framework Risk Mitigation Tools Grouping	Security Risk Control Grouping (ISO27002:2022)	Explicit Mention of IP in ISO27002:2022	Comment on Broader Relationship between IP Risk Framework Mitigation Tools Grouping and ISO27002:2022
			are no specifics for consideration under the following topics of the IP Risk Framework: • Model contracts & Insurance • IP Protection & Licence Model • Regulatory Sandbox/Framework
Governance & Policy	Organisational	IP Rights (5.32)	The standard identifies Policy as a control for information security (5.1) with guidance on the scope of content of such a policy and role of management in approval with more specific policies for topics such as access control, information transfer and asset management. This links to 'Policy & Standards' but only covers the security aspects of IP information.

IP Risk Framework Risk Mitigation Tools Grouping	Security Risk Control Grouping (ISO27002:2022)	Explicit Mention of IP in ISO27002:2022	Comment on Broader Relationship between IP Risk Framework Mitigation Tools Grouping and ISO27002:2022
			The standard identifies security considerations for 'Sector Audit & Accreditation Schemes' but does not discuss specific issues such as sector accreditations. Security Management provides a part of the 'Generic Assurance Model'

Table 15: Comparison of Risk Control Groupings in ISO 27002:2022 and the IP Risk Framework

Many of the other information security controls listed have been identified as relevant to IP risk management in the current research study, for example, 'Information Security Roles and Responsibilities' but there is no guidance in the current standards to relate to IP risk management to achieve the Purpose.

While Security and Safety have assurance cases, it is only recent academic studies that have sought to combine the assurance of Security and Safety together given the links between causes and initiating events and need to ensure mitigations are appropriate for both and to maintain assurance cases through changes, for example Wei *et al.,* 2024. While IP protection can be mitigated through Security assurance, if a breach occurs it can impact the Purpose which could be linked to a Safety Case. As such IP risk to collaboration needs to be integrated with Security and Safety Assurance. As the focus of this research study is to understand the factors important for IP risk to collaboration to achieve Purpose such integration will need to be the consideration of further studies.

6.5 Application of the Risk Framework

6.5.1 Introduction

The second aim of the research study was to:

Explore how this framework could be applied to assure that life-cycle Intellectual Property Risks to Digital Twin Collaborations are effectively managed in a regulated sector such as rail.

The data analysis identified several potential applications of the risk framework. Two potential applications were developed and subsequently presented in the Evaluation (Chapter 9). These two potential applications are described and justified in relation to the aim.

6.5.2 Using the Framework to Manage Risk

For a particular Goal & Context a set of cause-consequence diagrams can be established which link the IP Risk Influencers and the mitigating Risk Management Tools to support the management of risk. In order to explore this application example risk bow-ties (Ministry of Defence and Military Aviation Authority, 2018) were developed from risks identified in literature.

The examples considered included:

- Trade Secret misappropriation, for example Gorbatyuk (2016)
- Unclear ownership and permitted use of data used by AI developers (Druetta, 2018)
- Accidental, negligent and deliberate infringement of IP

Figure 17 provides a simple example to illustrate the application. Note that this is not a fully developed example but is intended to illustrate the application while fitting on the page.

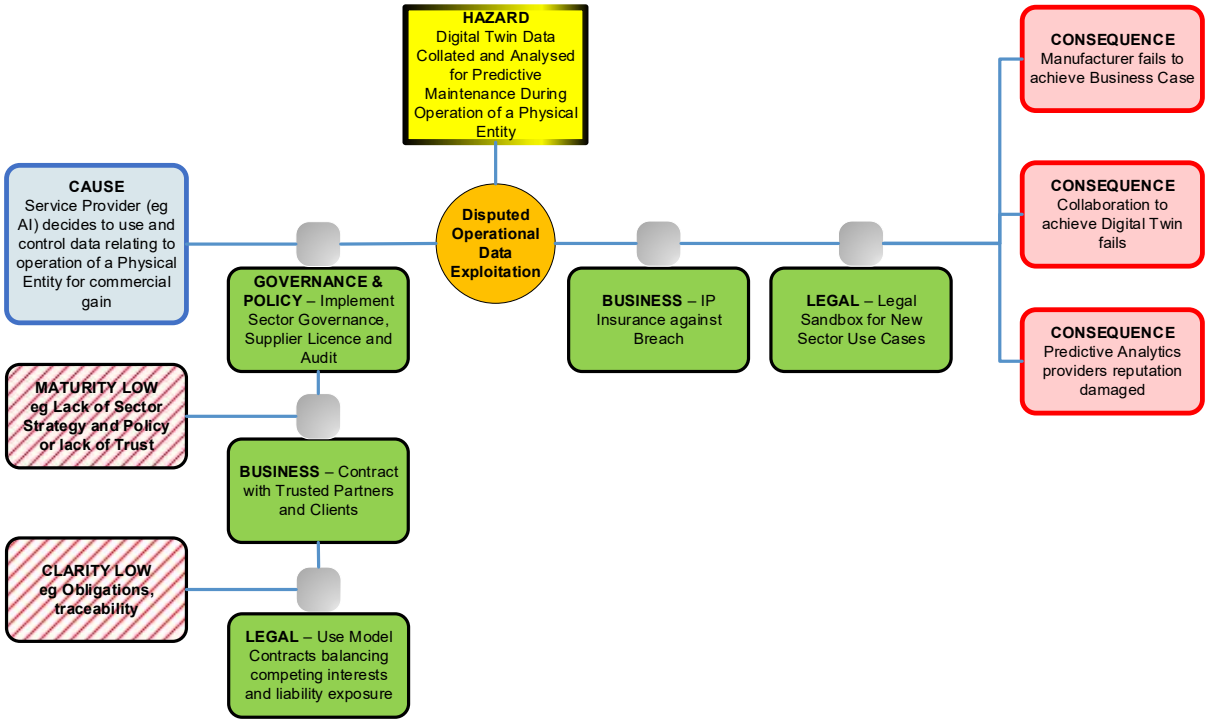


Figure 17 – Example Bow-Tie Cause-Consequence Risk

The cause (blue box) of the initiating event (orange circle) can be exacerbated by risk influencers (red hatched box) and mitigated through Risk Management Tools (green box). Once the initiating event has occurred the path to the consequences (red box) can be further mitigated or exacerbated by the risk influencers and tools.

As the Purpose for using a Digital Twin could contribute to system safety and security, and IP risk is mitigated through security considerations, application of the framework to Assurance Cases was explored. In particular as Risk Mitigation tools identified the need for a 'Generic Assurance Model' and use of 'Systems Methodology' the use of model based assurance frameworks was considered. GSN was used for the basis of evaluation (Chapter 9) as this is familiar to the researcher. However, as noted by Wei *et al.*, 2024, SACM (OMG, 2020) is developing as the basis for model based assurance as it is more appropriate to the continuous and changing assurance needs of systems through their operational life, so in a future project the IP Risk GSN can be presented in SACM.

The goals were supported by evidence. For example, evidence that the IP Inventory traced to both obligations and system solution and obligations traced to contracts such as 3rd Party IP License Agreements and Data Sharing Agreements.

6.5.3 Using the Framework to Evaluate System Alternatives

Where a sector has not yet identified a Digital Twin solution to achieve a Purpose or a stakeholder needs to evaluate procurement options for a Digital Twin supplier there is a need to evaluate the relative risk of options to support decision making. As such the potential application of the IP Risk Framework for this purpose was explored.

For the Maturity Risk Category, criteria indicative of effective risk management were identified and presented in a table. Columns were then provided to weight and score the criteria in a range 1-5. Multiplying the score by the weighting and adding these up provided an overall risk score. The full development, evaluation and application of the criteria is recommended as a subject of future research (Chapter 8). However, the participants in the evaluation were able to express a view on the potential of this application using the example as part of the current research study (Chapter 7).

6.6 Summary

The described risk framework identifies categories and factors which relate to support understanding of how IP can influence the risk to multi-stakeholder collaboration using Digital Twins for decision support through the life-cycle of a Physical Entity. While existing risk standards identify management of IP as a business risk and provide some discrete example considerations for individual stakeholders managing that risk from their viewpoint, by bringing categories and factors together, the constructed IP risk framework provides new understanding. In particular, it clarifies the combination of technical, legal, business, and governance and policy tools that are needed to manage risk and provides the basis for evaluating relative risk through risk influencers. This has clarified the importance of systems methodologies in providing traceability and clarity for managing risk, in particular linking Digital Twin service solutions through their enabling architectures and associated IP through to obligations and model contracts. It also clarifies the influence of complexity, maturity and longevity on overall risk.

It is also concluded that there is potential to apply the IP Risk Framework to assure that risks are effectively managed. The use of systems modelling approaches supports traceability and change impact assessment over time. There is potential to apply the framework to manage overall risk to a Digital Twin solution implementation and to also assess implementation and procurement options.

Chapter 7 Evaluation of the Risk Framework

7.1 Introduction

Stage 3 of the research study evaluated the IP risk framework against the following hypotheses:

H2: The described Framework explains how Intellectual Property Risks potentially impact multi-stakeholder collaboration using Digital Twins for life-cycle decision support.

H3: Application of the framework could mitigate risks to achievement of multi-stakeholder collaboration using Digital Twins for life-cycle decision support.

Evaluation of H3 also considered that the framework could potentially be usefully applied to assure that IP risks are managed over time. A TACT empirical verification approach was considered (Daniel, 2018) in development of the evaluation stage (Appendix 7) to reflect on the rigour of the evaluation design. The evaluation comprised an Expert Review of the framework by those with the expertise and experience of IP issues and Physical Entity decision support and, additionally, application of the framework to compare Digital Twin for Decision Support case studies based on information in the public domain. The two separate approaches were adopted to both minimise bias by providing different evaluation approaches and also as it was anticipated that there would not yet be the depth of case study information in the public domain in the rail sector. The Case Study evaluation also allowed certain aspects of the framework to be reviewed in more detail to explore the application.

A further evaluation was conducted by comparing the IP related legal issues identified as important for consideration when leveraging Big Data in managing transport operations (LeMo) with the constructed IP Risk Framework. This was considered to provide a contribution to triangulation of factors in support of H2 as although the focus of the LeMo study was Big Data it is evident that lifecycle data and AI relating to Digital Twins for decision support includes Big Data considerations.

7.2 Expert Review

The Expert Review involved presenting the IP Risk Framework to individual experts and asking them for their views on the framework through structured questions. The review was supported by a structured presentation which allowed an aspect of the framework to be

presented and then questions asked before moving on to another aspect of the framework. The presentation slides are captured in Appendix 8.

At each pause in the presentation a Yes-No or 5-scale Likert question was asked and comments explaining the response were also captured to provide context.

The review comprised 10 participants: 5 legal experts and 5 asset managers, the latter currently working for companies with responsibility for Physical Entities in the rail sector.

The legal experts comprised 2 Patent Attorneys, 2 In-House Legals and 1 IP Academic. The asset managers represented a Rolling Stock owner, OEM, Train Operator, Infrastructure Manager and Engineering Technical Services.

For reliability and validity, the review required consistent support across participants. The expectation was that if there were significant changes required to the framework such changes would be reviewed again by the experts until they were all supportive. Such a second review was not required as all the participants responded positively to the framework from the first round of review and changes to the framework only related to clarifications of descriptions. For example, the term "MBSE Methodology" was replaced with "Systems Methodology" as MBSE is not a common term for legal experts in particular and it was advised to change "contract length" to "contract term". The experts were asked to challenge the framework with scenarios and cases from their experience. These discussions also provided more context specific illustration of issues of particular concern to stakeholders and views on the content they would expect to see within the categories. All such issues explored during the review were found to be reflected by the framework. Table 15 provides a summary of the responses illustrated with examples of supporting comments, including example views on content anticipated within each category description, especially the Risk Management Tools.

Question	**Responses**
Q1 To what extent to you agree with the following statement: "The conceptual framework forms the basis of understanding how	All Agreed or Strongly Agreed Example comments were:

Question	Responses
Intellectual Property risks potentially impact achievement of a Digital Twin Purpose."	*"…the key issues are identified in the centre and the factor groupings are well classified and comprehensive. It seems easy to structure an audit based on this framework.*" (Participant 02) "*Recognise could be different levels of complexity of Digital Twins. Could apply from a subsystem through to a system. Increased complexity could bring in greater numbers of stakeholders*." (Participant 03) "*On face of it is complex but the individual steps within the framework are great*" (Participant 07) "*Clear way of managing risk and segmenting the factors. It should help to facilitate better understanding among the range of stakeholders, not just the legal sector.*" (Participant 10)
Q2 Risk Influencers: In your view are any Risk Influencer Categories missing or out of place? In your view do the descriptions of Risk Influencers adequately convey their meaning?	One Participant responded "Yes" to Risk Influencer out of place, but their comment was "*Check that the current business performance/business health is considered within the categories – and attitude to risk and finance*." (Participant 05) It was concluded that this related to ensuring ongoing review of risks over time, responding to business, legal and technology changes. Longevity – Contract Timeframe recognises that for longer contract terms there could be more exposure to risk from change, where business health and attitudes to risk could be more likely to change over time. Also of relevance is Maturity – Trust and Clarity, for example use of the Collaboration Standards Framework was considered to improve management of collaboration risks. The

Question	Responses
	Inputs can be periodically reviewed for change as Goals of Tolerable Risk and Value/Business Case could change over time. One other participant agreed that the categories were complete but "*Under 'Trust and Capabilities' it would be good to check that validity of IP Documents/clauses is checked*." (Participant 02) It was concluded that this was the case and validity checks were additionally supported by Tools with 'Clarity' considerations through 'Traceability' between 'Goals' and 'Accountabilities & Obligations' using 'Systems Methodology'. All agreed that the descriptions were clear with Participant 07 suggesting use of the terminology "Contract Term" rather than "Contract Length" and Participant 02 suggesting that "Maturity – Policy, Strategy & Management" and "Complexity – Structure & Incentives" may need supporting explanatory notes to aid application.
Q3 Risk Mitigation Categories: In your view are any Risk Mitigation Categories missing? In your view do the descriptions of Mitigation Categories adequately convey their meaning?	Supportive consensus for this area. Contextual comments provided views on an area of importance at the level below the category descriptors and enabled discussion and testing of the relationship between categories. For example, Participant 02 stated "*No major categories are missing but consider including subcategory of 'IP Ownership when Commissioning Digital Twins'. This could be considered within 'IP Protection & Licence Model'.*" This links to the

Question	Responses
	'Input-Viewpoint' - Life-Cycle Stage(s). Participant 07 also stated no category missing but provided some views on what they would like to see within the categories for example: *"Heads of Terms within 'IP Protection and Licence Model'… all agreements within 'Model Contracts & Insurance" …ensuring AI covered under 'Governance & Policy"*". Both Participant 07 and Participant 08 took an interest in 'Defined Stakeholder Types and Roles' seeking "*RACI model to clarify obligations"* (Participant 07), and stating "*Clarity of who is involved, what they do etc is important."* (Participant 08). This relates to the IP Risk Influencers 'Clarity – Accountabilities & Obligations' and 'Complexity – Stakeholders Map of IP Owners, Users & Governance.' Relating to the descriptors, Participant 07 suggested adding the word 'Governance' to 'Generic Assurance Model' to become 'Generic Governance & Assurance Model'. It was noted that the legal participants tended to query the meaning of the term 'standard system architecture' but understood with explanation and did not suggest alternative wording. For now, this is retained and highlighted the need for a glossary to clarify the meaning of the terms in the context of the Risk Framework.
Q4 Relationship between: Risk Influencers, Mitigation Tools and "Context & Purpose" In your view are there any relationships between Tools,	Consensus was not required for this question as it was looking for perception of equality of importance or whether certain scenarios were a particular concern. 60% responded 'Yes' and 40% responded 'No'.

Question	Responses
Context & Purpose and Risk Influencers that are particularly important?	Of those that responded 'No' (Participants 03, 06, 07, 10), three out of the four were legal experts. An example of explanations for the response included "*Depends where you are in the supply chain – could all be equally important with application identifying some more important than others*." (Participant 03) "*All important but perhaps Insurance will be particularly important due to the financial risks from e.g. Intellectual Property infringement and pursuing remedy.*" (Participant 06) "*All important because all categories are intertwined. For example, by way of illustration, within a business it is easy to implement IP risk management at board and management level but training at employee level is equally important (linking policy, structure, stakeholders, capabilities etc).*" (Participant 10) For participants responding 'yes' the threads of importance were: • Clarity of the business case and how it and incentives align with and transfer to each stakeholder (Participants 05, 08, 09) • Clarity of accountabilities and obligations (Participant 04), • Maturity: some categories currently better understood and managed than others: current areas of importance – IP ownership and definition and clarity of roles and obligations. (Participant 08) • Insurance to protect against damages particularly important, together with the legal, financial and insurance stakeholder roles

Question	Responses
	(Participants 01, 04, also mentioned by Participant 06) • Legal validity of agreements between stakeholders (Participant 02) • Lifecycle consideration (Input) and how it relates to technology and maturity changes over time (Challenge of legislators/policy lagging behind) (Participant 09)
Q5 Relationship between Risk Frameworks (Risk, Safety, Security) The research suggests a framework for IP risk management sits within the existing risk standards framework as shown. To what extent do you agree?	There were positive responses from 80% of Participants with two of the Technical Participants selecting "Neither Agree nor Disagree" which was due to them not claiming to be familiar enough with the content of all the standards identified. For example, Participant 02 stated "*Agree with the overlap and that IP has some of its own controls and mitigations*." Participant 01 responded similarly. Several participants identified the importance of standards to provide common understanding to "*avoid "chaos""* (Participant 03) and agreed that "*IP risk is something that needs to be considered together with other risk management streams rather than standalone. There will always be some elements of IP risk that need to be considered separately*." (Participant 10) with *"..the vast majority sit within the overall risk management circle but may be references to the security and safety risk standards as well*." (Participant 04)
Q6 Application of the Framework – Risk Management Assurance	All agreed or strongly agreed. (50% Agree, 50% Strongly Agree)

Question	Responses
To what extent do you agree with the following statement: "This conceptual framework could be used as the basis, and developed, to assure that IP risks are managed to support use of Digital Twins for Life-Cycle Decision Support ..."	Examples responses included: "*I think it successfully helps the visibility of an assurance case*." (Participant 07) "*It provides a helpful structure to prompt the right questions to be asked to make sure there are responses to those questions…The framework will provide the start. The next level of detail is needed which requires the right level of expertise within the stakeholder groups.* " (Participant 09)
Q7 Application of the Framework – Compare Options To what extent do you agree with the following statement: "This conceptual framework could be used as the basis to compare relative risk between options."	All agreed or strongly agreed. (40% Agree, 60% Strongly Agree) Comments additionally highlighted the following issues of importance: • Experience and capability of those scoring (Participants 01, 08, 09) • Weighting of score for appropriate solution selection (Participant 10) • Ability to stimulate discussion (early) to reduce risk (Participants 02, 04, 05)

Table 15: Expert Evaluation Results

The expert review enabled the structure of the framework (Figure 11), including categories and sub-categories, to be fixed, so that the hypotheses H2 and H3 could be further evaluated through the case study application.

7.3 Case Study Application

7.3.1 Introduction

The case evaluation associated with each hypothesis is outlined in Table 16:

Hypothesis	Evaluation
H2 – The described Framework explains how Intellectual Property Risks potentially impact multi-stakeholder collaboration using Digital Twins for life-cycle decision support.	For each Case Study: 1. Define the Goals, Business and IP Context. 2. Identify example Viewpoints 3. Use the framework to explain how IP risks could impact collaboration.
H3 – Application of the Framework could mitigate risks to the achievement of multi-stakeholder collaboration using Digital Twins for life-cycle decision support.	4. Apply the framework to explore how it can be used to mitigate example IP risks.

Table 16: Case Study Evaluation Approach

7.3.2 Case Study 1: HVAC MaaS within upgraded Class 444/450 for South Western Railway

Overview

Sources such as Ebert (2021), identify that the Class 444 Trains were built by Siemens Transportation Systems (Austria) between 2002 and 2004. The design is based on Siemens' Desiro platform and is an electric multiple unit comprising five cars. The trains are maintained at Northam depot initially for the train operator South West Trains and now for South Western Railway. Similarly, the Class 450 Trains were supplied by Siemens, based on their Desiro platform and are also operated by South Western Railway from Waterloo. In 2021 Knorr Bremse contracted with Siemens Mobility for provision of upgraded HVAC systems for the Class 444s and Class 450s for South Western Railway and digital MaaS of those HVAC through the Siemens Railigent® open maintenance platform. Although not described as a Digital Twin, it includes a digital representation of HVAC parameters, received from connected physical sensors and uses smart data analytics to determine when maintenance is required. The system is expected to reduce fleet maintenance costs and train energy consumption and control the flow of fresh air to the passenger more precisely. The evaluation steps are outlined as follows. Assumptions are stated where specifics of contracts and data exchange are not known.

Step 1: Define the Goals, Business and IP Context

This used the Goals & Context parts of the framework to capture essential information for risk assessment and management. The information relating to this Case Study is captured from Business internet sources, with additional information about the Siemens DT architecture from the LeMo report (Teoh *et al.*, 2019).

Goals	
DT Purpose, Need, Requirement	Condition monitoring, 'maintenance need prediction' and actions to deliver contracted MaaS for South Western Railway upgraded fleets for: • Train fleet (Siemens) • HVAC supplied to Siemens and fitted to train fleet (Knorr-Bremse)
Value, Business Case	Efficient and effective delivery of MaaS contract avoiding cost of any failures to deliver performance. Knorr-Bremse: • Proprietary HVAC IP Value retained, • Operational Data to inform future HVAC IP. Siemens: • Proprietary Class 444/450 IP Value retained. • Effective integration of Class 444/450 sub-systems from supplier's IP to achieve operational contracts. South Western Railway: Train operations with MaaS delivered to agreed performance.

	For this example, potential value in Operational Data that can be combined with other datasets for other decision support purposes is not considered as there is insufficient insight on this within the online sources.
Tolerable Risk	Not explicitly stated so assume: Delivery of Service Contract for Contract Period without Incurring Damages.
Context	
Business Context	
Geographic Scope	UK (MaaS delivered) UK & Germany (DT Platform & Data Store)
Application Sector	Rail
Enabling Technology & Tools	Siemens Railigent® Predictive Maintenance Service Platform with Data Analytics using AWS platform services, built on top of Siemens MindSphere®, cloud based, IoT operating system and secured data-lake. Sensors for process data, diagnostic and log messages, some potentially with edge processing. Secured Data Communications (AWS used by Siemens and JSON file format for storage and MQTT for data transfer protocol) Software languages: Python, pySpark and R.
IP Context	
IP Inventory (Owned and Used)	Siemens Owned: Railigent® and MindSphere® Siemens Used: AWS Platform Services, Data Format and Encryption Standards applied to electronic-design IP. AI Algorithms may be from 3rd Parties.

	Knorr-Bremse Owned: HVAC Design Data, HVAC Operational Data (assumed but not clear from Internet sources) Knorr-Bremse Used: Unknown – could be additional data-sets. *South Western Railway's IP ownership and use not considered for this example.*
Existing IP Protection and Licensing Policies	Siemens – commentary on the general approach to IP in the public domain suggests a value-driven IP strategy which aims for a quality assessed patent portfolio measured and tracked through a tool called "Patent Asset Index provided by PatentSight®", with IP specialists proactively involved in innovation processes. LexisNexis (2024) Knorr-Bremse – to secure and safeguard high quality IP
Legal, Financial and Insurance Stakeholders	Not considered for this Case Study, although Step 2 illustrates the stakeholder that financed the fleet of trains (ROSCO) and bought them from the manufacturer.

Table 17: Case Study 1 – Step 1

Step 2: Identify example Viewpoints

Stakeholders	• Siemens – Train Designer & Manufacturer, MaaS contract with Train Operator • Knorr-Bremse – HVAC Designer & Manufacturer, MaaS subcontractor • South Western Railway – TOC
Life-Cycle Stage	• Operations
Contract	• MaaS Interfaces (See Figure 16)

Table 18: Case Study 1 – Step 2

The Stakeholder viewpoints and Contract interfaces considered in this case study are illustrated in green in Figure 18. The ROSCO finances the purchase of the trains and their upgrade and maintenance and has a long term interest in their asset value.

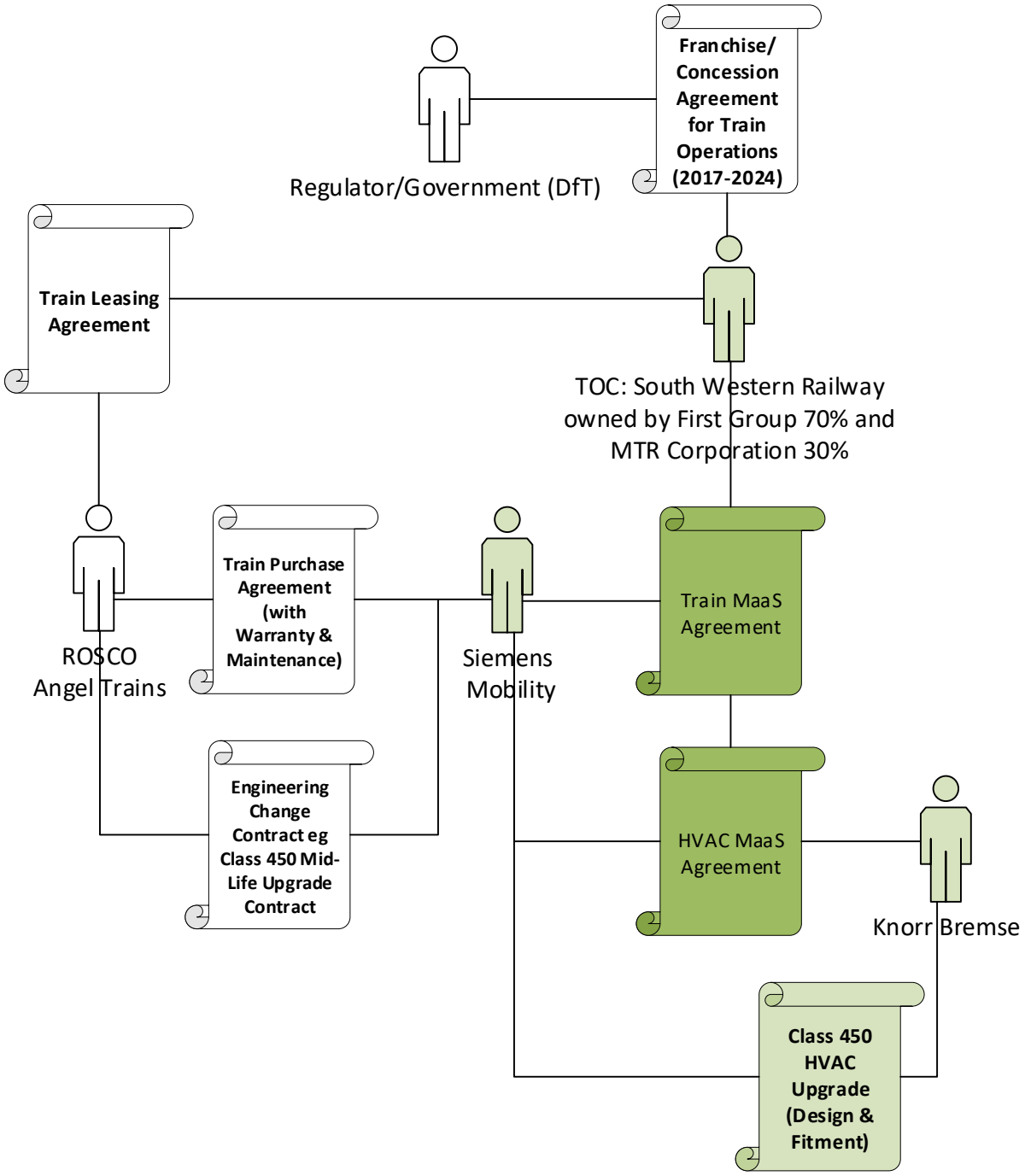


Figure 18 – Class 450 MaaS Contract Interfaces

Step 3: Use the framework to explain how example IP risks could impact collaboration

As this is an established contract relationship the collaboration initiation failure due to an owner of proprietary data perceiving an unacceptable risk of data breach will not be considered. Instead the example considered is as follows:

Hazard: HVAC IP valued by Knorr-Bremse is essential for achieving the MaaS through DT

Top Event(s): IP Infringement or Data Exploitation

Consequences: The consequences can be directly financial, reputational or a failure of purpose. For example, a breach of HVAC IP for Knorr-Bremse could de-value their IP and result in costs of IP dispute and defence. For Siemens, requiring the data to go through their Railigent® platform and IP infringement of data exploitation relating to HVAC IP could impact their reputation and they could incur costs of dispute and defence. The TOC will also experience failure or adverse impact on their MaaS through any dispute which causes the collaboration to fail.

The potential causes can be broadly categorised into:

- Accidental IP Infringement or Data Exploitation
- Deliberate or Reckless IP Infringement or Data Exploitation

Generally, the bow-tie or similar approaches can be used to map the path to the potential cause, through to the top event and through to the consequences. The Risk Influencers can interact with this chain and will be considered in relation to the case study to identify whether they provide explanation as to how IP risks could potentially impact collaboration in this case.

Risk Influencers	**Example Case Study IP Risk Indicators for collaboration impact**
Maturity	**Lower Risk Indicators** ***Policy, Strategy & Management*** MaaS approach provides opportunity for Knorr-Bremse and Siemens to control their own risks and focus on the essential data to share to achieve the service, although the specifics of the contracts are not

Risk Influencers	Example Case Study IP Risk Indicators for collaboration impact
	available to explore whether there is any imbalance in risk for each party. Both Siemens and Knorr-Bremse have IP Policies based on IP value although there is insufficient information in the public domain to assess the balance of maturity of compatibility. ***Trust, Competency & Capabilities*** Reflecting on the balance of trust, competency and capabilities relating to IP, DT and systems thinking between the collaborating parties. Knorr-Bremse provide competency relating to their HVAC. Siemens control the DT infrastructure and associated subcontractors which puts them in a dominant position which potentially increases the risk for Knorr-Bremse but Siemens are actively involved in Digital Maturity and Security initiatives perceived as mature, such as the Mindsphere® Security Model (Siemens, 2018) which includes a governance approach and applied expertise, security standards compliance (including BS EN ISO 27001 (British Standards Institution, 2023a)) and security architecture covering users, third party developers and providers. The publicly available literature suggests that Siemens intend to reassure users of their systems that their data is protected. As such risk of accidental breaches is perceived as controlled. **Higher Risk Indicators** ***Governance, Culture & Leadership*** Although there is a mature regulatory framework for rail safety and interoperability in the UK and EU (for example 'Council Directive 2016/798' (2016)), the Rail Sector Governance, Culture and Leadership to support and incentivise long term collaboration, and governance of data specifically related to DT applications and AI use

Risk Influencers	Example Case Study IP Risk Indicators for collaboration impact
	which mitigates IP risk, is not yet visibly mature. Arguably the regulatory framework for product safety through engineering change introduces further stakeholders such as Notified Bodies/UK Market Conformity Assessment Bodies to increase complexity and potential exposure to sources of IP infringement and data exploitation risk. As identified, Siemens have relatively mature governance and are reassuring users of their platform that they are managing the data and supply chain responsibly. However the absence of sector level governance to provide further reassurance to monitor general opportunism risk and trust changes over time, is a risk that could perhaps be better mitigated. ***Trust, Competency & Capabilities*** Although there are lower risk indications as identified, there are also higher risk indications which may require further mitigation. Siemens are managing the data through Railigent® and their 3rd parties and so need to have a mature supplier management framework with trust, competency and governance in their supply chain to avoid accidental, careless or deliberate misuse of data, such as by AI developers. Knorr-Bremse are dependent on Siemens diligence and competency in managing their supply chain. There may however be more they can do to ensure they are not sharing more than they need to achieve the Purpose based on an assessment of risk.
Clarity	Review of Clarity is limited to the information available in the public domain. **Lower Risk Indicators** ***Standards and Legal Environment*** Use of risk framework standards for security such as BS EN ISO 27001 (British Standards Institution, 2023a).

Risk Influencers	Example Case Study IP Risk Indicators for collaboration impact
	Use of collaboration and legal risk frameworks which will ensure risk of breach and exploitation at the end of contract is covered by obligations and checks would also be indicative of lower risk. ***Traceability*** Use of systems engineering frameworks. Siemens drives forward the use of tools such as SysML for traceability in product development and plans to extend management of the digital thread into operations and maintenance (Lionel, 2023) and so has the potential to extend this traceability to IP risk aspects from owned and licenced IP, via the Physical Entity Architecture through to Obligations and Contracts. Use of Tools such as standard architectures, stakeholder types and systems traceability linking need through solution to obligations and contracts could further indicate lower risk. While standard security architecture is evident the application architecture and traceability to obligations and contracts is not visible in the public domain. **Higher Risk Indicators** ***Traceability*** Higher risk would be indicated if the sharing, ownership, access to and use of collected operational data from sensors and software algorithms during the timeframe of MaaS is not clear. Traceability from Purposes from each stakeholder to the data generated and related obligations in contracts would indicate lower risk.

Risk Influencers	Example Case Study IP Risk Indicators for collaboration impact
Complexity	**Lower Risk Indicators** ***System Complexity*** MaaS allows the manufacturer to take more control over their data and reduces the number of stakeholders and 3rd parties interacting with data relating to valued IP. They have more control over their system architecture and can provide essential information, such as alerts, relevant to the purpose rather than detailed data that could provide information about their proprietary IP. The geography of system architecture, data storage location is potentially simplified through containment within Europe which limits complexity of regulation and remedies, although this would need to be confirmed. **Higher Risk Indicators** ***Stakeholder Map of IP Owners, Users & Governance*** The structure between ROSCO, TOC and Siemens, in particular, is complex, with Siemens in control of operational data from all systems and needs to ensure the risk of exploitation of data of relevance to these stakeholders and Knorr-Bremse is managed to avoid future dispute. It is not clear that there are sector incentives for avoiding future exploitation risk and supporting resolution if such were to occur. Siemens is in a dominant position in the collaboration, controlling data collection, storage and analysis. The complexity of the 3rd Party supply through Railigent®, including cloud services and AI services is not clear but is within Siemens control.
Longevity	**Lower Risk Indicators**

Risk Influencers	Example Case Study IP Risk Indicators for collaboration impact
	Contract Length and Timeframe Assuming the MaaS is limited to the period of contracted TOC operation this is a relatively short contract period for Knorr-Bremse which can limit exposure to risk and amount of data provided which provides other parties with information about their HVAC behaviour. **Higher Risk Indicators** ***Physical Entity Life Timeframe*** The remaining life of the Class 444 trains extends beyond the MaaS for the stated TOC. The ROSCO as owner and financier may retain contractual connections with Siemens for longer. This provides more time for the balance of business risk between stakeholders to change with operational data of particular importance to the ROSCO in later life whereas the importance of proprietary designs may potentially be of less value to Siemens with the passage of time. The specifics will need to be reflected by each stakeholder.

Table 19: Case Study 1 – Step 3

Step 4: Apply the framework to explore mitigation of the example IP risks

Appendix 8 identifies an example risk bow-tie relating to accidental or deliberate IP infringement causing failure of collaboration together with the architecture for this Case Study. This step develops example areas identified in Step 3 as indicators of higher risk and explores how Risk Management Tools can be applied to reduce these risks. These are summarised as:

IP Risk Influencer	Risk(s)	Example Risk Management Tools
Maturity	Imbalance in IP control due to single stakeholder management of DT	**Governance & Policy** ***Policies and Standards*** – Sector to require application of the

IP Risk Influencer	Risk(s)	Example Risk Management Tools
	Infrastructure and Operational Data AND Under-developed sector governance and incentives for long term collaboration	standard Collaboration, Risk, Security and Systems Frameworks. Sector defined architecture standards and structures which include mitigations relevant to the sector use cases such as protection for sub-system suppliers from sharing unprotected IP unnecessarily. Includes defining data types needed for the use case over the life of the Physical Entity. ***Sector Audit and Accreditation Schemes*** – Audit management of IP through the supply chain and Accredit AI developers for their responsibilities with supplier data. **Technical** ***IP Tracking and Cyber-Security Controls*** together with ***Generic System Architecture & Interfaces*** – Architecture which protects high value IP such as design data through supplier's own storage controls and cyber-protections. Use of edge

IP Risk Influencer	Risk(s)	Example Risk Management Tools
		computing before integration of data for the Purpose.
Clarity	Unclear operational and predictive data ownership, sharing and access.	**Technical** ***Systems Methodology*** – Tracing Purpose through Architecture to data created, value case, obligations and to contracts. ***Governance & Policy*** – Generic Assurance Model – Case that assures this clarity as part of collaboration risk assurance. For a future contract the Tools can be combined as a set and for suppliers to multiple rolling stock manufacturers the sector could develop this integrated toolset. For example: ***Generic System Architecture and Interfaces*** – A sector generic rolling stock Digital Twin Architecture will assist identify the data threads for the Purpose to support traceability to obligations and contracts and facilitate suppliers providing smart assets to various manufacturers with an

IP Risk Influencer	Risk(s)	Example Risk Management Tools
		architecture that mitigates their own risk. **Legal** ***Model Contracts and Insurance*** – which could potentially be developed at sector level by linking ***Business-Defined Stakeholder Types & Roles*** with the ***Generic System Architecture + Interfaces*** to ensure accountabilities and obligations are captured. **Business** ***Generic Risk & Mitigation Options*** - New types of business models are emerging and can be developed by sectors. For example, Data-as-a-Service identified by both Siemens advertising this type of contract through Railigent X (Siemens, 2024) and Utilities companies considering such contracts for Digital Twin (Cahn *et al.,* 2023). Such will need to show traceability to the Technical and Business tools and Generic Risk set to ensure clarity which may

IP Risk Influencer	Risk(s)	Example Risk Management Tools
		assist in mitigating the data ownership and data security concerns cited as barriers to adoption of DaaS by Cahn *et al.,* 2023.

Table 20: Case Study 1 – Step 4

This case illustrated that considering IP risk by relating the Goals & Context to IP Risk Influencers can provide an indication of how IP Risk could impact a particular collaboration and how the tools could be developed to mitigate risk. This case identified that the manufacturer and system integrator had developed the Digital Twin which enabled them to control their risk in particular. From the perspective of the sub-system supplier providing HVAC systems to multiple manufacturers, perhaps they could check that they are controlling the data submitted to achieve the maintenance need and that the sector could provide more external protection to mitigate risk to the TOC and ROSCO by providing further incentives to maintain collaboration in case of a future change of business risk for one of the collaborators.

7.3.3 Case Study 2: Class 345 Fleet Maintenance for Crossrail

Overview

The Class 345 Aventra trains for Crossrail (Elizabeth Line), which runs west to east across London are manufactured and maintained by Alstom (formerly Bombardier) and operated by MTR Elizabeth Line a subsidiary of MTR Corporation (Crossrail) Ltd under contract to Transport for London (Crossrail, 2022). The financing of these trains is complex, with Transport for London procuring the trains from Bombardier (now Alstom) for an initial £1bn with the European Investment Bank providing a loan to Transport for London of £500m (Railway Gazette International, 2013). In March 2019 Transport for London sold and leased back the order (20 year lease back for £1bn) from 345 Rail Leasing which is a consortium of Equitix Investment Management Ltd, NatWest and SMBC Leasing. (Rail, 2019)

Alstom operate the main maintenance depot at Old Oak Common as part of a 32 year construction and maintenance contract awarded in 2014. The maintenance utilises the train manufacturer's Automatic Vehicle Inspection System (AVIS) which includes brake, wheel and pantograph checks to provide an up to date view of asset condition to support maintenance (Rail Engineer, 2018). The health of on-train systems is sent through to Bombardier's Orbita System which provides the Digital Twin for the train systems health. Alstom are currently developing a HealthHub™ which converges Orbita with Alstom's existing HealthHub™ (Alstom, 2022). The focus of this case study is the relationship between stakeholders providing and using the Digital Twin of the Class 345 through the original Orbita (Provost, 2010), while anticipating there will be a future upgrade to HealthHub™.

Step 1: Define the Goals, Business and IP Context

From the available sources in the public domain the goals and context are as follows:

Goals	
DT Purpose, Need, Requirement	Condition monitoring and maintenance need prediction and actions to deliver contracted maintenance service for Class 345 trains for MTR Elizabeth Line (Operator).
Value, Business Case	Efficient and effective delivery of Maintenance contract avoiding cost of any failures to deliver contracted performance (Alstom). • Proprietary Class 345 IP Value retained. • Effective integration of Class 345 sub-systems from supplier's IP to achieve operational performance contract. MTR Corporation: • Train operations to agreed performance and value for money.

Tolerable Risk	Not explicitly stated so assume: Delivery of Service Contract for Contract Period without Incurring Damages.
Context	
Business Context	
Geographic Scope	UK (Maintenance delivered) UK and France (DT Platform & Data Store). The original Orbita system was networked to other control centres to include in Switzerland, Germany, Australia and North America (Provost, 2010).
Application Sector	Rail
Enabling Technology & Tools	See IP Inventory. Due to the acquisition of Bombardier by Alstom the legacy Orbita system will be converged with Alstom's HealthHub™.
IP Context	
IP Inventory (Owned and Used)	Alstom (formerly Bombardier) Owned: Orbita, HealthHub™ Alstom Used: Not available. *MTR Corporation and Transport for London are potential users of the Alstom system to support operations but this is not considered in detail as the contracts are not in the public domain.*
Existing IP Protection and Licensing Policies	Alstom – to secure valued IP
Legal, Financial and Insurance Stakeholders	Complex financial ownership of the Class 345 fleet.

Table 21: Case Study 2 – Step 1

Step 2: Identify Example Viewpoints

Stakeholders	• Alstom – Train Designer & Manufacturer (assuming titles to IP assets acquired through

	acquisition), Maintenance Contract with Train Operator • MTC Corporation – TOC • Transport for London – Class 345 Lease Holder • 345 Leasing – Class 345 fleet owner
Life-Cycle Stage	• Operations
Contract	Not considered for this Case Study

Table 22: Case Study 2 – Step 2

Step 3: Use the framework to explain how example IP risks could impact collaboration

The example considered for this case study is:

Hazard: Sensor data collated prior to March 2019 (trains sold) essential for achieving the maintenance service.

Top Event: Data Exploitation

Consequence: Dispute causing potential failure of Purpose and financial impact to resolve.

Potential causes: Accidental or Deliberate Data Exploitation

Risk Influencers	**Example Case Study IP Risk Indicators for collaboration impact**
Maturity	Not considered for this case study.
Clarity	**High Risk Indicators** Without visibility of the contracts this cannot be assessed with certainty. However without ***Traceability*** of data ownership, sharing and use agreement together with IP used and conditions of use, during the various changes of ownership of fleet owner and maintenance provider and subsequent potential migration of data between systems, together with insufficient clarity of data ***Accountabilities and Obligations***, there is risk of older data used out of agreement or

	carelessly handled. However, the risk will depend on the value of this data for the Purpose for the current maintainer and operator. **Lower Risk Indicators** Asset Register links to all IP records and supply chain licences and with the changes these are assessed for impact and change actions followed through.
Complexity	**Higher Risk Indicators** ***Stakeholders Map of IP Owners, Users & Governance*** The changes to fleet owner and manufacturer/maintainer will add complexity to the map of IP Owners and Users. The Bombardier supply chain contributing data may include suppliers that are not on the preferred supplier list for Alstom.
Longevity	***Contract Length Timeframe*** The maintenance contract is for 32 years which increases exposure to fluctuations in business risk attitude within the stakeholder collaboration and further significant changes of ownership and changes within the supply chain

Table 23: Case Study 2 – Step 3

Step 4: Apply the framework to explore mitigation of the example IP risks

This step develops example areas identified in Step 3 as indicators of higher risk and explores how Risk Management Tools could have been applied to reduce these risks. These are summarised as:

IP Risk Influencer	Risk(s) leading to: Data Exploitation	Example Risk Management Tools
Clarity	Unclear ownership and rights AND Changing map of IP owners and users	**Governance & Policy**

IP Risk Influencer	Risk(s) leading to: Data Exploitation	Example Risk Management Tools
Complexity Longevity	with different attitude to IP risk over time.	TfL could establish ***Policy & Standards*** for maintaining ongoing use of data that underpins the Purpose and provides rules for ownership and managing change and this would include ***Sector Audit & Accreditation*** covering the life of the Physical Entity contract to monitor compliance and changing risk profile. [The **Business** – ***Defined Stakeholder Types and Roles*** and **Technical** – ***Generic Architecture & Interface***s can assist develop these by providing clarity of obligations and impacted areas in a change.] AND **Legal** ***IP Protection and Licence Model*** which clarifies ownership, licence rules and value of various data to support change impact assessment. AND **Technical**

IP Risk Influencer	Risk(s) leading to: Data Exploitation	Example Risk Management Tools
		IP Tracking & Cyber-Security Controls with traceability from *Systems Methodology* linking to the *Generic System Architecture & Interfaces* to enable change impact to be assessed and related to the actual architecture to manage mitigation of risk in migration to the new architecture.

Table 24: Case Study 2 – Step 4

7.3.4 Case Study 3: Deutsche Bahn Digital Twin

Overview

In May 2021 Stadler and state owned rail company Deutsche Bahn (DB) declared that they had created the first complete Digital Twin of a train fleet with their virtual representation of DB's Flirt fleet 429.1 series in Germany which run regional train services in the Rhineland-Palatinate region. (Fender, 2021) The Digital Twin is intended to initially focus on the physical (including electrics and software) behaviour of the train's air conditioning, doors and wheelsets and is intended to increase fleet reliability and enable predictive maintenance.

The specifics of the contracts between DB and Stadler, especially relating to data sharing and the Digital Twin infrastructure, including data storage are not currently publicised. However, there are journal papers discussing DBs transition to a digital railway and the architecture it is adopting to implement this which includes digitising the infrastructure too. In particular DB has created a company for digitisation of the railway in Germany called Digitale Schiene Deutschland GmbH (DSD) and this is using NVIDIA Omniverse™ for the Digital Twin of its infrastructure network and associated services which will connect datasets shared from other suppliers such as from the train manufacturers. (Geyer, 2022). DSD set up their Data Factory project in 2022 (Digital Schieme Deutschland, 2024) and there are considerations for

creating a pan-European Data Factory for which a report has been created, co-funded by HaDEA to consider the feasibility (Neumaier *et al*, 2023). This includes a short section considering the legal and regulatory aspects, citing laws governing sensitive data, identifying the need for regulatory audits and contractual enforcement and the need for cyber-security controls to include consideration of standard risk frameworks, such as BS EN ISO 27001 (British Standards Institution, 2023a).

Step 1: Define the Goals, Business and IP Context

From the available sources in the public domain the goals and context are as follows:

Goals	
DT Purpose, Need, Requirement	Predictive maintenance. (DB and Stadler)
Value, Business Case	Increase the economic efficiency and availability of the trains and improve service performance for customers. (DB and Stadler in collaboration) IP Value (Stadler): • Proprietary Flirt IP Value retained. • Effective integration of Flirt sub-systems from OEM's IP (Stadler suppliers) to achieve the performance contract.
Tolerable Risk	Not explicitly stated so assume: Delivery of Service to agreed performance, for Contract Period without Incurring Damages nor Reputation Loss.
Context	
Business Context	
Geographic Scope	Germany (Maintenance delivered) Switzerland (Manufacturer)
Application Sector	Rail

Enabling Technology & Tools	Not explicitly stated so assuming using DSD used tools such as: NVIDIA Omniverse™ Platform of Services and APIs for enabling integration of OpenUSD and RTX rendering with other software simulation tools and tools for the development of AI.
IP Context	
IP Inventory (Owned and Used)	Examples include: • Stadler Owned and DB Used: Flirt Rolling Stock Design and Manufacture IP, with Stadler managing supply chain IP contributing to Flirt. • NVIDIA Owned and DB Used: Digital Twin enabling technology. • DB and Stadler Owned and Used (Specifics of contract unknown): Operational Data • DB Owned and Managed: Environment and Interface Data (e.g. Infrastructure) Through DBs Digital Subsidiary, DSD, there are several projects to include a "Data Factory" established in 2022 which contains sensor data from the infrastructure and trains, used to train AI. It is intended to enable data sharing with various stakeholders to include operators, manufacturers and suppliers of AI services. (Digitale Schiene Deutschland, 2024)
Existing IP Protection and Licensing Policies	DB values and protects IP. https://goodip.io/iq/assignee/deutsche-bahn-ag [Accessed 24/05/2024]. Stadler values and protects IP. https://goodip.io/iq/assignee/stadler-rail-ag [Accessed 24/05/2024]

Legal, Financial and Insurance Stakeholders	DB is a state owned enterprise controlled by the German government and DSD is a subsidiary for implementing the rail sector's Digital Rail in Germany. DSD is seeking co-development partnerships to create 'open platforms' rather than "classic client-contractor relationships." (Digital Schiene Deutschland, 2024) It lists current partners which include several rolling stock manufacturers: CAF, Hitachi, Alstom, Siemens but Stadler is not listed. It is assumed that DB are seeking to build on the Digital Factory for all Digital Twin implementations.

Table 25: Case Study 3 – Step 1

Step 2: Identify Example Viewpoints

Stakeholders	Stadler - Train Designer & Manufacturer DB – Train and Infrastructure Operator
Life-Cycle Stage	Operation and Maintenance
Contract	Not considered as visibility of the contract specifics is not publicly available.

Table 26: Case Study 3 – Step 2

Step 3: Use the framework to explain how example IP risks could impact collaboration

The specifics of the data architecture, from Stadler's perspective, is not in the public domain, nor whether the Digital Twin data is within Stadler's direct control or is managed through the DSD Data Centre. Assuming that there is a degree of data sharing with the DSD Data Centre the example considered is:

Hazard: Flirt IP valued by Stadler is essential for developing AI tools used through the DT for Predictive Maintenance

Top Event(s): IP Infringement

Consequences: The consequences can be directly financial, reputational or a failure of purpose. For example, a breach of IP for Stadler could de-value their IP and result in costs of IP dispute and defence. For DB, a dispute could impact achievement of Purpose and financial impact.

The potential causes can be broadly categorised into:

- Accidental IP Infringement
- Reckless IP Infringement
- Deliberate IP Infringement

Risk Influencers	**Example Case Study IP Risk Indicators for collaboration impact**
Maturity	**Low Risk Indicators** ***Policy, Strategy and Management*** DB has a strategy for Digital Twin across the rail sector in Germany and is developing collaborative relationships with multiple suppliers and using standard architectures and interfaces which will facilitate identification of risk. For example, they are developing a Germany located Data Centre to facilitate control and Clarity and adopting standard architectures to facilitate interoperability. They are also involved in European projects to explore Data Centre issues which is expected to include consideration of handling of shared and sensitive (includes IP) data. (Neumaier *et al.*, 2023). **Mix of Low and High Risk Indicators** ***Governance, Culture & Leadership*** Although digital governance across the European Rail Sector is still maturing and currently relatively low (Lis *et al.*, 2023), this Case Study provides some lower risk indications compared to the other Case Studies.

	DB as end user is state-owned and works with all suppliers and provides sector leadership. The culture is to support open data but there is recognition that there is sensitive data that relates to IP (Neumaier *et al.*, 2023). Development of external government and DB governance will need to ensure equitable influence of competitors in developing the collaborative DT solution, which it is assumed Stadler is required to use, to ensure it is in all manufacturers' interests. Related to this, DB may value ensuring a range of manufacturers are comfortable in engaging to ensure ongoing competition and value. Governance is related to Trust and low risk indicators could include the establishment of accreditation of 3rd Party Suppliers for AI training and technical and legal governance of sensitive data. **High Risk Indicators** ***Trust, Competency & Capabilities*** Trust – DB operates fleets from different manufacturers and as the owner of DSD has most influence over its development, architecture and use. Stadler will need to be assured of the Technical and Contractual protections in place for sensitive data threads that reveal IP relating to the Flirt platform specifically protections to ensure they are adhered to. This will require understanding of the competency and capabilities needed for engaging with sensitive data to include widespread understanding of the consequences for inadequate handling of sensitive data through an organisation. The DSD partnership includes competitors and where 3rd parties are involved in training AI, the governance of this may be via DB rather than Stadler. There could be imbalances in competency and capability relating to IP awareness and how this relates to risk for Stadler which requires low risk Clarity, specifically the support of a Systems Approach to identify the types of sensitive data of value to manufacturers and trace to architecture and obligations to protect it.

	Neumaier *et al.*, 2023, identify that the EU Data Centre will recognise the role of "Data Provider" which will have data sovereignty and control access to their data. However, such a role may not have direct control over the DT infrastructure and may be relying on specific 3rd party competencies and technical capabilities to manage risk.
Clarity	Not considered in this case study as the specifics of contracts are not in the public domain.
Complexity	**Low Risk Indicators** As DB is a state-owned Operator, leading delivery of the overall Purpose and with direct contract with manufacturers and other stakeholders this reduces complexity in the following areas: ***Stakeholders Map of IP Owners, Users & Governance*** While the governance structure for DSD is not considered in detail, there is a clear list of partners which should facilitate mapping of IP owners, users and licence conditions and there is the potential to minimise the number of contract interfaces and geography for the Purpose especially as this relates to regional rail services and not International cross EU services. Neumaier *et al*, 2023 also identify consortium roles ranging from financial contributors to contributors of tools and computing power. However, this is not a complete stakeholder map as it does not refer to the range of governance roles. This could link to Risk Management Tools for Defined Stakeholder Types and Roles to ensure coverage of roles. The risk will increase for a high number of 3rd party suppliers contributing to the Digital or Physical Twin. ***Structure & Incentives***

	DB, as state-owned operator, is incentivised to deliver a Purpose that is of benefit to the end-users. The direct relationship between operator and Stadler, as provider of the trains, suggests potential for facilitating incentive for Stadler to collaborate. The specifics of the contracts are however, not in the public domain. ***System Complexity*** The focus is a specific fleet of trains and limited subsystems within those trains operating in a specific geographical area. Assuming the DB Data Centre is used, this is located within the same geographical area. The overall system will still have some complexities and challenges for example location, interface and security of 'Touchpoints' for downloading data to the Data Centre, which will have particular IP risk.
Longevity	Not considered in this case study as the specifics of contracts are not in the public domain.

Table 27: Case Study 3 – Step 3

Step 4: Apply the framework to explore mitigation of the example IP risks

This step develops example areas identified in Step 3 as indicators of higher risk and explores how Risk Management Tools can be applied to reduce these risks. These are summarised as:

IP Risk Influencer	**Risk(s) leading to: Reckless IP Infringement**	**Example Risk Management Tools**
Maturity	DB procured 3rd Party developer/trainer of AI for predicting door health enables a competitor to access Stadler sensitive data.	**Technical** Sensitive data - IP Tracking & Cyber-security controls Generic System Architecture & Interfaces – Data only accessed by authorised users through the

IP Risk Influencer	Risk(s) leading to: Reckless IP Infringement	Example Risk Management Tools
		data architecture and APIs for AI development. **Business** Generic Risk and Mitigation options – EN ISO 27001 (British Standards Institution, 2023a) procurement policy Defined Training & Qualifications – Ensure procurement teams and all handling data understand Sensitive Data and its governance. Ensure Systems training to trace Sensitive Data through the system activities. **Legal** Model Contracts and Insurance to include (examples): • Laws and regulations for privacy, cybersecurity • Clarity of IP and licence conditions • Roles and obligations • Accountabilities for the movement of data, ownership and management of risk

IP Risk Influencer	Risk(s) leading to: Reckless IP Infringement	Example Risk Management Tools
		• Managing Changes • Remedies for breach

Table 28: Case Study 3 – Step 4

7.3.5 Case Study Application Summary

From the perspective of three case studies supporting rolling stock maintenance decision support, the Framework was able to explain how IP risks could potentially impact multi-stakeholder collaboration and supported identification of particular areas of risk exposure in each case. This contributed to providing support for H2.

Case 1 highlighted complexities of stakeholder relationships illustrating an issue that had emerged from the initial data collection of the different incentives to share and potential for changing value in IP over time that could impact risk for the Physical Entity owner and financier. The control of data was with the OEM through Maintenance-as-a-Service. Case 2 further illustrated the risks from significant changes to company ownership where the relative risk tolerance between stakeholders could change and illustrating a need for clarity of obligations through the changes. Case 3 provided a less complex stakeholder structure with leadership from a state-owned operator, responsible to end-users for the performance of the maintenance and creating partnerships with suppliers such as OEMs to facilitate integration of data sources.

The Framework facilitated identification of Risk Management Tools to mitigate the particular risks in each case, contributing support for H3. For example, Case 3 illustrated the importance of governance in balancing commercial interests with overall Purpose.

7.4 Comparison with LeMo Report Findings

The Horizon 2020 project Leveraging Big Data for Managing Transport Operations (LeMo) included a report led by legal firm Bird & Bird (Debussche *et al.*, 2018), examining legal issues relating to use of data in the transport sector. Given that Digital Twin is associated with significant data threads it would be expected that any issues relating to IP would be reflected in the current study's constructed risk framework, supporting in part that Research Question 1 is answered, with the framework then providing further explanation as part of

answering Research Question 2 to support H2. This was checked as part of the evaluation with Table 29 summarising the data issues raised in the LeMo report (Debussche *et al.*, 2018) and how they are considered and taken forward in the risk framework.

LeMo Report Legal Issue	**Applicable to IP Risk (Yes/No)**	**Considered in IP Risk Framework**
Privacy and Data Protection	Yes	Yes For example: 'Goals & Context – Goals – Digital Twin Purpose, Need, Requirement' will identify the data types, characterisation and threads, ideally from application of a systematic process ('Tool – Technical – Systems Methodology') linked to the system solution which may use "Tools – Technical – IP Tracking & Cyber Security Controls and Generic System Architecture & Interfaces. The 'Business Context – Geographic Scope' identifies the applicable legal environment which relates to 'IP Risk Influencer – Clarity – Standards & Legal Environment' and the business environment to the 'Complexity – Stakeholders Map'. This then links stakeholders with consideration of 'Clarity-Accountabilities & Obligations' to 'Context – IP Inventory (Owned & Used). Applies to Trade Secrets as well as personal data.
Cyber-Security	Yes	Yes

LeMo Report Legal Issue	Applicable to IP Risk (Yes/No)	Considered in IP Risk Framework
		For example, 'Risk Management Tools – Technical – IP Tracking and Cyber-Security Controls' and 'Business – Defined Training & Qualifications' Risk Influencers include 'Clarity – Standards & Legal Environment' which will seek adoption of standards such as BS EN 27001 (British Standards Institution, 2023a) and traceability to 'Accountabilities & Obligations'
Breach-related Obligations	Yes	Yes For example, 'IP Risk Influencers – Clarity – Accountabilities & Obligations' and Risk Management Tools 'Legal – Model Contracts & Insurance''
Anonymisation/ Pseudonymisation	No	IP viewpoint is the focus, but the framework potentially allows consideration of related legal issues and could be extended. Privacy & Data Protection relating to the data types, characterisation and threads arising from 'Goals & Context – Goals – Digital Twin Purpose, Need, Requirement' are considered. IPR risk from all data types identified will require reflection from an IP risk perspective to mitigate misuse and exploitation. There is potential that data may be both considered

LeMo Report Legal Issue	Applicable to IP Risk (Yes/No)	Considered in IP Risk Framework
		important for protection against exploitation as well as needing anonymisation / pseudonymisation such as relates to a user of a system providing information about the system behaviour and performance, which has characteristics which could potentially identify of the user.
Supply of digital content and services – personal data as counter-performance	No	Not considered as the LeMo report is focussed on end-user/consumer data whereas the framework has focussed on business to business decision support even if this benefits an end consumer. However, the risk model could potentially be applied to this end-user stakeholder and developed further. Relates to 'Goals – Digital Twin Purpose, Need, Requirements' and 'Goals – Value/Business Case'.
Free flow of data The LeMo report clarifies that this relates to free flow of data across-geographic borders which is restricted by "data localisation requirements" such as the French Ministerial Circular which makes it illegal to use a non-sovereign cloud for	Yes	Yes The Risk Framework accommodates this with 'Goal&Context' considering 'Geographic Scope' and Risk Influencers 'Clarity – Standards & Legal Environment' linked to Tools such as 'Legal – Model Contracts & Insurance' and the 'Technical – Generic System Architecture & Interfaces' and 'Business – Generic Risk & Mitigation Options'.

LeMo Report Legal Issue	Applicable to IP Risk (Yes/No)	Considered in IP Risk Framework
data produced by public administration.		Tools such as 'Tool – Technical – Systems Methodology' enable traceability from constraints and requirements through to the Tools.
IP in big data environment • Copyright • Database Rights • Trade Secrets & Confidentiality	Yes	Yes Goals and IP Context clarifies the IP Inventory and Existing Protection and Licencing Policies, and the Geographic Scope relates to consideration of the international, national and legal frameworks as highlighted by LeMo. This then links to IP Risk Influencers which includes Clarity of the Standards & Legal Environment and Risk Management Tools: Regulatory Framework. Risk Management Tools also includes 'Model Contracts & Insurance' which can include issues such as: rights conferred, obligations, confidentiality (NDAs), data disclosure to 3rd parties and 'IP Protection & Licence Model' and 'Technical – IP Tracking & Cyber-Security Controls' to support protection and confidentiality for information that needs protection. The IP Risk Framework additionally facilitates linking and tracing the stakeholders' roles with the Digital Twin Architecture (which includes the data

LeMo Report Legal Issue	Applicable to IP Risk (Yes/No)	Considered in IP Risk Framework
		architecture) using 'Generic System Architecture & Interfaces' to accountabilities and obligations traced to contracts.
Open data	Yes	Yes Goals & Context considers the 'Business Context – Enabling Technology, Tools & Systems' and 'IP Context – IP Inventory (Owned & Used). The 'IP Risk Influencers' such as 'Complexity' includes consideration of the data architecture and ownership model through 'System Complexity', 'Stakeholder Map of IP…' and 'Structure & Incentives' and such risks can be mitigated by 'IP Risk Management Tools – Generic System Architecture & Interfaces' which can be developed with 'Governance & Policy – Policies & Standards' to clarify application of Open Data in a Sector context.
Sharing Obligations	Yes	Yes The LeMo report considers obligations in the transport sector from legislation such as 'Council Directive 2010/40/EU' (2010) which led to specifications for ITS systems that contain data sharing obligations.

LeMo Report Legal Issue	Applicable to IP Risk (Yes/No)	Considered in IP Risk Framework
		This is covered in the Risk Framework through 'Tools – Governance & Policy – Policies & Standards' and 'Technical – Generic System Architecture & Interfaces' which through 'Tools – Defined Stakeholder Types & Roles' and 'Tools – Systems Methodology' can trace obligations through 'Tools- Model Contracts & Insurance'
Data Ownership The LeMo report discusses the legal ambiguities with the concept of data ownership, in particular that there aren't rights in data as such, and how the EU is intending to provide more clarity. It identifies objectives such as the protection of investments and assets and avoiding confidential data disclosure and offers possible legislative and non-legislative measures to take forward such as model contract terms and data producer's rights. It considers the viewpoint of different types of stakeholders with roles of relevance such as Data Providers, Data Analytics	Yes	Yes For example: 'Goals & Context – Goals – Digital Twin Purpose, Need, Requirement' will identify the data threads (most effectively with 'Tool – Technical – Systems Methodology') Environment' and relate to the 'Context – Value/Business Case' and 'Context – IP Inventory (Owned & Used) for a 'Viewpoint – Stakeholder'. This enables 'Tool – Systems Methodology' to provide 'Clarity – Accountabilities & Obligations' to trace to contracts using 'Tools – Model Contracts & Insurance'. As the Risk Influence of "Clarity-Standards & Legal Environment" is high risk at present there may be a need for 'Tools – Generic System Architecture & Interfaces' to provide a primary means of risk mitigation for stakeholders with high

LeMo Report Legal Issue	Applicable to IP Risk (Yes/No)	Considered in IP Risk Framework
Service Providers, IT Infrastructure Providers, Internet Service Providers and Data-Entrepreneurs.		value IP, supported by 'Tools-Model Contracts & Insurance' which provide both protections and incentives to share.
Data Sharing Agreements Highlights the European Commission's principles to govern data sharing agreements for B2B and B2G. The B2B principles are: • **Transparency** – of purpose, access rights and use • **Shared Value Creation** – where data is a by-product of using a service where multiple parties have contributed to it's creation. • **Respect for each other's commercial interests** – and the need to protect • **Ensure undistorted competition** – when exchanging commercially sensitive data	Yes	Yes For example: 'Tools – Model Contracts & Insurance' The European Commission's principles are reflected through the IP Risk Influencers of: 'Clarity – Traceability' delivered through 'Tool-Systems Methodology', and 'Tools – Governance & Policy – Policies & Standards, Generic Assurance Model and Sector Audit & Accreditation Schemes' to provide transparency, undistorted competition and support shared value creation and respect for each other's commercial interests. 'Tools – Model Contracts & Insurance' can provide evidence of Shared Value Creation, Respect for each other's commercial interests, and to minimise data lock-in. The latter subject to governance and supported by tools such as the 'Tools - Generic System Architecture & Interfaces.'

LeMo Report Legal Issue	Applicable to IP Risk (Yes/No)	Considered in IP Risk Framework
• **Minimise data lock-in** – allow portability of data.		'Goals&Context – Digital Twin Purpose, Need, Requirement' will identify Purpose in the public or private interest and so the specific Tools required in support.
Liability Highlights the interdependencies between tangible parts: sensors, actuators and hardware, intangible parts: software and applications, Data and Data Services which complicates liability issues.	Yes	Yes For example: Linking 'Tools – Model Contracts & Insurance' with 'Tools – Generic System Architecture & Interfaces' with the support of 'Tools – Systems Methodology'. This then links to 'Goals – Tolerable Risk' Risk Influencer 'Clarity-Standards & Legal Environment' relates, and may be high risk due to low clarity as well as complexity in many cases.
Competition	Yes	For example: 'Tools – Governance & Policy – Generic Assurance Model'

Table 29: Coverage of LeMo Report Legal Issues in IP Risk Framework

The review against the LeMo report legal issues provided further confidence that the constructed IP Risk Framework identified relevant factors (Research Question 1) and added understanding of the relationship between them (Research Question 2) in support of H2.

7.5 Summary

The IP Risk Framework was evaluated using both expert interviews and applying case studies and secondary studies using the approaches described in section 4.5. Both evaluation approaches provided support for the structure of the IP framework, the categories, sub-categories and factors. The evaluation also provided further exploration and explanation of the relationships and interdependencies between factors. As such the hypothesis:

H2 – The described Framework explains how Intellectual Property Risks potentially impact multi-stakeholder collaboration using Digital Twins for life-cycle decision support

was considered to be supported by the evaluation which also concluded the following supporting hypotheses.

Hypothesis: The Goals & Context sub-categories and factors provide the inputs to assess Intellectual Property risk to collaboration with Digital Twins.

Hypothesis: The IP Risk Influencer sub-categories and factors identified can potentially influence Intellectual Property risk to collaboration with Digital Twins.

Hypothesis: The Risk Mitigation Tools sub-categories and factors identify the considerations for mitigating Intellectual Property risk to collaboration with Digital Twins.

The experts concurred that the framework had the potential to support evaluation of risk in such collaborations and positively considered two potential scenarios of using the framework for evaluating Digital Twin solution options and providing assurance that risks were identified, mitigated and managed. The case study evaluation also suggested that causes of IP collaboration failure could be identified and potentially evaluated and mitigated with the support of tools. As such it is concluded that the hypothesis:

H3 – Application of the framework could mitigate risks to the achievement of multi-stakeholder collaboration using Digital Twins for operational decision support.

was met by the evaluation concluding that the framework could potentially mitigate such risks. The framework now provides the basis for further research to develop the tools and to test application in new Digital Twin collaboration contexts. This should lead to further testing of the hypotheses and further development of the framework (See section 8.6).

Chapter 8 Conclusions and Recommendations

8.1 Introduction

The outcomes from the research study are related to the original aims and objectives. Conclusions from the research study are stated together with reflections on the limitations of the study. The chapter concludes with recommendations to take the research further and dissemination of findings.

8.2 Review of Original Aims and Objectives

The project achieved its original aim of exploring and describing a framework for understanding how IP can influence the risk to multi-stakeholder collaboration using Digital Twins for decision support through the life-cycle of a Physical Entity (Chapter 2). The elicited categories, sub-categories and factors were constructed through application of the research methodology and the outline relationships were evaluated through both the expert evaluation and case review.

The project also aimed to explore how the framework could be applied to assure that life-cycle IP risks to Digital Twin Collaborations are effectively managed. This was explored within the scope of an example industrial sector, rail, and considered rolling stock decision support examples in the public domain. Within the constraints of the research study the project successfully explored this aim through consideration of the application of cause-consequence trees using the bow-tie method and creation of goals for IP risk for potential integration into system assurance cases for safety and security (Chapters 6 and 7). It also considered the potential to score and relate the risk of Digital Twin implementation options to support design and procurement. Such approaches were reviewed, in concept, through the expert evaluation and supported. The consideration of the rail rolling stock case studies also demonstrated the benefit of the framework in facilitating the exploration of potential areas of risk for a scenario. This second aim was achieved within the frame and constraints of this project, but future research studies should take this aim further, by applying the framework with collaborating stakeholders as they implement new Digital Twin solutions. This will test the hypotheses relating to the framework and provide a frame for further research studies to deepen understanding of the relationship between some risk factors, building a library of applied cases for study.

The original objectives to achieve these aims were followed. In particular the complex research design, which included qualitative methods for constructing theory, was concluded to be appropriate to the early stage of adoption of Digital Twin applications, with low levels of available empirical data, and allowed the construction of a risk framework, which can now be applied in future projects to test the stated theories and hypotheses as more Digital Twin application opportunities become available.

8.3 Study Conclusions

The study concluded that an IP risk management framework, grounded in theory from a systematic research process, could support business and legal experts to ensure such risks are considered and managed as part of their overall risk management activities for collaboration using Digital Twins for decision support.

The study identified that there has been limited research of this topic up to now, with separate discussions from legal, business and technical academic and practitioner specialists expressing concern about such risks which is resulting in developing research on Digital Twin architectures and technical approaches for improved information security, in particular. However, the inter-related risk factors from these viewpoints had not previously been brought together and related. Such has been shown through this project to improve understanding of the exposure to risk and the types of mitigation required to reduce this exposure. It also highlights research gaps and areas that require further research to better manage these inter-related factors. One example is a better understanding of the impact of changing IP value and ownership over the life of a Physical Entity on the collaboration risk within the business context.

The study highlighted the importance of extending systems frameworks, methodologies and tools to provide traceability to support IP Risk management assurance particularly through management of changes. Information traceability approaches are established in model based systems engineering, BIM and model based assurance of safety and security but could be extended to provide traceability between contracts, obligations and IP registers and the Digital Twin and Physical Entity architectures for managing IP Risk to collaboration. This is an extension of the current use of model-based engineering and assurance methods where the link to contracts is currently focussed on the Physical Entity supply and integration rather

than broader operational use and life-cycle services risk. It also identified a link between IP risk to collaboration and Safety and Security Assurance Cases.

Existing risk management framework standards include a guidance part for legal risks which includes IP risk, ISO31022:2020 (British Standards Institution, 2020), but this only lists specific example considerations such as ensuring clarity of ownership and obligations on termination of contracts and is broad in application. The constructed risk framework was applied to the particular context of decision support based on Digital Twins and the categories of risk mitigations for that purpose, constructed from the research study, identified a relationship and overlap with risk standards focussed on security and safety. However, a standards gap was identified for consideration of additional legal considerations for the collaborative decision support context.

8.4 Significance & Contribution to Academic Knowledge and Professional Practice

The significance and contribution to academic knowledge and professional practice are summarised in Table 30.

IP Risk Framework	The constructed IP Risk Framework uniquely brings together legal (IP), business and systems engineering factors, through application of the research methodology, to support the understanding, assessment and mitigation of IP risks to stakeholder collaboration using Digital Twins for decision support. As the demand for complex systems-of-systems decision support tools using Digital Twins increases, the framework is intended to assist stakeholders anticipate, mitigate and manage these risks and provides a frame for further research and application, including the development of technical, legal and business tools.
Data	Novel data was sourced, collected and analysed from questionnaires and semi-structured interviews, from senior managers, IP professionals and emerging case studies during the study. This data was related to findings from secondary studies to improve understanding of the IP Risk Framework factors and their relationships.

	The original purpose of the secondary studies included ranged from commentary on IP law related to complex digital systems, understanding business collaboration risks, complex systems assurance to Digital Twin architectures and data security.
Application	The IP Risk Framework was developed for the needs of stakeholders collaborating to use and provide decision support services based on Digital Twins and the sectors which rely on the effectiveness of such services. The primary data from questionnaires and semi-structured interviews represented rail predominantly with case studies relating to decision support for maintenance of rolling stock specifically. While this was the area of focus for industry evaluation and context, literature data sources and legal expert participants involved in the evaluation represented a broader sector client base and evaluating applicability for broader application is recommended as an area for further work.
Method	The application of a complex research design with concurrent mixed-methods design dominated by qualitative analysis, and based on abductive Charmez constructive grounded theory, in a systems engineering context, was shown to be useful in developing and describing a framework in an emerging area. This then provides a framework that can be applied for the benefit of Digital Twin collaborators early in the maturity lifecycle.

Table 30: Research Contributions

8.5 Limitations of the Study

The study has developed and evaluated the IP Risk Framework to illustrate the factors, sub-categories and categories of importance for managing risk and the relationship between them. The complex design allowed regular reflection and periodic review of data quantity and characteristics and triangulation of findings. Further research and application of the framework will develop the application specifics of IP Risk Mitigation Tools which are expected to be expressed at a generic application layer and context specific layer.

The legal and literature sources have covered a broad range of digital application, country of focus and industry sector from manufacturing to the built environment and defence. However, the study's jurisdictional limitations are focussed on the UK, European Union and English common law for the following reasons:

- Legal and literature sources were limited to those in the English language, while this included US, European, Australian and some Asian perspectives, it excluded sources targeted at local jurisdictions.
- Participants were located within the UK, working within the UK and EU legal systems for UK, European and Canadian companies with a client base and supply chain predominantly in the European Union.

The study targeted two sectors: rail and gas, with participants to the initial questionnaires all identifying as representing 'Rail, airline and pipeline transportation.' This sector perspective influenced the development of the constructed framework. However, for the Stage 3 evaluation the case studies related to rail rolling stock in the UK and EU and the industry expert evaluators were based in the UK working predominantly for UK and EU owned companies. One evaluator worked for a Canadian owned company but the focus of the evaluator's day to day activity was within the EU and UK context.

As such the generalities of the framework ought to be further evaluated against a broader range of sectors and case studies. However, the feedback from the legal experts, in particular, that work across a range of sectors, suggested general applicability was likely at the factor, sub-category and category levels.

8.6 Recommendations

During the period of the research study and particularly in the early stages when the research plan was developed, there were limited developed case studies accessible to the researcher and issues were emerging, which led to the research approach implemented. As more cases and empirical data become available a study could be used to evaluate the relative significance of factors and quantify the significance of their relationships in defined contexts such as rail and relate rail to other sectors. A further project could include a Collaborative Action Research study which applies the framework to further cases with stakeholders, observes the implementation and reflects to further refine and develop the risk mitigation tools.

Further research could also include:

- Developing the integration of IP risk into system assurance cases using SACM.
- Exploring the challenges of valuing IP and providing value governance in multi-stakeholder collaborations to achieve a dependent Purpose over a sustained timeframe.
- Improving understanding of the required balance between IP protection for innovation and achieving and maintaining the Purpose in dependent collaborative Digital Twin services.
- A linear study to re-assess the case studies for Maintenance-as-a-service, over several years, to identify how successful the different business, contract and governance structures were in achieving and maintaining Purpose and avoiding realisation of risks.

8.7 Dissemination

During the early implementation of the research design, legal issues with using Digital Twins in an additive manufacturing context were presented at a conference (Clementson *et al.*, 2021a) and assisted in confirming concern for IP risk as a legal risk for collaboration. This paper is cited by Su *et al.* (2023) as part of a Digital Twin application scoping activity informing development of a life-cycle framework of digital twin enabled construction.

Early findings from the questionnaires and interviews relating to IP risk factors to collaboration, applied in a rail context, were then explored at the Annual INCOSE UK Systems Engineering Conference (Clementson *et al.*, 2021b). The audience represented several sectors from rail infrastructure to defence and provided further support for the research topic and confirmation that context factors in the business environment would be important considerations. Further progress was presented at dissemination seminars within the University of Derby college of science and engineering. On invitation, the resulting framework was outlined at an Arts and Humanities Research Council funded Digital Twins and the Law Workshop held at York University on 23rd October 2024 as part of the Alan Turing Institute's project, *Trustworthy and Ethical Assurance of Digital Twins (TEA-DT)* (2024).

Further dissemination activities, through journal papers and workshops are in progress.

8.8 Summary

Overall, it is concluded that the original aims and objectives of the research study were achieved, and the resulting IP Risk Framework contributes further understanding of the risks to collaboration when using Digital Twin based decision support systems. It also provides the basis for building further research and applications.

References

Abdelrahman, M., Macatulud, E., Lei, B., Miller, C., Biljecki, F. (2025), 'What is a Digital Twin anyway? Deriving the definition for the built environment from over 15,000 scientific publications', *Building and Environment*, Volume 274, pp.112748, Available at: https://doi.org/10.1016/j.buildenv.2025.112748

Adeagbo, MO., Wang, S-M., Ni, Y-Q. (2024), 'Revamping structural health monitoring of advanced rail transit systems: A paradigmatic shift from digital shadows to digital twins', *Advanced Engineering Informatics*, Volume 61, pp.102450, Available at: https://doi.org/10.1016/j.aei.2024.102450

Adu-Amankwa, K., Rentizelas, A., Daly, A., Corney, J., Wodehouse, A., Peron, M. (2023), 'Decision Considerations for Securing and Managing Intellectual Property within Additive Manufacturing Supply Chains', *IFAC-PapersOnLine*, Vol 56, Issue 2, Pages 6543-6548. Available at: https://doi.org/10.1016/j.ifacol.2023.10.304

Aguiar, A., Fernandes, P., Guerreiro, AP., Tomás, R., Agnelo, J., Santos, JL., Margarida, FA., Coelho, C., Fonseca, CM., d'Orey, PM., Luís, M., Sargento, S. (2022) 'MobiWise: Eco-routing decision support leveraging the Internet of Things', *Sustainable Cities and Society*, Volume 87, pp.104180, Available at: https://doi.org/10.1016/j.scs.2022.104180.

Ahmed, U., Petri, I., Rana, O., Raza, I., Hussain, SA. (2020) 'Federating Cloud Systems for Collaborative Construction and Engineering', *IEEE Access*, Volume 8, Available at: https://doi.org/10.1109/ACCESS.2020.2990233

Alkhabbas, F., Spalazzese, R. Cerioli, M. Leotta, M. Reggio, G. (2020) 'On the Deployment of IoT Systems: An Industrial Survey', *Proceedings - 2020 IEEE International Conference on Software Architecture Companion,* ICSA-C 2020, pp. 17–24, 9095740. Available at: https://doi.org/ 10.1109/ICSA-C50368.2020.00012

Almarri, K., Aljarman, M. and Boussabaine, H. (2019) 'Emerging contractual and legal risks from the application of building information modelling', *Engineering, Construction and Architectural Management* Vol. 26 No. 10, 2019 pp. 2307-2325, Available at: https://doi.org/10.1108/ECAM-06-2018-0224

Almarri, K., Aljarman, M. and Boussabaine, H. (2020) 'Emerging managerial risks from the application of building information modelling', *Journal of Facilities Management* Vol. 19, Issue 2, pp.228-248, Available at: https://doi.org/10.1108/JFM-01-2020-0002

Alstom (2022), *Services: It's a people business 07 Feb 2022*, Available at: https://www.alstom.com/press-releases-news/2022/2/services-its-people-business [online] (Accessed: 17/05/2024)

Altan, E., Isjk, Z. (2023) 'Digital twins in lean construction: a neutrosophic AHP-BOCR analysis approach', 'Engineering, Construction and Architectural Management', Vol. ahead-of-print, Available at: https://doi-.org.derby.idm.oclc.org/10.1108/ECAM-11-2022-1115

Anugerah, DP., and Indriani, M. (2018) 'Data Protection in Financial Technology Services: Indonesian Legal Perspective', *IOP Conference Series: Earth and Environmental Science*, Volume 175, International Conference on Industrial Technology for Sustainable Development (Icon-ITSD) 2017 25-26 October 2017, Makassar, Indonesia, Available at: https:// doi.org/10.1108/ECAM-06-2018-0224

Anda, AA., and Amyot, D. (2022), 'Self-Adaptation Driven by SysML and Goal Models – A Literature Review', *In e-Informatica Software Engineering Journal*, vol 16, no 1 pp 220101. Available at: https://doi.org/10.37190/e-Inf220101

Aniruddha, G., Yavari, R., Montazeri, M., Cole, K., Bian, L., Rao, P. (2019), 'Toward the digital twin of additive manufacturing: Integrating thermal simulations, sensing and analytics to detect process faults', *IISE Transactions,* Available at: https://doi.org/10.1080/24725854.2019.170.1753

Anwer, A. (2017), 'New Opportunities for Protecting and Managing Your Data', *Managing Intellectual Property*, 7/10/2017, p16-161p1 Chart ISSN 0960-5002 Database Business Source Complete

Autiosalo, J., Vepsalainen, J., Vitala, R., Tammi, K. (2019), 'A Feature Based Framework for Structuring Industrial Digital Twins', *IEEE Access*, Volume 8, 2020, Available at: https://doi.org/ 10.1109/ACCESS.2019.2950507

Axelrod, CW. (2013), 'Managing the risks of cyber-physical systems', *9th Annual Conference on Long Island Systems*, *Applications and Technology*, *LISAT 2013.* Available at: https://doi.org/ 10.1109/LISAT.2013.6578215

Baruffaldi, G., Accorsi, R., Manzini, R. (2019) 'Warehouse management system customization and information availability in 3pl companies: A decision-support tool', *Industrial Management and Data Systems*, Volume 119(2), pp.251-273, Available at: https://doi.org/10.1108/IMDS-01-2018-0033

Bechtold S. (2015) 'Economic Research Working Paper No 28, 3D Printing and Intellectual Property System', *WIPO Economic & Statistics Series.* Available at: https://www.wipo.int/publications/en/details.jsp?id=3999&plang=EN (Accessed: 2 May 2019)

Bécue, A., Maia, E., Feeken, L., Borchers, P., Praça, I.becue (2020) 'A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future'. *Applied Sciences*. 2020; Volume: 10(13). pp.4482. Available at: https://doi.org/10.3390/app10134482

Belfadel, A., Horl, S., Tapia, RJ., Politaki, D., Kureshi, I., Tavasszy, L., Puchinger, J. (2023) 'A conceptual digital twin framework for city logistics', *Computers, Environment and Urban Systems*, Volume 103, pp. 101989, Available at: https://doi.org/10.1016/j.compenvurbsys.2023.101989

Bickford, J., Van Bossuyt, DL., Beery, P., Pollman, A. (2020), 'Operationalizing digital twins through model-based systems engineering methods', *Systems Engineering*, 3030:23: pp. 724-750, Wiley. Available at: https://doi.org/10.1002/sys.21559

Binot, A., Duboz, R., Promburom, P., Phimpraphai, W., Cappelle, J., Lajaunie, C., Goutard, FL., Pinyopummintr, T., Figuie, M., Roger, FL. (2015) 'A framework to promote collective action within One Health community of practice: Using participatory modelling to enable interdisciplinary, cross-sectoral and multi-level integration', *One Health* 1 (2015), pp. 44-48. Available at: https://doi.org/10.1016/j.onehlt.2015.09.001

Bird & Bird LLP. (2020) 'Legal Implications of Digital Twins in the Supply Chain', LEXOLOGY[online], 10 November 2020, Available at : https://www.lexology.com/library/detail.aspx?g=55f86213-a6ff-404d-bfe7-

d1b0bbbf1c86&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2020-11-12&utm_term= (Accessed: 12 November 2020)

Bishop, P., Bloomfield, R. (1998) 'A Methodology for safety case development', In: Redmill, F, Anderson, T. (eds) *Industrial Perspectives of Safety-Critical Systems*. London: Springer. Available at: https://doi.org/10.1007/978-1-4471-1534-2_14

Blakley, CT., Li, LW., Eakman, G., Baker, BC. (2022), 'Engineering resilient systems cloud computing architecture (ECCA): a collaborative and secure analysis framework', *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, Volume 19, Issue 3, pp.299-311, Available at: https://doi.org/10.1177/1548512920960539

British Standards Institution (1994) *BS ISO 10303-21:1994 Industrial automation systems and integration – Product data representation and exchange Part 21 Implementation methods: Clear text encoding of the exchange structure*, BSI: BSI Standards Limited, ISBN 0-580-24664-7

British Standards Institution (2010) *BS EN 61508-1:2020 Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1 General Requirements*, BSI: BSI Standards Limited, ISBN 978-0-580-56233-4

British Standards Institution (2018) *BS ISO 31000:2018: Risk Management –Guidelines*, BSI: BSI Standards Limited, Second Edition, ISBN 978-0-580-88518-1

British Standards Institution (2020) *BS ISO 31022:2020: Risk Management. Guidelines for the management of legal risk*. BSI: BSI Standards Limited, First Edition, ISBN 978-0-580-91826-1

British Standards Institution (2021a) *BS ISO 23247-2:2021:Automation systems and integration – Digital twin framework for manufacturing Part 2: Reference Architecture*, BSI: BSI Standards Limited, First Edition 2021-10-07, ISBN 978-0-539-05409-5

British Standards Institution (2021b) *BS ISO/IEC/IEEE 16085:2021: Systems and software engineering – Life cycle processes – Risk Management*, BSI: BSI Standards Limited, First Edition 2021-01, ISBN 978-0-539-00198-3

British Standards Institution (2022) *BS EN ISO/IEC 27002:2022: Information Security, cybersecurity and privacy protection. Information security controls*. BSI: BSI Standards Limited, ISBN 978-0-539-03716-6

British Standards Institution (2023a) *BS EN ISO/IEC 27001:2023*:*Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems - Requirements*, BSI: BSI Standards Limited, 2023-07, ISBN 978-0-539-25646-8

British Standards Institution (2023b) *BS ISO/IEC 30173:2023*: *Digital Twin – Concepts and terminology*, BSI: BSI Standards Limited, First Edition, 2023-11, ISBN 978-2-8322-7680-8

British Standards Institution (2023c) *BS ISO/IEC/IEEE 15288:2023: Systems and Software Engineering – System Life Cycle Processes – Tracked Changes to compare with 15288:2015*, BSI: BSI Standards Limited, ISBN 978 0 539 27135 5

British Standards Institution (2024a) *BS ISO/IEC 27562:2024: Information technology – Security techniques – Privacy guidelines for fintech services*, BSI: BSI Standards, 2024, ISBN 978-0-539-17483-0

British Standards Institution (2024b) *BS ISO 44001:2017+A1:2024*: *Collaborative business relationship management systems – Requirements and framework*, BSI: BSI Standards, 2024, ISBN 978-0-539-30739-9

British Standards Institution (2024c) *BS ISO 55001:2024*: *Asset management – Asset management system – Requirements*, BSI: BSI Standards Limited 2024, Second Edition, 2024-07, ISBN 978-0-539-17976-7

Burr, C., Leslie, D. (2023) 'Ethical assurance: a practical approach to the responsible design, development, and deployment of data-driven technologies', *AI and Ethics*, Volume 3, pp. 73-98, Available at: https://doi.org/10.1007/s43681-022-00178-0

Cahn, A., Katz, D., Ghermandi, A., Prevos, P. (2023) 'Adoption of data-as-a-service by water and wastewater utilities', *Utilities Policy* 81 (2023), 101492. Available at: https://doi.org/10.1016/j.jup.2023.101492

Celik, Y., Petri, I., Barati, M. (2023), 'Blockchain supported BIM data provenance for construction projects', *Computers in Industry*, Vol 144, Available at: https://doi.org/ 10.1016/j.compind.2022.103768

Celoza, A., De Oliveira, DP., Leite, F (2023)., 'Qualitative Analysis of the Impact of Contracts on Information Management in AEC Projects', *Journal of Construction Engineering and Management,* Vol 149, No 3, 4022185, Available at: https://doi.org/10.1061/JCEMD4.COENG-12359

Charmez, K. (2014) *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*, Second Edition, London: Sage Publications,

Chandru, A., Kumar, J. (2009) 'Walking the Intellectual Property Tight Rope: Recommended Strategies for the New Millennium Corporation', *GNLU Law Review*, 2(1), pp 1-36.

Chelouati, M., Boussif, A., Beugin, J., El Koursi, E-M. (2023) 'Graphical safety assurance case using Goal Structuring Notation (GSN) – challenges, opportunities and a framework for autonomous trains', *Reliability Engineering & System Safety*, Volume 230, pp.108933, Available at: https://doi.org/10.1016/j.ress.2022.108933

Chien, K-F., Wu, Z.-H., Huang, S-C (2014) 'Identifying and assessing critical risk factors for BIM projects: Empirical Study', *Automation in Construction*, Volume 45, pp 1-15, Available at: https://doi.org/10.1016/j.autcon.2014.04.012

Cinque, M., Russo, S., Esposito, C., Free-Nelson, F., Kamhoua, C.A. (2018), 'Cloud Reliability: Possible Sources of Security and Legal Issues?'*, IEEE Cloud Computing*, 5(3), pp. 31–38, Available at: https://doi.org/10.1109/MCC.2018.032591614

Clementson, J., Teng J., Wood, P., Windmill, C. (2021**a**), 'Legal Considerations for Using Digital Twins in Additive Manufacture - A Review of the Literature', *Advances in Transdisciplinary Engineering Series, Volume 15, Advances in Manufacturing Technology*

XXXiV, ISBN 978-1-64368-198-6 (print), pp 91-96. Available at: https://doi.org/ 10.3233/ATDE210018

Clementson, J., Wood, P., Windmill, C., Teng, J. (2021**b**), 'Managing Intellectual Property Issues with Digital Twins', *Proceedings of INCOSE UK Annual Systems Engineering Conference (ASEC) 2021*, Leeds, 23rd and 24th November 2021 Presented to ASEC 2021 on 24th November 2021. Available at: https://repository.derby.ac.uk/item/9wq3x/managing-intellectual-property-issues-with-digital-twins

Cohen, Y., Faccio, M., Pilati, F., Yao, X. (2019) 'Design and Management of Digital Manufacturing and Assembly Systems in the Industry 4.0 era', *The International Journal of Advanced Manufacturing Technology*, Available at: https://doi.org/10.1007/s00170-019-04595-0

Cole, A. (2018) 'An Update on BIM under English Law', *Construction Law International*, Volume 13, Issue 2, pp51-55, ISSN 1819-1371

'Commission Regulation (EU) No. 1078/2012 of 16 November 2021 on a common safety method for monitoring to be applied by railway undertakings, infrastructure managers after receiving a safety certificate or safety authorisation and by entities in charge of maintenance' (2012), *Official Journal* L320, p.8-13, Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32012R1078

Congès, A., Evain, A., Benaben, F., Chabiron, O., Rebière, S. (2020) 'Crisis Management Exercises in Virtual Reality' IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Atlanta, GA, USA. pp. 87-92, Available at: https://doi.org/10.1109/VRW50115.2020.00022.

Conrado, DJ., Karlsson, MO., Romero, K., Sarr, C., Wilkins, JJ. (2017) 'Open Innovation: Towards Sharing of Data, Models and Workflows', *European Journal of Pharmaceutical Sciences,* Volume 109, pp S65-S71, Available at: https://doi.org/10.1016/j.ejps.2017.06.035

'Council Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases' (1996), *Official Journal* L77, p.20-28, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009 (Accessed 02/02/2020)

‘Council Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the legal protection of databases’ (2008), *Official Journal* L191, p.1-45, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0057 (Accessed: 02/02/2020)

‘Council Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport’ (2010), *Official Journal* L207, p.1-13, Available at: https://eur-lex.europa.eu/eli/dir/2010/40/oj (Accessed: 02/02/2020)

‘Council Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (2016) *Official Journal* L138, p.44-101, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0797 (Accessed: 10/05/2024)

‘Council Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety’ (2016) *Official Journal* L138, p.102-149, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0798 (Accessed: 10/05/2024)

‘Council Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (2016) *Official Journal* L157, p.1-18, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943 (Accessed 10/05/2024)

‘Council Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022) *Official Journal* L333, p.1, Available at: https://eur-lex.europa.eu/eli/dir/2022/2555 (Accessed 18/11/2024)

‘Council Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data

Governance Act), *Official Journal L152*, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868 (Accessed 05/06/2023)

Cresswell, JW.(2009) *Research Design – Qualitative, Quantitative and Mixed Methods Approaches*, Third Edition, London: Sage Publications

Crossrail (2022) *Over 200 Metres Long, Providing Space for Up to 1,500 Passengers*[Online], Available at: https://www/crossrail.co.uk/project/new-trains/ (Accessed 08/04/2022)

Cutrona, V., Bonomi, N., Montini, E., Delinavelli, G., Pedrazzoli, P. (2024), 'Extending factory digital twins through human characterisation in asset administration shell', *International Journal of Computer Integrated Manufacturing*, Volume 37, pp.1214-1231, Available at: https://doi.org/10.1080/0951192X.2023.2278108

Cui, Y., Kara, S., Chan, KC. (2020) 'Manufacturing Big Data Ecosystem: A Systematic Literature Review', *Robotics and Computer Integrated Manufacturing* 62, 101861, Available at: https://doi.org/10.1016/j.rcim.2019.101861

Culnane, C. (2019) 'Misconceptions in Privacy Protection and Regulation', *Law in Context: A Socia-Legal Journal*, Volume 36, Issue 2, pp 49-60, Available at: https://doi.org/10.26826/law-in-context.v36i2.110

D'Agostino, D., Borg, M., Hallett, SH., Thompson, A., Papadimitriou, L., Knox, JW. (2020) 'Multi-stakeholder Analysis to Improve Agriculture Water Management Policy and Practice in Malta, *Agricultural Water Management*, Volume 229, Article No. 105920, Available at: https://doi.org/10.1016/j.agwat.2019.105920

dos Santos, CH., Montevechi, JAB., de Queiroz, JA., de Carvalho Miranda, R., Leal, F. (2021). 'Decision support in productive processes through DES and ABS in the Digital Twin era: a systematic literature review'. *International Journal of Production Research*, 60(8), 2662–2681. Available at: https://doi.org/10.1080/00207543.2021.1898691

Daly A (2016), *Socio-Legal Aspects of the 3D Printing Revolution*, London: Palgrave Macmillan.

Dambra, C (2021), *IAMS system architecture and guidelines for its implementation in the demonstrators*, Deliverable D3.1 IN2SMART2, 31/05/2021, H2020-S2RJU-CFM-2019, Available at: https://projects.shift2rail.org/s2r_ip3_n.aspx?p=IN2SMART2 (Accessed November 2024)

Daniel, BK. (2018) 'Empirical verification of the "TACT" framework for teaching rigour in qualitative research methodology', *Qualitative Research Journal*, 2018, Vol 18 (3), pp 262-275, Available at: https://doi.org/10.1108/QR-J-D-17-00012

Debussche, J., Cesar, J., De Moortel, I. (2018) *Leveraging Big Data for Managing Transport Operations*, Deliverable D2.2 Report on Legal Issues, October 2018, MG-8-2-2007 – Big Data in Transport: Research opportunities, challenges and limitations, Available at:https://static1.squarespace.com/static/59f9cdc2692ebebde4c43010/t/5bdab3e2cd8366e9378d02b1/1541059569380/D2.2_Report+on+Legal+Issues_LeMO+-+FINAL.pdf (Accessed October 2019)

De Filippi, P., Maurel, L. (2015) 'The paradoxes of Open Data and how to get rid of it: Analysing the interplay between Open Data and Sui-Generis Rights on Databases [article]', *International Journal of Law and Information Technology*, Vol 23, Issue 1 (Spring 2015), pp. 1-22

Department for Transport (2023) *Transport Data Strategy – Innovation through Data*, Available at: https://assets.publishing.service.gov.uk/media/63eb62c9d3bf7f62e21c274a/dft-transport-data-strategy.pdf (Accessed November 2023)

Digitale Schiene Deutschland (2024), *Development Project – Data Factory*, Available at: https://www.digitale-schiene-deutschland.de/en/projects/Data%20Factory (Accessed: 24/05/2024)

Djalante, R..; Holley, C.; Thomalla, F.; Carnegie, M. (2013) 'Pathways for adaptive and integrated disaster resilience', *Natural Hazards*, Vol 69, Issue 3, Available at: https://doi.org/10.1007/s11069-013-0797-5

Dong, C., Xu, Y., Liu, X., Zhang, F., He, G., Chen, Y. (2020) 'Hardware trojans in chips: A survey for detection and prevention', *Sensors (Switzerland)*, Volume 20 Issue 18, 5165, Available at: https://doi.org/10.3390/s20185165

Druetta, C. (2018) 'Legal Perspectives on Predictive Maintenance: Case Study', *International In-House Counsel Journal*, 11(44), pp 1-7, Available at: https://www.iicj.net/paper/1187?key=1187 (Accessed: 2021)

Ebert, J. (2021) *Digitalization: Knorr-Bremse wins contract for extensive remote condition monitoring of climate control systems on UK train fleets*, Available at: https://newsroom.knorr-bremse.com/en/digitalization-knorr-bremse-wins-contract-for-extensive-remote-condition-monitoring-of-climate-control-systems-on-uk-train-fleets/ (Accessed 08/04/2022)

European Commission (2023) *Shaping Europe's Digital Future – Unlocking the potential of mobility data*, Available at: https://digital-strategy.ec.europa.eu/en/policies/mobility-data#:~:text=Towards%20a%20common%20European%20mobility%20data%20space&text=The%20EU%20Data%20Strategy%20announced,a%20controlled%20and%20secure%20way. (Accessed: November 2023)

Enzer, M., Bolton, A., Boulton, C., Byles, D., Cook, A., Dobbs, L., Kearney, E. *et al* (2019) *Roadmap for delivering the information management framework for the built environment* https://www.cdbb.cam.ac.uk/DFTG/DFTGRoadmap, Available at: https://doi.org/10.17863/CAM.38227 (Accessed: 19 June 2019)

Eriksson, K., Markussen, C. (2023) 'Quality Assurance of Digital Twins', *Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering – OMAE*, Available at: https://doi.org/10.1115/OMAE2023-105285

Errandonea, I., Beltran, S., Arrizabalaga, S. (2020) 'Digital Twin for maintenance: A literature review', *Computers in Industry* 123, 103316, Available at: https://doi.org/10.1016/j.compind.2020.103316

Ertle B (2023), 'Safeguarding Intellectual Property When Collaborating with External Parties', *Kiteworks: Safeguarding IP When Collaborating With Partners*, 15 April 2023, Available at: https://www.kiteworks.com/third-party-risk/safeguard-your-intellectual-property/ (Accessed: 26/04/24)

Fan, S-L., Lee, C-Y., Chong, H-Y., Skibniewski, MJ. (2018) 'A Critical Review of Legal Issues and Solutions Associated with Building Information Modelling', *Technological and*

Economic Development of Economy, Volume 24, Issue 5, pp. 2098-2130, Available at: https://doi.org/10.3846/tede.2018.5695

Fender, K (2021), *'Stadler and DB Launch Digital Twin Project for Flirt Fleet'*, *International Rail Journal*, 1 June 2021, Available at: https://www.railjournal.com/technology/stadler-and-db-launch-digital-twin-project-for-flirt-fleet/ (Accessed 24/05/2024)

Galvin, P., Tywoniak, S., Sutherland, J. (2021) 'Collaboration and opportunism in megaproject alliance contracts: The interplay between governance, trust and culture', *International Journal of Project Management*, 39 (2021) 394-405, Available at: https://doi.org/10.1016/j.ijproman.2021.02.007

Geyer, M. (2022) 'On Track: Digitale Schiene Deutschland Building Digital Twin of Rail Network in NVIDIA Omniverse'. *Nvdia*, 20 September 2022, Available at: https://blogs.nvidia.com/blog/deutsche-bahn-railway-system-digital-twin/ (Accessed 06/10/2023)

Ghosh, J. (2020) 'Power Play of Artificial Intelligence upon Intellectual Property Rights'. *Indian Journal of Law and Justice*, Vol.11, no.1, pp.100-114, Available at: HeinOnline

Gooding, P. (2019) 'Mapping the rise of digital mental health technologies: Emerging issues for law and society', *International Journal of Law and Psychiatry*, 62, 101498, Available at: https://doi.org/10.1016/j.ijlp.2019.101498

Gorbatyuk, A., van Overwalle, G,. von Zimmermen, E. (2016) 'Intellectual Property Ownership in Coupled Open Innovation Processes', IIC International Review of Intellectual Property and Competition Law, Volume 47(3), pp.262-302, Available at: https://doi.org/10.1007/s40319-016-0461-1

Gregor, S., Hevner, AR. (2013) 'Positioning and Presenting Design Science Research for Maximum Impact, MIS Quarterly, Volume 37, No 2, pp.337-355, Available at: https://www.jstor.org/stable/43825912

Grieves, M., Vickers, J. (2017), *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behaviour in Complex Systems*, Switzerland : Springer International Publishing,

2017, F-J-Kahlen *et al*, Transdisciplinary Perspectives on Complex Systems, pp. 85-113, Available at: https://doi.org/10.1007/978-3-319-38756-7_4

Gromova, E., Koneva, N., Titova, E. (2022) 'Legal barriers to the implementation of digital industry (Industry 4.0) components and ways to overcome them', *The Journal of World Intellectual Property*, Volume 25, pp 186-205 Available at: https://doi.org/10.1111/jwip/12215

Grudinschi, D., Sintonen, S., Hallikas, J. (2014), 'Relationship risk perception and determinants of the collaboration fluency of buyer-supplier relationships in public service procurement', *Journal of Purchasing & Supply Management*, 20 (2014) p.82-91, Available at: https://doi.org/10.1016/j.pursup.2014.03.004

Guttieres, D.; Stewart, S.; Wolfrum, J.; Springs, S.L.(2019) 'Cyberbiosecurity in Advanced Manufacturing Models', *Frontiers in Bioengineering and Biotechnology*, Volume 7, 210, Available at: https://doi.org: 10.3389/fbioe.2019.00210

Hansen, OH., and Jaiswal, V. (2023) 'A Framework for Trustworthy Digital Twins Over their Lifecycle.' *Paper presented at the Offshore Technology Conference Brasil, Rio de Janeiro, Brazil, October 2023*. Available at: https://doi.org/10.4043/32851-MS

Hart, LE. (2015), 'Introduction to Model-Based System Engineering (MBSE) and SysML', *Lockheed Martin* , Presented at the Delaware Valley INCOSE Chapter Meeting July 30 2015. Available at: https://www.incose.org/docs/default-source/delaware-valley/mbse-overview-incose-30-july-2015.pdf (Accessed 23/06/2020)

Health and Safety at Work etc Act 1974, Available at: https://www/legislation.gov.uk (Accessed 01/03/2021)

Hennink, M., Kaiser, BN. (2022) 'Sample sizes for saturation in qualitative research: A systematic review of empirical tests', *Social Science & Medicine*, Volume 292, January 2022, p.114523, Available at: https://doi.org/10.1016/j.socscimed.2021.114523

Hessami, AG.; Karcanias, N. (2009) 'Complexity, emergence and the challenges of assurance the need for a systems paradigm', *IEEE International Systems Conference Proceedings*, Available at: https://doi.org:10.1109/SYSTEMS.2009.4815779

Horváth, L., Rudas, IJ. (2022) 'Intelligent Computing Methods for Contextual Driving in Smart Engineering Model Systems', *Electronics (Switzerland)*, volume 11, issue 11, pp.1728, Available at: https://doi.org/ 10.3390/electronics11111728

Hoseini, E., Hertogh, M., Bosch-Rekveldt, M. (2021) 'Developing a generic risk maturity model (GRMM) for evaluating risk management in construction projects', *Journal of Risk Research*, 24:7, pp.889-908, Available at: https://doi.org/10.1080/13669877.2019.1646309

HS2 (2022) *The Digital Twin – A Vision for HS2*, Available at: https://assets.hs2.org.uk/wp-content/uploads/2022/09/Digital-Twin-A-Vision-for-HS2-August-2022-web-version.pdf, (Accessed: 02 February 2023)

Hsu, K-M., Hsieh, T-Y., Chen, J-H. (2015) 'Legal risks incurred under the application of BIM in Taiwan', *Forensic Engineering*, Volume 169, Issue FE3. Proceedings of the Institution of Civil Engineers, Available at: https://doi.org/10.1680/feng.14.00005

Hu, W., Chang, C-H., Sengupta, A., Bhunia, S., Kastner, R., Li, H. (2021) 'An overview of hardware security and trust: Threats, countermeasures and design tools', *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Volume: 40(6), Available at: https://doi.org/10.1109/TCAD.2020.3047976

Huang, S., Wang, G., Yan, Y., Fang, X. (2020) 'Blockchain Based data management for digital twin of product', *Journal of Manufacturing Systems* S4 pp.361-371, Available at: https://doi.org/10.1016/j.jmsy.2020.01.009

INCOSE (nd) *Systems Engineering Definition*, Available at: https://www.incose.org/about-systems-engineering/system-and-se-definitions/systems-engineering-definition (Accessed: 12 December 2024)

Institution of Gas Engineers and Managers (2018*), IGEM/GL/4 Edition 3 – Gas System Assets – Safety Management System*, Mar 2018, Available at: https://www.igem.org.uk/resource/igem-gl-4-edition-3-gas-system-assets-safety-management-system.html (Accessed: March 2020)

Issa, M., Remy, S., Ducellier, G., Landes, B. (2023), 'Updating a Railway Infrastructure Digital Twin by The Integration of a Variety of Data Sources', *Transportation Research Procedia*, Volume 72, pp. 666-673, Available at: https://doi.org/10.1016/j.trpro.2023.11.453

Jæger, B., Bach, T., Pedersen, SA. (2019) 'A Blockchain Application Supporting the Manufacturing Value Chain', *IFIP Advances in Information and Communication Technology*, Available at: https://doi.org/10.1007/978-3-030-30000-5_58

Jeschke, S., Grassmann, R. (2021) 'Development of a Generic Implementation Strategy of Digital Twins in Logistics Systems Under Consideration of the German Rail Transport', *Applied Sciences* 2021, 11, pp.10289, Available at: https://doi.org/10.3390/app112110289

Jo, TM., Ishak, SSM., Zakiyuddin, Z., Rashid, A. (2018) 'Overview of the Legal Aspects and Contract Requirements of the BIM Practice in Malaysian Construction Industry', *MATEC Web of Conferences* 203, 02011, ICCOEE 2018, Available at: https://doi.org:10.1051/matecconf/201820302011

Kaewunruen, S., Lian, Q. (2019) 'Digital Twin Aided Sustainability-Based Lifecycle Management for Railway Turnout Systems', *Journal of Cleaner Production*, 228, pp.1537-1551, Available at: https://doi.org/10.1016/j.jclepro.2019.04.156

Kalogiamno, E., Oosteram, P., Dimopoutou, E., Lemmen, C. (2020) '3D Land Administration: A Review and a Future Vision in the Context of a Spatial Development Lifecycle', *ISPRS International Journal of Geo-Information*, 9,107, Available at: https://doi.org:10.3390/ijgi9020107

Kartskhiya, A., Makarenko, D. (2019) 'Status and risks of artificial intelligence: Legal aspects', *CEUR Workshop Proceedings*, Available at: https://ceur-ws.org/vol-2603/short5.pdf

Keller, J., Lindenmeyer, A., Blattmann, M., Gaebel, J., Schnieder, D., Neumuth, T., Franke, S. (2023) 'Using digital twins to support multiple stages of the patient journey', *Studies in Health Technology and Informatics*, Volume 301, pp.227-232, Available at: https://doi.org/10.3233/SHTI230045

Kelly, T., Weaver, R. (2004) 'The Goal Structuring Notation – A Safety Argument Notation', *In Proceedings of the Dependable Systems and Networks 2004: Workshop on Assurance Cases*, July 2004, Available at: https://www.researchgate.net/publication/228990118_The_goal_structuring_notation-a_safety_argument_notation (Accessed: 6 June 2020)

Kerber, W. (2016) 'Governance of Data: Exclusive Property vs Access', *IIC* 47 (2016) 759-762 [Published online 27 October 2016] *Max Planck Institute for Innovation and Competition*, Munich 2016

Kitchenham, B., Brereton P. (2013) 'A systematic review of systematic review process research in software engineering', *Information and Software Technology*, Volume 55, Issue 12, pp.2049-2075, Available at: https://doi.org/10.1016/j.infsof.2013.07.010

Knapp, GL., Mukherjee, T., Zwback, JS., Wei, HL., Palmer, TA., De, A., DebRoy, T. (2017) 'Building Blocks for a digital twin of additive manufacturing', *Acta Materialia* 135(1017) 390-399, Available at: https://doi.org/10.1016/j.actamat.2017.06.039

Korth, B., Schwede, C., Zajac, M. (2018) 'Simulation-ready digital twin for realtime management of logistics systems' *IEEE International Conference on Big Data (Big Data), Seattle, WA, USA*, pp. 4194-4201, Available at: https//doi.org/10.1109/BigData.2018.8622160.

Kremers, M. (2018) *Digital Manufacturing of Composites*, 21 November 2018, Airborne, Available at: www.airborne.com https://nag.aero/wp-content/uploads/2018//NAG-digital-twin-meeting-21-nov-2018.pdf (Accessed: 12/02/2021)

Kritzinger, W., Karner, M., Traar,G., Heryes, J., Sihn, W., (2018) 'Digital Twins in Manufacturing: A Categorical Literature Review and Classification', *IFAC Papers Online*, 51-11, p.1016-1022, Available at: https://doi.org/10.1016/j.ifacol.2018.08.474

Lamb, K., (2018) 'Challenges of Digitalisation in the Aerospace and Aviation Sectors', *CDBB*, Series No: CDBB_REP_002_March 2018, Available at: https://doi.org/10.17863/CAM.26276

Lambert, R., Temple, P. (2015) *The Relationship between Standards, Standards Development and Intellectual Property*, Available at: https://www.bsigroup.com (Accessed: 25 March 2022)

LexisNexis (2024), *How Patents Became A Managing Board Agenda Item At Siemens with PatentSight*, Available at: https://www.lexisnexisip.com/resources/stories/increasing-patent-portfolio-strength-and-patent-income-at-siemens/ (Accessed: 26 April 2024)

Lionel, G. (2023) *Digital Thread from Systems Engineering to Service and Asset Lifecycle Management, Siemens and IBM extend their partnership to accelerate sustainable product development and operations*, 03 May 2023, Available at: https://www.engineering.com/story/digital-thread-from-systems-engineering-to-service-and-asset-lifecycle-management (Accessed: 10 May 2024)

Lis, D., Arbter, M., Spindler, M., Otto, B. (2023) 'An investigation of antecedents for data governance adoption in the rail industry – findings from a case study at Thales', *IEEE transactions on engineering management* [Online] Volume 70 (7), pp.2528-2545

Liu, H., Ning, H., Mu, Q., Huang, R., Ma, J. (2019) 'A review of the smart world', *Future Generation Computer Systems*, 96, pp. 678–691, Available at: https: //doi.org/10.1016/j.future.2017.09.010

Macchi, M., Roda, I., Negri, E., Fumagalli, L. (2018) 'Exploring the role of Digital Twin for Asset Life Management', *IFAC – PapersOnLine*, Volume 51(11), pp.790-795, Available at: https://doi.org/10.1016/j.ifacol.2018.08.415

Madni, AM., Madni, CC., Lucero, SD. (2019) 'Leveraging Digital Twin Technology in Model-Based Systems Engineering', *Systems*, 7, 7, Available at: https://doi.org/10.3390/systems7010007

Mandolla, C., Petruzzelli, AM., Percoco, G., Urbinati, A. (2019) 'Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry', *Computers in Industry*, Volume 109, pp.134-152. Available at: https://doi.org/10.1016/j.compind.2019.04.011

Mauritz, K. (2020) 'AI & Intellectual Property: Towards an Articulated Public Domain', *Texas Intellectual Property Law Journal*, Volume 28, Issue 3, pp. 297-342

Mbabu, A., Underwood, J., Munir, M. (2023) 'The BIM Maturity Process to the Digital Twin for Lean Strategic Facility Management', *Proceedings of the European Conference on Computing in Construction*, Available at: https://doi.org/10.35490/EC3.2023.325

McNulty Report (2011), *Realising the Potential of GB Rail: Report of the Rail Value for Money Study* – 19 May 2011, ISBN 978 1 84864 123 5 Available at: https://www.gov.uk/government/publications/realising-the-potential-of-gb-rail (Accessed: 5 June 2022)

Mendis, D., Nordemann, JB., Ballardini, RM., Brorsen, H., Moreno, M del C., Robson, J., Dickens, P. (2020) 'The Intellectual Property Implications of the Development of Industrial 3D Printing', *European Commission*, Available at: https://doi.org/10.2873/85090

Millwater, H., Ocampo, J., Crosby, N. (2019) 'Probabilistic Methods for Risk Assessment of Airframe Digital Twin Structures', *Engineering Fracture Mechanics*, Volume 221, November 2019, p.106674, Available at: https://doi.org/10.1016/j.engfracturemech.2019.106674

Ministry of Defence and Military Aviation Authority (2018) *Bow-Tie: a visual tool to keep an overview of risk management practices*, Available at: https://www.gov.uk/government/news/bowtie-a-visual-tool-to-keep-an-overview-of-risk-management-practices (Accessed: 20 July 2022)

Mohr, S., Khan, O. (2015) '3D Printing and Its Disruptive Impacts on Supply Chains of the Future', *Technology Innovation Management Review*, 5(11): 20-25, Available at: https://doi.org/10.22215/timreview/942

Moyne, J, Qamsane, Y., Balta, EC., Kovalenko, I., Faris, J., Barton, K., Tilbury, DM. (2020) 'A Requirements Driven Digital Twin Framework: Specification and Opportunities', *IEEE Access*, 2020, 8: p.107781-107801. Available at: https://doi.org/10.1109/ACCESS.2020.3000437

Mugge, J., Hahn, IR., Riedelsheimer, T., Chatzis, J. (2023) 'End-of-life decision support to enable circular economy in the automotive industry based on digital twin data', *Procedia CIRP*, Volume 119, Pp.1071-1077, Available at: https://doi.org/10.1016/j.procir.2023.03.150

Mukherjee, T., DebRoy, T. (2019) 'A digital twin for rapid qualification f 3D printed metallic components', *Applied Materials Today*, 14(2019) 59-65, Available at: https://doi.org: 10.1016/j.amt.2018.11.003

Muller, G. (2013) 'Systems Engineering Research Methods', *Procedia Computer Science*, Volume 16, pp.1092-1102, Available : https://doi.org/10.1016/j.procs.2013.01.115

Munn, Z., Peters, MDJ., Stern, C., Tufanaru, C., McArthur, A. (2018), 'Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach', *BMC Med Res Methodol*. Volume 1, 143 Available at: https://doi.org/10.1186/s12874-018-0611-x

Murray, A. (2016) *Information Technology Law – The Law and Society*, 3rd Edition, Oxford University Press 2016, ISBN 978-0-19-873246-4

Nair, S., de la Vara, JL., Sabetzadeh, M., Briand, L. (2014) 'An extended systematic literature review on provision of evidence for safety certification', *Information and Software Technology*, Volume 56 (7), pp.689-717, Available at: https://doi.org/10.1016/j.infsof.2014.03.001

Nati, M., Mayer, S., Capossele, A., Missier, P. (2019) 'Toward Trusted Open Data and Services', *Internet Technology Letters*, 2019,2:69. Available at: https://doi.org/10.1002/itl2.69

National Science Foundation (2024) 'NSF 24-581 - Cyber-Physical Systems (CPS)', Posted 4 June 2024 (replaces NSF 21-551), Available at: https://new.nsf.gov/funding/opportunities/cps-cyber-physical-systems/nsf24-581/solicitation (Accessed: 07 June 2024)

Neumaier *et al* (2023), *CEF2 RailDataFactory D1- Data Factory Concept, Use Cases and Requirements, Connecting Europe Facilities Digital Grant Agreement 101095272*, Available

at: https://www.digitale-schiene-deutschland.de/Downloads/2023-04-24_RailDataFactory_CEFII_Deliverable1_published.pdf (Accessed: 24 May2024)

Novarty, AK. (2021) 'The Outsourcing Conundrum: Misappropriation of intellectual property in supply chains', *Naval Res Logistics* 2021, 68:229-240, Available at: https://doi.org: 10.1002/nav.21942

Offermann, P., Levina, O., Schonherr, M., Bub, U. (2009) 'Outline of a Design Science Research Process', *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, pp1-11, Available at: https://doi.org: 10.1145/1555619.1555629

Omrany, H., Al-Obaidi, KM., Husain, A., Ghaffarianhoseini, A. (2023) 'Digital Twins in the Construction Industry: A Comprehensive Review of Current Implementations, Enabling Technologies, and Future Directions', *Sustainability*, Volume 15, pp.10908, Available at: https://doi.org/10.3390/su151410908

Open Data Institute (2023), *Responsible Data Stewardship*, Available at: https://theodi.org/insights/reports/defining-responsible-data-stewardship/ (Accessed: 04 April 2024)

Ogbeifun, E., Mbohwa, C., Pretorius, J-HC. (2016) 'Achieving consensus devoid of complicity: adopting the Delphi technique', *International Journal of Productivity and Performance Management*, Vol 66, No.6, pp 766-779, Available at: https://doi.org/ 10.1108/IJPPM-08-2015-0112

O'Leary T, Armfield T (2020), 'Adapting to the Digital Transformation', *Alberta Law Review, Energy Law Edition*, Volume 58, Issue 2, pp 249-272

OMG (2020), *Structured Assurance Case Metamodel (SACM) Version 2.1*, April 2020, Available at: https:/www.omg.org/spec/SACM/2.1/PDF (Accessed: 12 February 2021)

Palachuk, GF. (2020) 'The New Decade of Construction Contracts: Technological and Climate Considerations for Owners, Designers, and Builders', *Seattle Journal of Technology, Environmental & Innovation Law (SJTEIL)*, Volume 11, Issue 1, pp 171-213

Papacharalampopoulos, A., Giannoulis, C., Stavropoulos, P., Maurtzis, D. (2020) 'A digital twin for automated root-cause search of production alarms based on KPIs aggregated from IoT', *Applied Sciences (Switzerland),* Volume 10 (7), pp.2377, Available at: https://doi.org/10.3390/app10072377

Pickering, N., Duke, M., Kit Au, C. (2023), 'Towards a Horticulture System of Systems: A case study of modular edge AI, Robotics and an Industry Good Digital Twin', 18th *Annual System of Systems Engineering Conference, SoSe 2023*, Available at: https://doi.org/10.1109/SoSE59841.2023.10178520

Polacsek, M., Boardman, G., McCann, T. (2018) 'Understanding, Choosing and Applying Grounded Theory: Part 2'. *Nurse Researcher*, Available at: https://doi.org 10.7748/nr.2018.e1593

Peffers, K., Tuunanen, T., Rothenberger, MA., Chatterjee, S. (2007) 'A Design Science Research Methodology for Information Systems Research', *Journal of Management Information Systems*, 24:3, 45-47, Available at: https://doi.org/10.2753/MIS0742-1222240302

Phoon, K-K., Ching, J., Cao, Z (2022), 'Unpacking data-centric geotechnics', *Underground Space*, Volume 7 (6), pp.967-989, Available at: https://doi.org/10.1016/j.undsp.2022.04.001.

Piovesan, A., Griffor, E. (2017) 'Reasoning about safety and security: The Logic of Assurance', Handbook of System Safety and Security, pp.221-129, Available at: https://doi.org/10.1016/B978-0-12-803773-7.00007-3

Pombo, I., Godino, L., Sanchez, JA., Lizamaldo, R. (2020) 'Expectations and Limitations of Cyber-Physical Systems (CPS) and Advanced Manufacturing: A View from the Grinding Industry', *Future Internet* 2020, 12, 159, Available at: https://doi.org/10.3390/fi12090159

Provost, M. (2010) 'Bombardier Orbita: Railway Asset Management for the 21st Century', *MOD Reliability & Maintainability Seminar Defence College of Management and Technology*, 9th – 10th February 2010, Safety and Reliability, Volume 30, 2010-Issue 1, Available at: https://doi.org/10.1080/09617353.2010.11690903

Qi, Q., Tao, F., Hu, T., Anwer, N., Liu, A., Wei, Y., Wang, L., Nee, AYC. (2021) 'Enabling Technologies and Tools for Digital Twin', *Journal of Manufacturing Systems*, Available at: https://doi.org /10.1016/j.jmsy.2019.10.001

Qiao, L., Dang, S., Shihada, B., Alouini, MS., Nowak, R., Lv, Z. (2022) 'Can blockchain link the future?', *Digital Communications and Networks*, Vol 8, Issue 5, Available at: https://doi.org/ 10.1016/j.dcan.2021.07.004

Rail (2019), *TfL Agrees £1 billion sale and leaseback deal for Elizabeth Line trains, 22/03/2019* [Online], Available at: https://www.railmagazine.com/news/fleet/tfl-agrees-1-billion-sale-and-leaseback-deal-for-elizabeth-line-trains (Accessed: 08 April 2022)]

Rail Business UK (2021), *Desiro air-conditioning goes digital*, Available at: https://www.railwaygazette.com/uk/desiro-air-conditioning-goes-digital/60505.article (Accessed 16 February 2024)

Rail Engineer (2018), *Transport for London's new Old Oak Common Depot,* Available at: https://www.railengineer.co.uk/transport-for-londons-new-old-oak-common-depot/ (Accessed 08/ 04/2022)

Railway Gazette International (2013), *EIB Provides £500m Loan for Crossrail Trains, 13/12/2013* [Online], Available at: https://www.railwaygazette.com/eib-provides-500m-loan-for-crossrail-trains/38973.article (Accessed 08/04/2022)

Rail Industry Standard on Supplier Assurance (2021), RIS-2750-RST, Issue: 1.1, Date: December 2021 Available at: https://www.rssb.co.uk/standards-catalogue/CatalogueItem/RIS-2750-RST-Iss-1-1 (Accessed: Issue 1.0 22/01/2021, Accessed updated Issue 1.1: 12/07/2024)

Ramdas, A., Goncalves, DP., Duarte, P., Sunjka, B. (2020) 'Applying a Case Study Method in Systems Engineering Research', *INCOSE International Symposium*, Volume 30 (1), pp.1173-1787, Available at: https://doi.org/10.1002/j.2334-5837.2020.00819

Raptis, TP., Passarella, A., Conti, M. (2019) 'Data Management in Industry 4.0: State of the Art and Open Challenges', *IEEE Access*, Volume 7, Available at: https://doi.org/10.1109/ACCESS.2019

Rasheed, A., San, O., Kvamsdal, T., (2020), 'Digital Twin: Values, Challenges and Enablers from a Modelling Perspective', *IEEE Access*, Vol 8 21980-21012, Available at: https://doi.org/ 10.1109/ACCESS.2020.2970143

Redlinghuys, A., Basson, A., Kruger, K. (2020) 'A Six-Layer Architecture for the Digital Twin: A Manufacturing Case Study Implementation', *Journal of Intelligent Manufacturing*, Volume 31, pp.1381-1402. Available at: https://doi.org/10.1007/s10845-019-01516-6

Rock, S., Harris, J., Judson, R. (2021) *Legal Roundtable Outcomes Report*, Version 1.0, 13/01/2021, Published by cdbb, University of Cambridge (Not for Public Release)

ROGS (2006) – Railways and Other Guided Transport Systems (Safety) Regulations 2006 (as amended). Available at: www.legislation.gov.uk (Accessed: 05 June 2020)

Royal Academy of Engineering (nd), *Choosing the right sample size for your evaluation.* Available at: https://raeng.org.uk/programmes-and-prizes/programmes/uk-grants-and-prizes/ingenious-public-engagement-grants-scheme/evaluation/choosing-the-right-sample-size-for-you-evaluation (Accessed 02 February 2024)

RSSB (2017) *Autonomous Systems – Facing Up to the Regulatory Challenges*, RSSB Blog[online], 01 November 2017, Available from: https://RSSB.co.uk/InsightsandNews/Blogs/AutonomousSystems_FacingUpto Regulatory Challenges, (Accessed: 30 June 2020],

Ruhe, S., Nicolai, S., Bretschneider, P., Westermann, D. (2022) 'Real-Time Approach of Grid-Parallel Simulation for Automated Distribution Grids' *57th International Universities Power Engineering Conference (UPEC)*, Istanbul: Turkey pp. 1-6, Available at: https://doi.org/10.1109/UPEC55022.2022.9917713

Sahlab, N., Braun, D., Kohler, C., Jazdi, N., Weyrich, M. (2022), 'Extending the intelligent Digital Twin with a context modelling service: A decision support use case', *Procedia CIRP*, Volume 107, pp. 463-468, Available at: https://doi.org/10.1016/j.procir.2022.05.009

Santaguida, P., Dolovich, L., Oliver, D., Lamarche, L., Gilsing, A., Griffith, LE., Richardson, J., Mangin, D., Kastner, M., Parminder, R. (2018) 'Protocol for a Delphi consensus exercise to identify a core set of criteria for selecting health related outcome measures (HROM) to be

used in primary health care', *BMC Family Practice*, Volume 19, Issue 1, Article Number 152, Available at: https://doi.org/10.1186/s12875-018-0831-5

Sato, H. (2019) 'Using Grounded Theory Approach in Management Research', *Annals of Business Administrative Science* 18, 65-74, Available at: https://doi.org/10.7880/abas.0190326a, April 13, 2019

Saunders, M., Lewis, P., Thornhill, A. (2016) *Research Methods for Business Students*. England: Pearson Education Limited.

Schenk, A., Clausen, U. (2020) 'Creating Transparency in the Finished Vehicles Transportation Process Through the Implementation of a Real-Time Decision Support System' *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Singapore, Singapore, pp. 1017-1021, Available at: https://doi.org 10.1109/IEEM45057.2020.9309978.

Schoonenboom, J., and Johnson, RB. (2017) 'How to Construct a Mixed Methods Research Design', *Kolner Zeitschrift Fur Soziologie und Sozialpsychologie*, 69 (Suppl 2), 107-131. Available at: https://doi.org/10.1007/s11577-017-0454-1

SEBoK contributors (2024) *Guide to the Systems Engineering Body of Knowledge (SEBoK)*, v2.10, 06 May 2024, Available at: https://sebokwiki.org/w/index.php?title=Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK)&oldid=72061> (Accessed 10 June 2024)

Settani G, Shovgenya Y, Skopik F, Graf R, Wurzenberger M., Fiedler R (2017), *Acquiring cyber threat intelligence through security information correlation*, 2017 3rd IEEE International Conference on Cybernetics, CYBCONF 2017 – Proceedings, Doi: https://doi.org /10.1109/CYBConf.2017.7985754

Shafiee, ME., Rasekh, A., Sela, L. Preis, A. (2020) 'Streaming smart meter data integration to enable dynamic demand assignment for real-time hydraulic simulation', *Journal of Water Resources Planning and Management*, Volume 146, Issue 6. Available at: https://doi.org/10.1061/(ASCE)WR.1943-5452.0001221

Shaydullina, VK. (2018) 'Review of institutional and legal issues for the development of the Fintech industry', *European Research Studies Journal*, Volume 21 pp 171-178, ISSN 11082976

Siemens (2018) *MindSphere Security Model Version 1.0 Enabling customers to confidently operate in a secure cloud environment*, Available at: https://assets.new.siemens.com/siemens/assets/api/uuid:6b876b5e-5594-4da4-90e0-e9e0c6f1f1e1/version:1557483304/siemens-plm-mindsphere-security-model-wp-75966-a7.pdf (Accessed: 10 May 2024)

Siemens (2024) *Digital transformation for sustainable mobility – with Railigent X*, Available at: https://www.mobility.siemens.com/global/en/portfolio/digital-solutions-software/digital-services/railigent-x.html (Accessed 17th May 2024)

Si, Sheng-Li., You, Xiao-Yue., Liu, Hu-Chen., Zhang, P. (2018) 'DEMATEL Technique: A Systematic Review of the State-of-the-Art Literature on Methodologies and Applications', *Mathematical Problems in Engineering*, Hindawi, Available at: https:doi.org/10.1155/2018/3696457

Sim, J., Saunders, B., Waterfield, J., Kingstone, T. (2018) 'Can sample size in qualitative research be determined a priori?', *International Journal of Social Research Methodology*, Volume 21, Issue 5, Available at: https://doi.org/10.1080/13645579.2018.1454643

Sinclair, M., Siemieniuch, C., Palmer, P. (2019) 'The Identification of Knowledge Gaps in the Technologies of Cyber-Physical Systems with Recommendations for Closing those Gaps', *Systems Engineering*, 2019, 22:3-19, Wiley, Available at: https://doi.org/10.1002/sys-21464

Soares, MN., Kauffman, ME. (2018) 'Intellectual Property Law in the fourth industrial revolution: trade secrets risks and opportunities. *Revista Juridica*, 4 (53), pp.199-224

Son, B-G., Kim, H., Hur, D., Subramanian, N. (2021) 'The dark side of supply chain digitalisation: supplier-perceived digital capability asymmetry, buyer opportunism and governance', *International Journal of Operations & Production Management*, 41(7), pp 1220-1247

Stefanouli, M., Economou, C. (2019) 'Data Protection in Smart Cities: Application of the EU GDPR', *In: Nathanail E, Karakikes I (eds), Data Analytics: Paving the Way to Sustainable Urban Mobility. CSUM 2018, Advances in Intelligent Systems and Computing*, Volume 879, Pringer, Cham. Available at: https://doi.org/10.1007/978-3-030-02305-8_90

Stein, A. (2020) 'Artificial Intelligence and Climate Change', *Special Issue: Regulating the Technological Frontier, Yale Journal on Regulation*, Volume 37, Issue 3, pp 890-939

Su, S., Zhong, RY., Jiang, Y., Song, J., Fu, Y., Cao, H. (2023) 'Digital Twin and its Potential Applications in Construction Industry: State-of-art Review and a Conceptual Framework', *Advanced Engineering Informatics*, Volume 57, page 102030, Available at: https://doi.org/10.1016/j.aei.2023.102030

Sun, Y., Fesenko, H., Kharchenko, V., Zhong, L., Kliushnikov, I., Illiashenko, O., Morozova, O., Sachenko, A. (2022) 'UAV and IoT-Based Systems for the Monitoring of Industrial Facilities Using Digital Twins: Methodology, Reliability Models, and Application. *Sensors*. Volume: 22(17), pp.6444. Available at: https://doi.org/10.3390/s22176444

Teicher, U,. Ben Achour, A., Selbmann, E., Demir, OE., Arabsolgar, D., Cassina, J., Ihlenfeldt, S., Colledani, M. (2023) 'The RaRe2 Attempt as a Holistic Platform for Decision Support in Rapidly Changing Process Chains'. *In: Galizia, F.G., Bortolini, M. (eds) Production Processes and Product Evolution in the Age of Disruption. CARV 2023. Lecture Notes in Mechanical Engineering*. Springer, Cham. Available at: https://doi-org.derby.idm.oclc.org/10.1007/978-3-031-34821-1_38

Teoh, T., van Berne, B., Hindriks, I., Waldenfels, R., Eichhorn, T., Ivanov, T., Hong, M., Akerkar, R., Benkic, M., Sangwan, J., Russotto, R., Debussche, J., Cesar, J. (2019) *Deliverable 3.2 Case Study Reports on Constructive Findings on the Prerequisites of Successful Big Data Implementation in the Transport Sector*, Leveraging Big Data for Managing Transport Operations, Horizon 2020 Research Innovation Programme, Available at: https://cordis.europa.eu/project/id/770038/results (Accessed: 6 June 2020)

The Centre for Digital Built Britain (2018), *The Gemini Principles*, Available at: https://www.cdbb.cam.ac.uk/Resources/ResoucePublications/

TheGeminiPrinciples.pdf (Accessed: 18 June 2019)

The Railways (Safety Case) Regulations 2000 (SI 2000/2688), Available at: https://www.legislation.gov.uk/uksi/2000/2688/contents/made (Accessed: November 2020)

Tie, YC., Birks, M., Francis, K. (2019), 'Grounded theory research: A design framework for novice researchers', *SAGE Open Med*. Available at: https://doi.org/10.1177/2050312118822927

TRIB (2023), *Digital Twin Roadmap 2035*, Available at: https://trib.org.uk/roadmap, (Accessed 19/04/2024)

Trustworthy and Ethical Assurance of Digital Twins (TEA-DT), Available at: https://www.turing.ac.uk/research/research-projects/trustworthy-and-ethical-assurance-digital-twins-tea-dt (Accessed 20 October 2024)

Uehara Sasaki, HA., Cardozo de Mello, P., Aoun Tannuri, E. (2022) 'Digital Twin of a Maneuvering Ship: Real-Time Estimation of Drift And Resistance Coefficients Based on Ship Motion and Rudder and Propeller Commands.' *Proceedings of the ASME 2022 41st International Conference on Ocean, Offshore and Arctic Engineering. Volume 5B: Ocean Engineering; Honoring Symposium for Professor Günther F. Clauss on Hydrodynamics and Ocean Engineering*. Hamburg: Germany. June 5–10, 2022. ASME. Available at: https://doi.org/10.1115/OMAE2022-78714

Unknown Author. (nd a) *South West Trains Class 450.* Available at: https://live.staticflicker.com/2873/12910823025_8880092b02_b.jpg (Accessed: June 2021)

Unknown Author. (nd b) *A stock photo of train wheels.* Available at: https://cdn.railuk.co/wp-content/uploads/2017/06/24102346/Shutterstock_363488648-768x512.jpg (Accessed: June 2021)

Wang, J., Li, X., Wang, P. (2024) 'Bibliometric analysis of digital twin literature: a review of influencing factors and conceptual structure', *Technology analysis & strategic management,* 224, Vol 36 (1), p 166-180, Available at: https://doi.org/10.1080/09537325.2022.2026320

Wang, K-J., Lee, T-L., Hsu, Y. (2020), 'Revolution on Digital Twin Technology – A Patent Research Approach', *The International Journal of Advanced Manufacturing Technology* (2020) 107:4687-4704, Available at: https://doi.org/10/1007/s00170-20-05314-w

Wang, L. (2019) 'Overview and Analysis of Data Utilisation and Cases in China', *European Data Protection Law Review (EDPL)*, 5(1), 114-119.

Wang, P., Gao, RX., Fan, Z. (2015) 'Cloud Computing for Cloud Manufacturing: Benefits and Limitations', *Journal of Manufacturing Science and Engineering*, 137(4), p. 040901.

Wang, Y., Kang, M., Liu, Y., Li, J., Xue, K., Wang, X. (2023) 'Can Digital Intelligence and Cyber-Physical-Social Systems Achieve Global Food Security and Sustainability?' *In IEEE/CAA Journal of Automatica Sinica,* vol. 10, no. 11, pp. 2070-2080, Available at: https://doi.org/ 10.1109/JAS.2023.123951.

Watkins, D., Bolger, M., Hetherton, L., Harrison, SM., Cohen, RCZ. (2021) 'Using workspace to implement Digital Twins in the Mixed Reality Lab', *Proceedings of the International Congress on Modelling and Simulation, MODSIM*, pp.190-196, Australia: Modelling and Simulation Society of Australia and New Zealand Inc. (MSSANZ)

Wei, R., Foster, S., Mei, H., Yan, F., Yang, R., Habli, I., O'Halloran, C., Tudor, N., Kelly, T., Nemouchi, Y. (2024), *'ACCESS: Assurance Case Centric Engineering of Safety-Critical Systems', The Journal of Systems and Software*, 213 (2024) 112034, Available at: https://doi.org/10.1016/j.jss.2024.112034

Wei, R., Kelly, TP., Dai, X., Zhao, S., Hawkins, R. (2019*)* 'Model based system assurance using the structured assurance case metamodel', *The Journal of Systems and Software*, 154 (2019) 211-233, Available at: https://doi.org/10.1016/j.jss.2019.05.013

WIPO (2019*) Conversation on Intellectual Property (IP) and Artificial Intelligence (AI), WIPO/IP/AI/EE/INF4, October 31, 2019*, Geneva: WIPO, September 27, 2019, Available at: https://wipo.int/wipo_ip_ai_ge_19_inf_4.docx, (Accessed: June 2020)

World Economic Forum (2019), *World Economic Forum Centre for the Fourth Industrial Revolution*, Available at: https://www.weforum.org/centre-for-the-fourth-industrial revolution/about (Accessed 14 June 2019)

World Intellectual Property Organization (2010), *An Overview*, Available at: https://www.wipo.int/edocs/pubdocs/en/general/1007/wipo_pub_1007_2010.pdf (Accessed: 2 February 2020)

Wu, H., Zhang, G. (2020) 'Electronic Evidence in the Blockchain Era: New Rules on authority and integrity', *Computer Law & Security Review*, volume 36, April 2020, 105401, Available at: https://doi.org/10/1016/j.clsr.2020.105401

Yadykin, V., Barykin, S., Badenko, V., Bolshakov, N., de la Poza, E., Fedotov, A. (2021), 'Global challenges of digital transformation of markets: Collaboration and digital assets', *Sustainability (Switzerland)*, volume 13, issue 19, 10619, Available at: https://doi.org/ 10.3390/su131910619

Yan, M.-R., Hong, L.-Y. and Warren, K. (2022) 'Integrated knowledge visualization and the enterprise digital twin system for supporting strategic management decision', *Management Decision*, Vol. 60 No. 4, pp. 1095-1115. Available at: https://doi-org.derby.idm.oclc.org/10.1108/MD-02-2021-0182

Yeo, K., Ren, Y., (2009), 'Risk Management Capability Maturity Model for Complex Product Systems (CoPS) Projects', *Systems Engineering*, 13(4), Available at: https://doi.org/10.1002/sys.20123

Yitmen, I., Alizadehsalehi ,S., Akıner, İ., Akıner, ME. (2021) 'An Adapted Model of Cognitive Digital Twins for Building Lifecycle Management'. *Applied Sciences*. Volume 11(9). pp:4276. Available at: https://doi.org/10.3390/app11094276

Zanitti, M., Ferens, M., Ferrarin, A., Shien, M., Kosta, S. (2023) 'MetaLung: Towards a Secure Architecture for Lung Cancer Patient Care on the Metaverse', *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, Kyoto, Japan, 2023, pp. 201-208, Available at: https://doi.org/ 10.1109/MetaCom57706.2023.00047.

Appendix 1: Prior Work Literature Search Criteria

The initial Prior Work Study covers articles to the end of 2020 to represent the influence on the initiation of the research design. Any new publications from 2021 to June 2024 are also identified for impact on the current research project.

Question 1: What are the prior studies of legal issues with the adoption of digital technologies for decision support? Which of these studies specifically relates to intellectual property issues? Which of these studies specifically relates to Digital Twin?

Example Scopus Search

Criteria

Article Title, Abstract, Keywords = (("Legal issues" OR "Legal risks") AND ("Industry 4.0" OR "IIOT" OR "Digital Twin" OR "Additive Manufacture" OR "Smart Sensors" OR "Cyber-Physical Systems")

Screening Criteria

- In English
- Article or Conference Paper
- Subset concerned with understanding legal issues as opposed to just mentioning.

Scopus Search Results

Publication Type	To end 2020		2021 to June 2024	
	Pre-Screened (In English*)	**Screened**	**Pre-Screened (In English)**	**Screened**
Article	2	2	5	4
Conference Paper	8	6	7	6
Books, Book Chapters and Reviews	4	0	10	0
Total	14	8	22	10

Note * - 3 Additional Articles non in English (2 German, 1 Russian)

Screened to 2020 – specifically relates to IP issues = 0 (2018, Hallo & Gorod, 2020 mentions IP only)

Screened 2021-2024 – specifically relates to IP issues = 2

Screened to 2020 – specifically relates to Digital Twin = 0

Screened 2021-2024 – specifically relates to Digital Twin = 3

Screened Publications to end 2020

Screened Articles

Cinque, M. Russo, S. Esposito, C. Free-Nelson, F. Kamhoua, C.A. (2018), 'Cloud Reliability: Possible Sources of Security and Legal Issues?*'*, *IEEE Cloud Computing*, 5(3), pp. 31–38 (8 Citations)

Liu, H. Ning, H. Mu, Q. Huang, R. Ma, J. (2019) 'A review of the smart world', *Future Generation Computer Systems*, 96, pp. 678–691 (41 Citations)

Screened Conference Papers

Ghulam, S. Schubert, J. Tamm, G. Stantchev, V. (2014) 'Integrating smart items and cloud computing in healthcare scenarios', *SENSORCOMM 2014 - 8th International Conference on Sensor Technologies and Applications*, pp. 75–81 (1 Citation)

Rault, R. Trentesaux, D. (2018) *'*Artificial Intelligence, Autonomous Systems and Robotics: Legal Innovations*'*, *Studies in Computational Intelligence*, 762, pp. 1–9 2018 (14 Citations)

Habrat, D (2020) 'Legal challenges of digitalization and automation in the context of Industry 4.0', *Procedia Manufacturing,* 51, pp. 938–942 (13 Citations)

Hallo, L. Gorod, A.(2020) 'Engineering management principles for improving quality and efficiency in patient centred care', *ASEM 41st International Annual Conference Proceedings "Leading Organizations through Uncertain Times*" (1 Citation)

Alkhabbas, F. Spalazzese, R. Cerioli, M. Leotta, M. Reggio, G. (2020*)* 'On the Deployment of IoT Systems: An Industrial Survey, Proceedings', *IEEE International Conference on Software Architecture Companion*, ICSA-C 2020, pp. 17–24, 9095740 (16 Citations)

Lhotska, L. (2020) 'Application of industry 4.0 concept to health care', *Studies in Health Technology and Informatics*, 273, pp. 23–37 (10 Citations)

Screened Publications from 2021 to June 2024

Screened Articles

Aghimien, D.O. Aigbavboa, C. Edwards, D.J. Nash, H, Onyia, M. .(2022) 'A fuzzy synthetic evaluation of the challenges of smart city development in developing countries', *Smart and Sustainable Built Environment* 11(3) pp405-421 (49 Citations) - Six dimensions of Smart City Challenges identified from literature: governance, economic, social, technological, environmental and legal issues. Applications to a Smart City Case Study in Nigeria identified prominence of social and legal challenges.

Gillespie T (2022), 'Building trust and responsibility into autonomous human-machine teams'*,* *Frontiers in Physics*, 10, 942245 (2 Citations) – Identified areas for research in autonomous human machine team systems and where legal input is needed to minimise legal and financial risk.

Hsu C-H, He X, Zhang T-Y, Liu W-L, Lin, Z-Q, (2022) 'Enhancing Supply Chain Agility with Industry 4.0 Enablers to Mitigate Ripple Effects Based on Integrated QFD-MCDM: An Empirical Study of New Energy Materials Manufacturers', *Mathematics* 10(10), 1635 (8 Citations) – Study identified need to strengthen guarding against legal risks.

Yang RJ, Shang L, Zhang H (2022) 'Risk Factor Identification of the Information Technology Project based on the DEMATEL-ISM Model', *Journal of Engineering Science and Technology Review* 15(4) pp53-59 (1 Citation) – Established a risk factor system for information technology projects using expert analysis and DEMATEL. Political and legal risks identified as important. Identified importance of accurate needs analysis.

Screened Conference Papers

Clementson J, Wood P, Teng J (2021) 'Legal considerations for using digital twins in additive manufacturing a review of the literature', *Advances in Transdisciplinary Engineering* 15 pp 91-96) (1 Citation) – Paper related to current research study.

Gutsu S, Mkrtchyan M, Strielkina A (2021) 'Social and Legal Aspects of the Transition to Industry 4.0', *Lecture Notes in Networks and Systems* 188, pp726-737 (3 Citations) – Highlights trends and provides overview of socio-legal issues with Industry 4.0. Identifies IP as a new challenge relating to artificial intelligence.

Suffia G (2022) 'Legal issues of the digital twin cities in the current and upcoming European legislation: Can digital twin cities be used to respond to urbanisation problems?', *ACM International Conference Proceeding Series* pp 534-537 (0 Citations) – Describes ongoing research relating to "Digital Twin Cities" and considers legal and ethical issues identifying four: ethics of software use, compliance with legislation, using personal data and role of independent authorities.

Bundin M, Martynov A, Shireeva E (2022), 'Legal Issues on the Use of "Digital Twin" Technologies for Smart Cities', *Communications in Computer and Information Science* 1529 CCIS, pp77-86 (1 Citation) – Discusses formation of regulation and challenges of DT technologies for public administration. Declares the most important issues as data security, personal data protection, ensuring personal rights and freedoms and liability sharing.

Shimpo F, (2023) 'Legal Issues Concerning Cybernetic Avatars', *Frontiers in Artificial Intelligence and Applications*, 366, pp640-648 (0 Citations) – Examines the legal implications of avatars and identifies a need to consider international legal issues.

Gomathi L, Mishra AK, Tyagi AK (2023), 'Industry 5.0 for Healthcare 5.0: Opportunities, Challenges and Future Research Possibilities', *7th International Conference on Trends in Electronics and Informatics, IC)EI 2023 – Proceedings* pp204-213 (41 Citations) – The study considers the potential of Healthcare 5.0 and the challenges that need to be considered for successful implementation. These issues include mention of ethical and legal issues as well as data security.

Example Scopus Search

As the numbers of articles found was low and to explore Prior work relating to Intellectual Property and Digital Twins further searches with broader criteria were carried out. For example*:*

Criteria

Article Title, Abstract, Keywords = ("Intellectual Property") AND ("Digital Twin")

Screening Criteria

- In English
- Article or Conference Paper

- Subset concerned with understanding legal issues as opposed to just mentioning.

Scopus Search Results

3 Articles to end 2020, all of which were relevant qualitative studies as follows:

Jæger B.; Bach T.; Pedersen S.A.(2019), 'A Blockchain Application Supporting the Manufacturing Value Chain', *IFIP Advances in Information and Communication Technology* - Discusses the use of blockchain in the supply chain and applies to a case study. Mentions that blockchain can be used in the life cycle management of digital twins to protect IP and enforce license agreements.

Kartskhiya A.; Makarenko D. (2019), 'Status and risks of artificial intelligence: Legal aspects', *CEUR Workshop Proceedings* – Discusses legal issues with AI and need to create a legal framework and rules for their use.

Wang K.-J.; Lee T.-L.; Hsu Y. (2020), 'Revolution on digital twin technology—a patent research approach', *International Journal of Advanced Manufacturing Technology* – Provides a view on the scope of worldwide patents for Digital Twin technologies.

Criteria

Article Title, Abstract, Keywords = ("Legal Issues") AND ("Digital Technologies")

Screening Criteria

- In English
- Article or Conference Paper
- Subset concerned with understanding legal issues as opposed to just mentioning.

Scopus Search Results

53 items of which 31 to the end of 2020, 29 of which in English. Of these 29, 20 relate to Articles and Conference Papers.

Example papers of interest:

Gooding P (2019), 'Mapping the rise of digital mental health technologies: Emerging issues for law and society', *International Journal of Law and Psychiatry*, 62, 101498 (34 Citations) – Explore socio-technical issues of digital technologies

Shaydullina VK (2018), 'Review of institutional and legal issues for the development of the Fintech Industry', *European Research Studies Journal*, 21, pp171-178 (3 Citations) – Aimed to identify the institutional and legal methods for FinTech Industry development through assessment of experience to date.

Stefanouli M (2019), 'Data protection in smart cities: Application of the EU GDPR', *Advances in Intelligent Systems and Computing*, 879 pp748-755

Example HeinOnline Search

Criteria

Article Term, Title, Author, Citation = ("Intellectual Property" AND "Risk" AND ("Industry 4.0" OR "IIOT" OR "Digital Twin" OR "Additive Manufacture" OR "Smart Sensors")

Screening Criteria

- In English
- Article or Conference Paper

- Subset concerned with understanding legal issues as opposed to just mentioning.

Scopus Search Results

From 1995 to 2000 search identified 38 articles but 0 were relevant. The issue was due to "IIoT" picking up "Irrevocable Income Only Trusts".

Criteria were modified to focus on Digital Twin as follows:

("Intellectual Property" AND "Risk" AND "Digital Twin") in All Databases

From 1995 to 2000 no articles found

From 2000 to 2020, 11 articles found of which 10 were relevant based on title. On closer reading these 10 were reduced to 5 applicable, 3 not directly applicable but potentially transferable issues and 2 not applicable.

The 5 most applicable articles are as follows:

Cole A (2018), 'An update on BIM under English Law', *Construction Law International*, Vol 13, Issue 2 (July 2018) pp 51-55 – Discusses the legal and practical implications of using BIM in construction projects and the importance of ensuring risk allocation and contractual architecture for digital twin of an infrastructure system are appropriate. It discusses the differences between traditional contracting with adversarial risk transfer and collaborative contracting and identifies recent case law cautioning on the need to ensure IP rights are clear at the outset and that contractors and consultants may need to protect know-how and confidential information from disclosure to current or future competitors

Mauritz K (2020), 'AI & Intellectual Property: Towards an Articulated Public Domain', *Texas Intellectual Property Law Journal*, Vol 28, Issue 3 pp297-342 – Discusses output data from a Digital Twin's AI and machine learning process stating that such qualifies for a sui generis data base right but clarifies that an AI system than generated data and created a database cannot own the sui-generis database rights because an AI system has no legal personhood.

O'Leary T, Armfield T (2020) 'Adapting to the Digital Transformation'*, Energy Law Edition, Alberta Law Review*, Vol 58, Issue 2 pp 249-272 – Discusses challenges of AI use with Digital Twins and risk from 3rd parties teaching AI and whether a licence is sufficient to secure rights.

Druetta C (2018). 'Legal Perspectives on Predictive Maintenance: A Case Study', *International In-House Counsel Journal*, Vol 11, Issue 44 pp1-7 – Discusses legal issues and identifies clarity of data ownership as a particular issue. Highlights risk from 3rd party analytics providers obtaining copy of data stored and using this to the detriment of the manufacturer.

Palachuk GF (2020), 'The new decade of construction contracts: Technological and Climate Considerations for Owners, Designers and Builders'*, Seattle Journal of Technology, Environmental & Innovation Law (SJTEIL)*, Vol 11 Issue 1 – Discusses risk to contracting parties from proprietary information and IP and comments on need to clarify ownership and obligations.

Example Internet Search

"Digital Twin Programme"

- National Digital Twin Programme (Gov.UK)
- National Digital Twin Programme (Digital Twin Hub)

- National Digital Twin Programme (Centre for Digital Build Britain)
  UK Digital Twin Centre (Digital Catapult)
- Digital Twin Hub (Connected Placed Catapult)

"Digital Twin US"

- Digital Twin Consortium (digitaltwinconsortium.org)

Question 2: What are the prior studies to understand risks to multi-stakeholder collaboration of complex systems ? Which of these studies specifically relates to intellectual property issues? Which of these studies specifically relates to Digital Twin ?

Example Scopus Search

Criteria

Search 1: Article Term, Title, Author, Citation = ("Risk" AND "stakeholder" AND "collaboration" AND ("complex system" OR "BIM" OR "Digital Twin" OR "complex" OR "system")

Search 2: Search 1 AND "Intellectual Property"

Search 3: Search 1 AND "Digital Twin"

Screening Criteria

- In English
- Article or Conference Paper
- Subset concerned with understanding legal issues as opposed to just mentioning.

Scopus Search Results

Article Term, Title, Author, Citation = ("Risk" AND "stakeholder" AND "collaboration") = 3,255 documents

Search 1: = 1,450 documents

Search 1 (Screening - English): 1,426 English (8 French, 6 German, 4 Chinese, 3 Italian)

Search 1 (Screening – Article or Conference): 1,120 documents

Search 1 (Screening – Legal): Search 1 + AND "Legal" : 51 documents of which 26 to end 2020 (the remainder are 2021 to 2024)

Keywords in these documents were : "Article", "Risk Assessment", "United States", "Human", "Legal Aspect".

For Example those with keyword = "Risk Assessment" are:

Journal Papers (2 of 3 relevant)

Almarri K, Aljarman M, Boussabaine H (2019), 'Emerging contractual and legal risks from the application of building information modelling', *Engineering Construction and Architectural*

Management, 26(10) pp 2307-2325 – Primary data from questionnaires combined with literature review. Intellectual property rights and liability was an identified as one of the issues of concern.

Goeke L, Mohammadi NG, Heisel M (2018), 'Context analysis of cloud computing systems using a pattern-based approach', *Future Internet* 10(8) 72 (4 Citations) – use of the pattern in design stage to support risk assessment.

Conference Papers (1 of 2 relevant)

Huzaimi Abd Jamil A, Syazli Fathi M (2019), 'Contractual issues for Building Information Modelling (BIM)- based construction projects: An exploratory case study', *IOP Conference Series: Materials Science and Engineering*, 513(1) 012035 – exploratory case study using Qualitative Context Analysis applied to a BIM project to establish the legal and contractual risks to include IP. Applied in a Malaysian context.

Search 2: Search 1 AND "Intellectual Property"

2 Documents (1 Article, 1 Conference Paper)

Mastio E, Dovey K (2019), 'Power dynamics in organisational change: an Australian case', *International Journal of Sociology and Social Policy* 39(9-10) pp796-811 (3 Citations) – Explored abstract forms of power in organisational change. Applied to an Australian IP law firm.

Huzaimi et al, 2019 – identified above.

Search 3: Search 1 AND "Digital Twin"

2 Documents (2 conference papers) – Neither applicable as focus is using Digital Twin to manage collaboration risk rather than collaboration risk using Digital Twin.

Other broader searches included ("Risk" OR "Issue") AND "BIM" AND "Intellectual Property"

Question 3: What are the prior studies to develop Risk Management and Systems Assurance related to complex systems and Digital Twins? Which of these studies specifically relates to intellectual property issues?

Criteria

Search 1: Article Term, Title, Author, Citation = ("Risk Management" AND "systems assurance")

Search 2: Search 1 AND "Complex systems"

Search 3: Search 1 AND "Digital Twin"

Screening Criteria

- In English
- Article or Conference Paper
- Subset concerned with understanding legal issues as opposed to just mentioning.

Scopus Search Results

Search 1: 17 documents of which 13 to 2020.

Screened for further consideration to 2020 = 3 later than 2010

Shoemaker D.; Woody C.(2015), 'Model-based engineering for supply chain risk management', *CrossTalk* (0 citations) – Suggests using Architecture Analysis & Design Language (AADL) for describing components to facilitate their life-cycle management.

Martin Y.-S.; Kung A.(2018), 'Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering', *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*, doi.org /10.1109/EuroSPW.2018.00021 (48 citations) – Position Paper relating introduction of privacy into software engineering tools.

Baldwin K.; Popick P.R.; Miller J.F.; Goodnight J. (2012), 'The United States Department of Defense revitalization of system security engineering through program protection', *SysCon 2012 - 2012 IEEE International Systems Conference, Proceedings* doi.org: 10.1109/SysCon.2012.6189463 (15 citations) – integration of security into systems engineering.

Criteria

Search 4: Article Term, Title, Author, Citation = ("Develop" AND "assurance" AND "framework" AND "complex system")

Scopus Search Results

Search 4: 13 documents of which 12 to 2020 but only 6 after 2010. Only 1 document after 2020

Documents of interest include:

Hessami A.G.; Karcanias N.(2009), 'Complexity, emergence and the challenges of assurance the need for a systems paradigm', *IEEE International Systems Conference Proceedings*, doi.org:10.1109/SYSTEMS.2009.4815779 – Develops a framework for understanding emergent properties of complex systems and states that a systems approach is needed. Focusses on safety, security and sustainability performance.

Murugesan A.; Wong I.H.; Stroud R.; Arias J.; Salazar E.; Gupta G.; Bloomfield R.; Varadarajan S.; Rushby J.(2023), 'Semantic Analysis of Assurance Cases using s(CASP')', *CEUR Workshop Proceedings* – Automation strategies for supporting with creating and assessing assurance cases. Builds on Assurance 2.0. Uses a goal-directed top down solver.

Appendix 2: Grounded Theory Process Examples

A2.1 Example Coding

Each line from the questionnaires and interviews and batch of literature was initially reviewed for relevant factors. Coded framework requirements for managing perceived legal risks with Digital Twins were prefixed "F". Coded risks of concern for managing collaboration with Digital Twins were prefixed "R". An integer was used to give each code a unique identifier, so R1, R2…Rn where n is an integer.

Examples of initial coded factors and related quotes are as follows. A particular quote may contribute to multiple initial codes.

Examples of Initial Coded Factors	**Example quotes**
R7 Data rights - Unclear - No common understanding/ interpretation - Not fit for purpose	"The novation of contracts at the time of privatization was difficult. It was difficult to know what information you could get access to. There were issues with **interpretation** of contracts. There always seems to be parts of **information missing** with the supplier…**interpreting** that the asset owner doesn't' have rights to the information and the asset owner stating they do have rights. To resolve these issues "licensing agreements" have been established, but it takes a long time to get the information. There is **no common understanding of rights within contracts**. Entitlements are **not clear**. "
R9 Intellectual Property access restriction - Inhibits Predictive Maintenance Purpose - Drives Reverse engineering	Legal and IPR is a big risk. For **predictive** Digital Twin these issues pose challenges. For example, for **Predictive** Digital Twin in order to understand the behaviour of the asset e.g. engine, there may be a need to carry out a degree of **reverse engineering**, if design information is not available. There can be **reluctance** by OEMs **to share** design information due to the perceived level of **commercial interest** and potential future competition." "Clients have not yet got to grips with what digital IP they want and so are not yet able to tell the supply chain. For example, the

Examples of Initial Coded Factors	**Example quotes**
- Impacts Business Case	client looks for 2D drawings associated with digital delivery of models with the **contractor retaining the 3D models**." "**Cost and sharing of data** with other parties."
F1 Purpose/need - Focus on - To improve reliability and availability - For predictive maintenance - For safety	"Understanding who the end user is and ensuring cross-industry stakeholder solutions remain **focused on** this **need**." "Predictive Digital Twins will look **to improve reliability and availability** – it is intended to use data to produce **predictive** models for "pro-active **maintenance**"" "..have we got access to the information. Back to the IP issue and the different stakeholder **needs**." "Digital Twin will provide richer root cause assessment and influence **safety** cases."
F2 Business Value/ Benefits Case - Value of purpose - Costs of solution (actual/estimate)	"They are managed through our project management frameworks however **compute costs of simulation** in the public cloud are hard to estimate until you have built the model." "Understanding the **value** and convincing management for the need to invest." "If **lease** does not involve the [redacted] in maintenance there is little the [redacted] can do as **value** is driven by the operator BUT on "soggy **lease**" where the [redacted] is involved in heavy maintenance there is **value** in condition monitoring and Digital Twin."
F3 Leadership - Contract Boundaries - Clarity	"Hardware and software architectures cross traditional **contract boundaries**. There are stakeholders with specialisms e.g. firmware, but there needs to be systems integration to pull the specialisms together – there is no guidance on how to do this at present."

Examples of Initial Coded Factors	**Example quotes**
	"Lack of **clarity** and **leadership**" "The asset owners should be driving what they want.."
F4 Obligations - Information share - Lifecycle - Continuity	"There's a need to determine how far we need to go to **share information** to meet needs and **obligations**." "**Continuity** of data management over the asset **life** is a challenge. This can come from the asset owner, who is involved for the **lifetime** of the asset. The asset owner can provide access to historic data for predictive analysis e.g. with a new lease and Train Operator."
F6 Systems Approach - Requirements - Architecture - Interfaces - Framework - Systems Integration - Stakeholders - Standards	"There aren't sector level **frameworks** for data. PAS 1192 **framework** for BIM is followed but clients are not yet asking for it." "The asset owners should be driving what they want as, to fill the **requirements** gap, they get what they are given from suppliers. New **systems** will drive requirements." "Lack of user **requirements**."
F7 Standardisation - Common architecture - Data Platform - Data Exchange - Sharing	"**common** rail platform and **standard** for **data exchange**" "Each party is developing their ***own*** **data platforms** rather than developing ***shared*** platforms at present."

Examples of Initial Coded Factors	Example quotes
F8 Contracts - Data Own/Share	"Data Issues – term of "**Data Sharing** is better and much preferred to "**Data Ownership/Rights** – current sector culture is sceptical relating to data but this could be because **Data Sharing** on the scale to benefit from Digital Twin is new."
F9 Change and Transition	"Cultural issues and adaptability to **change"** "midlife upgrades" "standards **changes**" "..need to consider the **transition** from older (pre-digital age) assets to a future where assets are design with a digital lifecycle in mind."

Table A21: Sample of Coding

Issues were separately coded from literature and pre-fixed with "C" where they relate to characteristics considered important for legal risk management and "L" for legal issues. Examples are listed in **Appendix 4**.

The codes from literature were then related to the codes from the questionnaires and interviews as there was some overlap. The analysis was captured as a Memo and the resulting set of codes was used as the basis for relating to the quantitative questions and then for testing theoretical saturation.

A2.2 Theoretical Saturation Test

The chronology of data gathering is illustrated in Table A2.2.1 with the final column identifying the stage of coding and where saturation was identified.

Source	Count	Timeframe	Coding Stage
Rail Sector Interviews Rail Operator 15/06/20 Asset Owner/Maintainer (Rolling Stock) 04/09/20 Asset Owner/Maintainer (Infrastructure) 14/05/20	3	May 2020 to Dec 2020	Initial Coding – All new categories
Energy Sector Interviews Digital Twin Supplier to Energy Sector 30/10/20	2		

Source	Count	Timeframe	Coding Stage
IGEM 24/07/20			
Questionnaire Responses Direct approaches to rail companies and IGEM sent out to committee members (18/09/20)	7		
Subtotal	12		
Rail Sector Interviews Asset Owner/Maintainer (Rolling Stock) 08/01/21	1		
Separate Literature Analysis for Coding – Documented in Confirmation of Registration March 2021	-	Dec 2020 to Mar 2021	Initial Coding and Focussed Coding
Questionnaire Responses (additional) Noting RFM sent out to Rolling Stock Leasing Companies, Operators, OEMs and Tier 1s on 28/12/20. Derby Railway Society also supported with contacts.	9	January 2021 to December 2021	Review Coding and Focussed Coding Iteratively. Relate coding from Literature with Questionnaires and Interviews Reflect on saturation
Subtotal	10		
Total to end of December 2021	22		
Questionnaire Responses (additional) Focus on Rail Sector – strengthening Operations lifecycle stage view	3	January 2022 to April 2022	Reflect on saturation – Theoretical saturation confirmed for Rail Sector and to take forward to test on rail sector Case Studies.
Literature Search and Analysis Focussed on Gaps in Focussed Coding	-		Focussed Coding – expanding on explanations
Total to end of April 2022	**25**		

Table A22.1: Theoretical Saturation

Codes were related to the consolidated set to see where a code was identified for the first time. This was then identified as a new code for that chronological set. There was only one interview in the period of literature analysis.

Chronology	May to Dec 20	Literature plus Interview to Mar 21	Quest. To Dec 21	Quest. Jan 22-Apr 22
Participant Numbers	12	1	9	3
Number of New Codes (related to consolidated set)	14	5	0	0

Table A22.2: Participant Numbers

A2.3 Example Purposive and Theoretical Sampling

The literature review in Stage 1 formed the basis of Purposive Sampling which directed the design of the initial questionnaires and semi-structured interviews and identified the types of participants to be targeted. Theoretical sampling progressed from the initial codes and categories to address gaps in understanding, clarify uncertainties and assess interpretations.

The University of Derby library database was used to identify literature for explanation. Typically the search criteria related to a coded factor or category, for example Title or Abstract contains: ["Assurance Framework"] or ["Intellectual Property" AND ("value" OR "business case")] or ["Digital Twin" AND "Architecture"] . The main purpose was to elaborate and refine categories relating to the theory. Theoretical sampling continued until no new properties emerged relating to the purpose of the search.

A2.4 Example Memo Extracts

A2.4.1 Consolidating Coding from Literature, Questionnaires and Interviews

The following table is an example extract of a memo used to draw together similar codes and related context from literature, questionnaires and interviews.

Coded Framework Characteristic from Literature	**Summary of Importance**	**Coded Key Risks of Concern (Risk) or Framework Requirement for managing legal risks (Framework) from Questionnaires and Interviews**
C1: Purpose	Clear purpose to include productivity and quality objectives. For example, predicting when maintenance is due and scheduling before in-service failures occur. Ability to achieve the purpose will have direct legal implications, for example where it contributes to regulatory or contractual duties and	F1: Purpose/need for Digital Twin and Services R3: Purpose for the Digital Twin is unclear or cannot be achieved

Coded Framework Characteristic from Literature	Summary of Importance	Coded Key Risks of Concern (Risk) or Framework Requirement for managing legal risks (Framework) from Questionnaires and Interviews
	derived implications from the implementation of the purpose.	
C2: Value Case (Cost Benefit Evaluation)	The benefits of achieving the purpose are balanced against the lifecycle costs and this informs the implementation choices. Legal considerations relating to Intellectual Property management, including the cost-benefit from protection of designs and data and access and related contractual obligations, will need to be part of this value case. Moyne *et al* (2020) stresses that the financial benefit of correct operation of the Digital Twin in its environment also needs to be balanced against the costs of incorrect operation in the environment and this needs to be ascertainable and quantifiable.	R2: Inability to make the Cost-Benefit/ROI/Business Case for each dependent stakeholder over the asset lifetime F2: Business Value/Benefits Case
C3: Models and Frameworks	The literature identifies requirements based frameworks and feature based frameworks. These frameworks may allow a systematic evaluation of legal risks, for example identifying the Intellectual Property and licencing issues	F10: Use of existing frameworks

Coded Framework Characteristic from Literature	Summary of Importance	Coded Key Risks of Concern (Risk) or Framework Requirement for managing legal risks (Framework) from Questionnaires and Interviews
	associated with the framework elements with traceability to Value Case and Purpose.	
C4: Architecture	Features include: - Modularity and Re-Use - Integration - Data: reference library, foundation data model, information template which considers ownership and sharing rules	F6: Systems Approach: Requirements, Architectures and Interfaces F7: Common Sector Architecture and Data Exchange Standard for Implementation
C6: Stakeholder Collaboration	Failure to collaborate can have legal implications through contract in relation to Quality of Service or directly, depending on the use case and impact, on safety and security.	R4: Unable to maintain trust and effective collaboration over the lifecycle to maintain the purpose F5: Sector Life-Cycle Collaboration Agreement

Table A24.1: Memo Extract – Relating Codes (Characteristics)

Coded Legal Issue with Digital Twin from Literature	**Example Areas from the Literature**	**Related Coding from Questionnaires and Interviews**
L1: Intellectual Property: Digital Twin Parts (Data, Services, Models, Connections, Digital Twin) and Physical Twin	Data: Ownership and Sharing, Data Use Agreements. Applicability of trade secrets, contracts and database rights for protecting data and data sets. Virtual Models Representing Protected Physical Assets and Processes: Patents, Design Rights and Trade Secrets Digital Twin Infrastructure: Ownership, Patents and Design Rights Licence Management	R2: Value Case - Changes in Value of Intellectual Property in "as designed" data over Asset Lifecycle impacting access to data
L2: Legal Compliance: Data Protection, Security and Information Governance	Usage Restrictions Privacy, Trust and Security Authenticity/ Traceability Information Governance	R8: Unclear data management responsibilities and data access conditions to achieve life-cycle Design Support Use Cases F8 Data Management Agreements (Sharing/ Quality/ Maintenance/ GDPR/ Confidentiality)

Coded Legal Issue with Digital Twin from Literature	Example Areas from the Literature	Related Coding from Questionnaires and Interviews
L3: Liabilities e.g. impacts of decisions made using Digital Twins and relationship with decision capability, data quality, artificial intelligence, service failures and sharing and segregation of liabilities	Guaranteed capability over defined period in a defined environment E.g. data quality such as completeness, consistence and prevision. 5Vs of Data (Volume, Velocity, Veracity, Variety, Volume), access to computing infrastructure (edge, and cloud computing) Decision Making (Physical Realism/Accuracy and Reliable Future Projections Risk of in-service product failure and liability. Decision making by automation and Artificial Intelligence – levels of autonomy should not undermine the ability to monitor, supervise and intervene (RSSB, 2017)	R4: Unable to maintain trust and effective collaboration over the lifecycle to maintain the purpose F4: Stakeholder Obligations and Responsibilities
L4: International Legal Issues, particularly as services and infrastructure can cross national borders; internet governance	Regulatory Interoperability Demonstrating safety, reliability of machine learning models.	International Dimension not explicitly identified in the interviews and questionnaires although relates to:

Coded Legal Issue with Digital Twin from Literature	Example Areas from the Literature	Related Coding from Questionnaires and Interviews
	Sharing and segregation of liabilities between stakeholders Internet Governance Liability for a failed or unavailable system.	F4: Stakeholder Obligations and Responsibilities

Table A24.2: Memo Extract – Relating Codes (Legal Issues)

A2.4.2 Diagrams to Visually Support Analysis of Relationships between Factors

The following diagrams are examples of visual Memos used to relate factors as part of the analysis. These visual Memos led to Theoretical Sampling of academic and online literature and re-analysis of collated literature to explore the relationships and further refine.

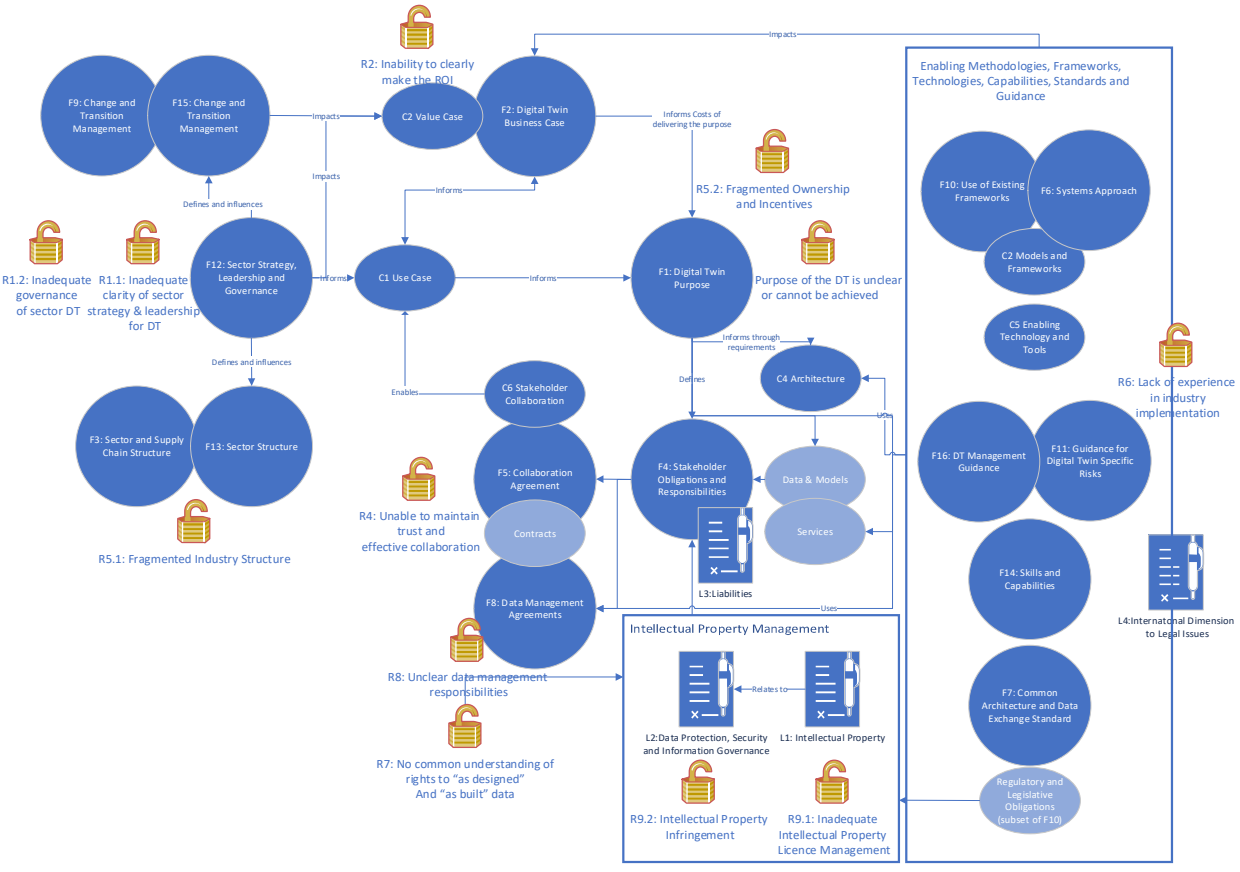


Figure A2.4.1: Relating Codes Visually (Example 1)

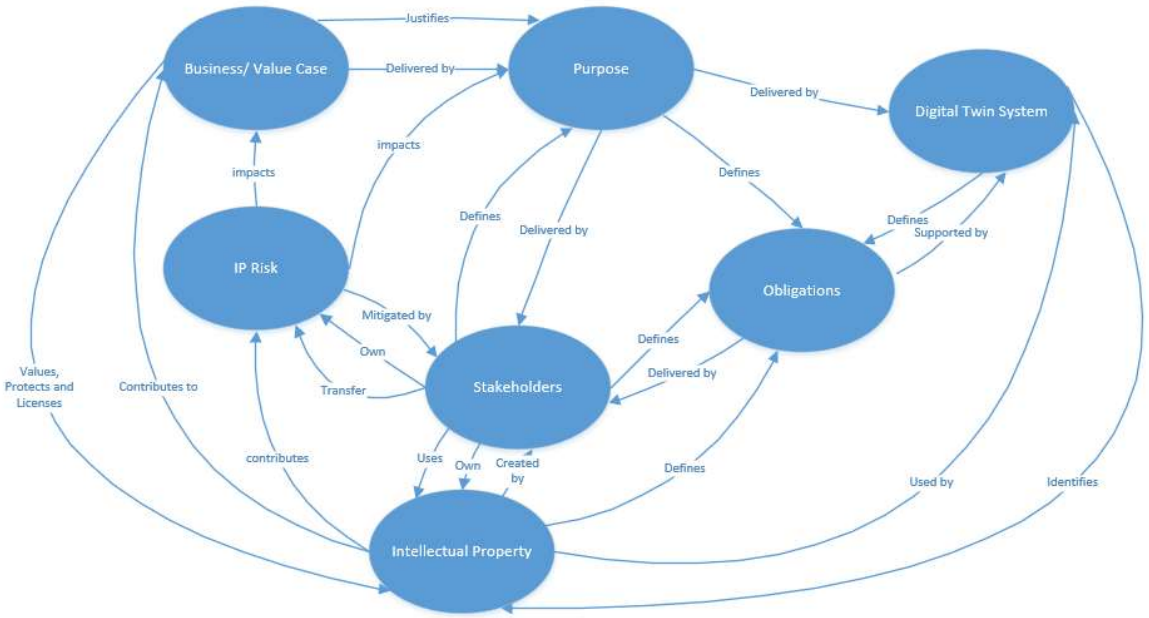


Figure A2.4.2: Relating Codes Visually (Example 2)

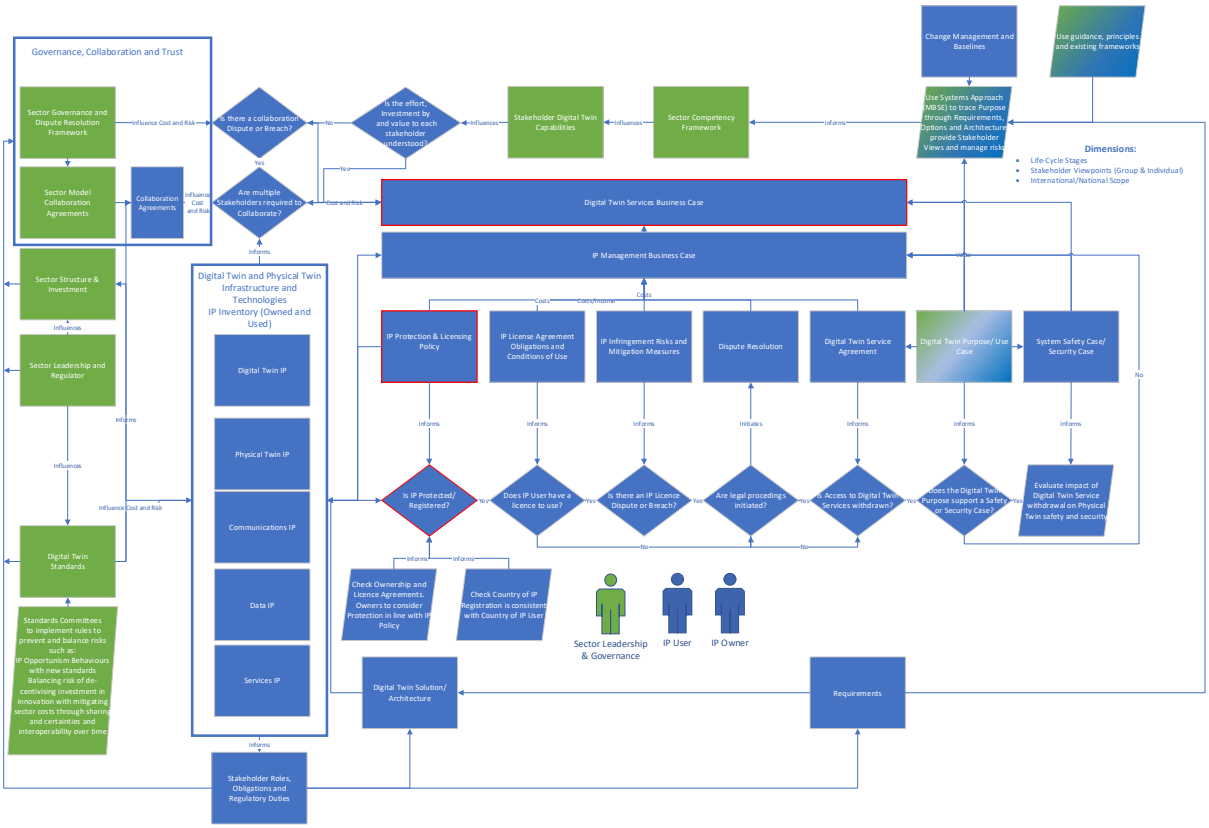


Figure A2.4.3: Relating Codes Visually (Example 3)

A2.4.3 Analysis of Categories of Factors and their Relationships

As the analysis progressed Memos exploring the relationship between groups of factors and how they relate to manage risk were developed. These had a standard format for capturing analysis and supporting data as shown by the template in Figure A2.4.5 below.

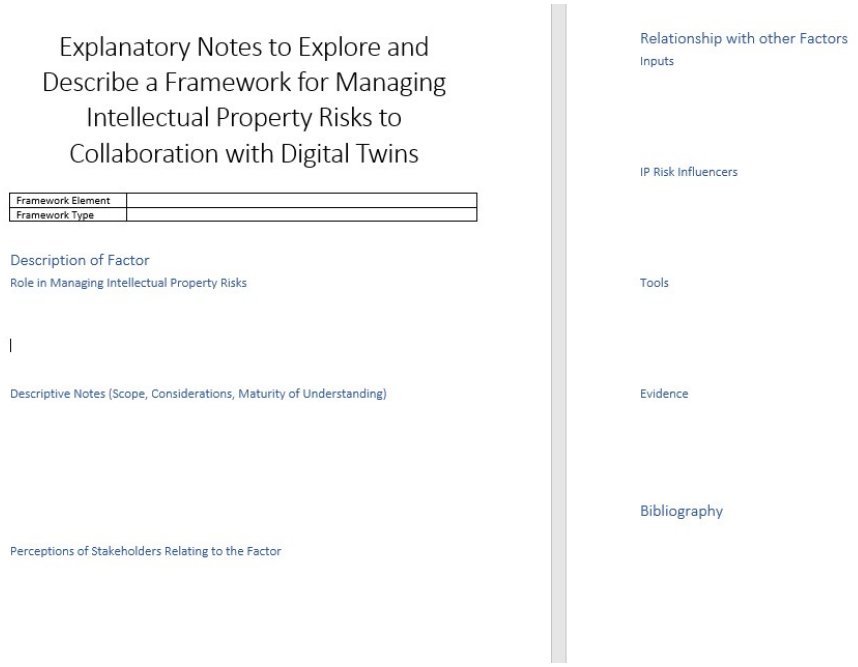


Figure A2.4.5: Structured Memo Template

Appendix 3: Ethics Approval

A3.1 Introduction

Data collection involved semi-structured interviews and questionnaires in Stage 2 and participant review of the framework during Stage 3. The ethical issues with these two stages were considered and each of these two stages were planned and submitted for ethical review and approval to the University of Derby, College of Science and Engineering Ethics Committee. The ethical considerations and approvals are summarised in the following sections.

A3.2 Ethical Considerations for Interviews and Questionnaires

The considerations for the semi-structured interviews and questionnaires were:

- Criteria for selecting participants and approach to recruitment. (A3.4)
- Consent to participate in the research study for the purpose of data collection and review and clarity on the process for withdrawal of consent by a declared date, before the results are published. (section A3.5)
- Consent to be approached for follow-up questions. (section A3.5)
- Clarity as to how collated data is used and stored.
- Anonymity of results and quotes presented in the research results.
- Ensuring the participant has visibility of interview notes and opportunity to clarify any points recorded.

Anonymity in attributing a particular response to an individual participant was considered to ensure participants were confident to freely express views from their professional experience. Data was stored in a restricted area of the University cloud, accessible to the researcher.

The design of the interviews and questionnaires and the justification of each question in relation to the research aims was also presented.

A3.3 Ethical Approval

Ethics application reference ETH1819-0080 was submitted for the overall research approach and for carrying out the semi-structured interviews and questionnaires. This application was approved subject to providing visibility of the questionnaire in its final form and approach to pre-consent of any follow-up. This was reviewed by the University data governance team

January 2020. The interviews were carried out using Microsoft Teams with manual recording of notes and quotes that were passed to the participant for review. The questionnaires were administered using Microsoft Forms. Results were exported to Microsoft Excel for analysis.

Ethics application reference ETH2223-5311 was submitted for the process of participant review of the risk framework. This was approved September 2023. A presentation using Microsoft PowerPoint, led the participant through a briefing, including consent, research background and then presented aspects of the framework and asked questions which were recorded on screen into the presentation. An extract of the slides used for the review, including consent are provided in Appendix 8.

A screenshot of the approval status within Haplo Ethics Manager is recorded as Figure A3.1.

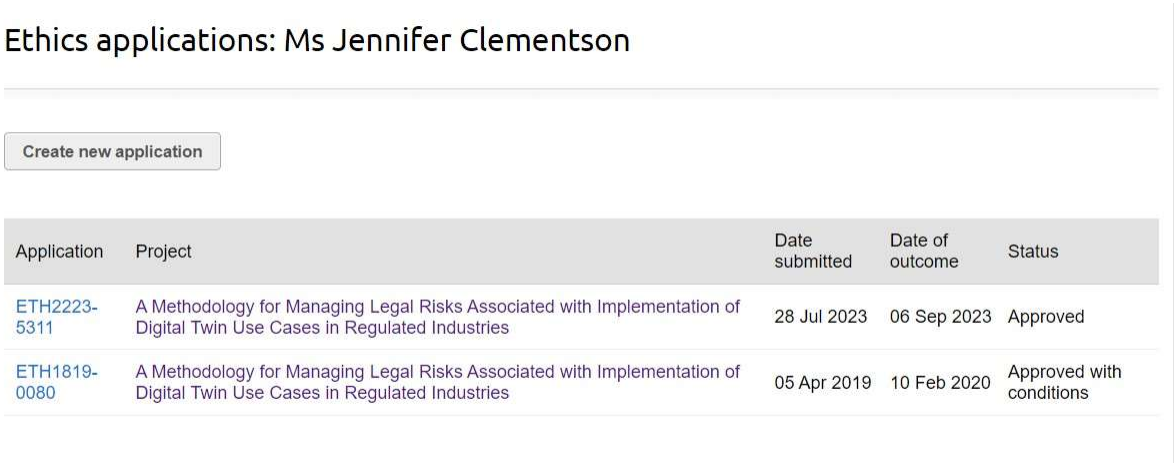


Figure A3.1 Screenshot of approval status within Haplo Ethics Manager

A3.4 Participant Recruitment

The participants for the questionnaires and interviews were sought from companies within target sectors with responsibility for Physical Entity management during a part of the life-cycle such as Physical Entity manufacturers, owners, operators, maintainers and consultants involved in Physical Entity management services. Two sectors were initially targeted with the support of sector membership bodies. For rail this was primarily Rail Forum UK with some support from the Railway Industry Association. For gas pipeline this was the Institution of Gas Engineers and Managers (IGEM). An email seeking interest in participation, was sent to the membership of the organisations via their leadership with request to access the link to the questionnaire or contact the researcher if they were interested

in interview. For example, the following is an extract sent to the IGEM membership from their then Head of Technical and Policy.

"From: [redacted]

Sent: 18 September 2020 16:17

To: REDACTED

Subject: Managing Legal Risks of Digital Twin Applications in Regulated Industries

Dear Committee member,

IGEM are looking to support research being undertaken by Derby University relating to Asset Management and Digital Twin. The link below gives access to the form. I'm told it takes around 15minutes to complete.

Ideally the researcher is looking for multiple respondents to the questionnaire to get a balanced view across organisations and roles so if there are others you feel could also provide a response I'd be grateful if you could forward this on to them.

Additionally there is an opportunity to take part in an interview and I would be grateful if you could advise if you wouldn't mind being interviewed.

Here's the link to the form "Managing Legal Risks of Digital Twin Applications in Regulated Industries":

https://forms.office.com/Pages/ResponsePage.[redacted]

Kind regards

[redacted]

Head of Technical and Policy

Institution of Gas Engineers & Managers (IGEM)"

This targeted the following companies: ALH-Systems, DNV GL, National Grid, Tata Steel Europe, Northern Gas, AVKUK, Cadent Gas, AFAA Ltd, BPA Ltd, Wales & West Utilities, Rosen-group, SGN, British Steel, Radius Systems, Calor, HSE, Pipeline Integrity Engineers UK, OAE Ltd, GTC-UK Ltd, Premtech Ltd, Lloyds Register, Greenflame, Global Energy, SGN.

The Rail Forum targeted all the OEMs on their membership, ROSCOs, Operators (train and infrastructure) and some supply chain. The list included Porterbrook, Eversholt, Angel Trains; East Midlands Railway, Nottingham Trans, Rail Operations Group, DB; Network Rail; Alstom, Bombardier, Knorr-Bremse, Atkins, Unipart Rail, Pandrol, Alonyx, Amey, Elastacloud, DB ESG, Wabtec, Balfour Beatty, Amco Griffen, Story Contracting.

In order to secure a balance of Physical Entity management representation across the lifecycle, follow-up emails were sent to targeted individuals within companies and where an individual within the company identified a colleague with a related Physical Entity management role an invite was forwarded to them. More direct email contact was made to recruit participants for the expert review in Stage 3. The wording of this email was as follows:

"Dear

As part of my PhD research a conceptual framework for understanding how Intellectual Property risks potentially impact achievement of multi-stakeholder collaboration using Digital Twins for operational decision support has been developed and there is a need to review this with stakeholders for completeness and clarity and capture views on whether application of the framework could be used to mitigate such risks.

I'm seeking a mix of legal experts and IP owners and users, including those using and developing Digital Twin services for Decision Support and who may have contributed to earlier questionnaires and interviews.

The review will involve an online interview (using MS Teams) where the researcher will run through the framework and ask questions, recording responses as they go. The process is expected to take around 1 hour. Depending on the collated responses across all participating

stakeholders the framework may be updated and the researcher may then seek to run the updated framework by participants again focussing on the changes.

I'd be very grateful if you would consent to take part by return email and if so to let me know suitable dates and times that we could set up the interview. If you have any further questions please do not hesitate to ask.

I look forward to hearing from you.

Best regards

Jenny

Version: 01 28/07/2023"

A3.5 Consent

Consent was sought from participants to collect and analyse their responses in accordance with the declared purpose. For the questionnaires the briefing is stated immediately before the first question (Appendix 4). Question 2 sought consent for the participant to be contacted to enable the PhD student to clarify any responses and this was confirmed through the participant's provision of an email address in Question 3.

For the semi-structured interviews consent was sought prior to scheduling the interviews, to include consent for follow-up clarifications. A sample consent form is provided as Figure A3.2.

UNIVERSITY OF DERBY

Lonsdale House
Quaker Way
Derby
DE1 3HD

21/09/2020

Dear [redacted]

Request for Interview Participation in Support of PhD Level Research

I'm carrying out PhD level research that aims to develop a Framework for the effective management of legal risks associated with Digital Twin adoption in regulated industries. As part of this there is a need to elicit the Digital Twin Use Cases of importance to each sector and the context of Risk and Legislative Frameworks already in use within the sector and how they are applied to Digital Twin implementations and use. I'm also trying to elicit viewpoints about the perceptions of risk associated with Digital Twin adoption in these industries and whether there have been any legal challenges associated with the implementation and use of digital technologies.

As such I'm conducting a number of interviews to elicit this information across companies operating within regulated sectors and I would be grateful if you would consent to be interviewed.

The following questions will guide the interviews and will be supplemented with clarification questions during the interview:

Question 1	How is the sector structured and where does your organisation fit within this?
Question 2	What are the key Digital Twin Use Cases of importance to your organisation? (step through how a particular one works or would be intended to work if not yet implemented)
Question 3	What frameworks/methodologies do you use to manage risks and legal compliance associated with the implementation and operation of Digital Twin and Asset Management systems that you use?
Question 4	How well do you feel these frameworks manage these risks and support the implementation and management of these systems?
Question 5	Where do you feel there could be improvements in the control of risks?
Question 6	What are the main challenges to the implementation and operation of Digital Twin?
Question 7	Do you have any concerns about legal risks such as IP/security/contractual issues or data sharing and protection and has your sector or organisation been exposed to such risks?

I will write up the notes from the interview and pass back to you for your record. If you feel the notes accurately reflect the interview there is no need to confirm this and after 10days it will be presumed that they are accurate. However I'd be grateful of positive confirmation of accuracy and timely notification of any clarifications to ensure accuracy. It is possible that there may be a need for me to contact you again following the interview to clarify parts of the notes. As such, I would be very grateful if you felt able to support any follow-up.

The notes from the interview and any supplementary notes will be used by me, the PhD student, to identify patterns across the data as a whole and to compare and contrast subsets of responses in order to draw observations and conclusions. Any follow-up clarifications, will be sought by me directly as the PhD student and will not be passed on to anyone else or for any other purpose.

The overall aggregated results and observations will be presented in a PhD thesis and may be included in academic publications. Use Cases attributed to an industry sector may be included in such publications. If it seems relevant to include quotations from individuals in potential publications explicit consent will be sought from that individual in advance.
The notes from the interview and any supplementary notes will be held in a restricted area of the University network for the period necessary to support PhD thesis submission and award, which is estimated to be six to seven years (to 31st December 2027). After such time they will be securely destroyed. The lawful basis for processing this data is consent. This means that should you wish, you can withdraw your participation in this process. Owing to thesis submission deadlines you would need to notify me of your withdrawal before 1st January 2025.

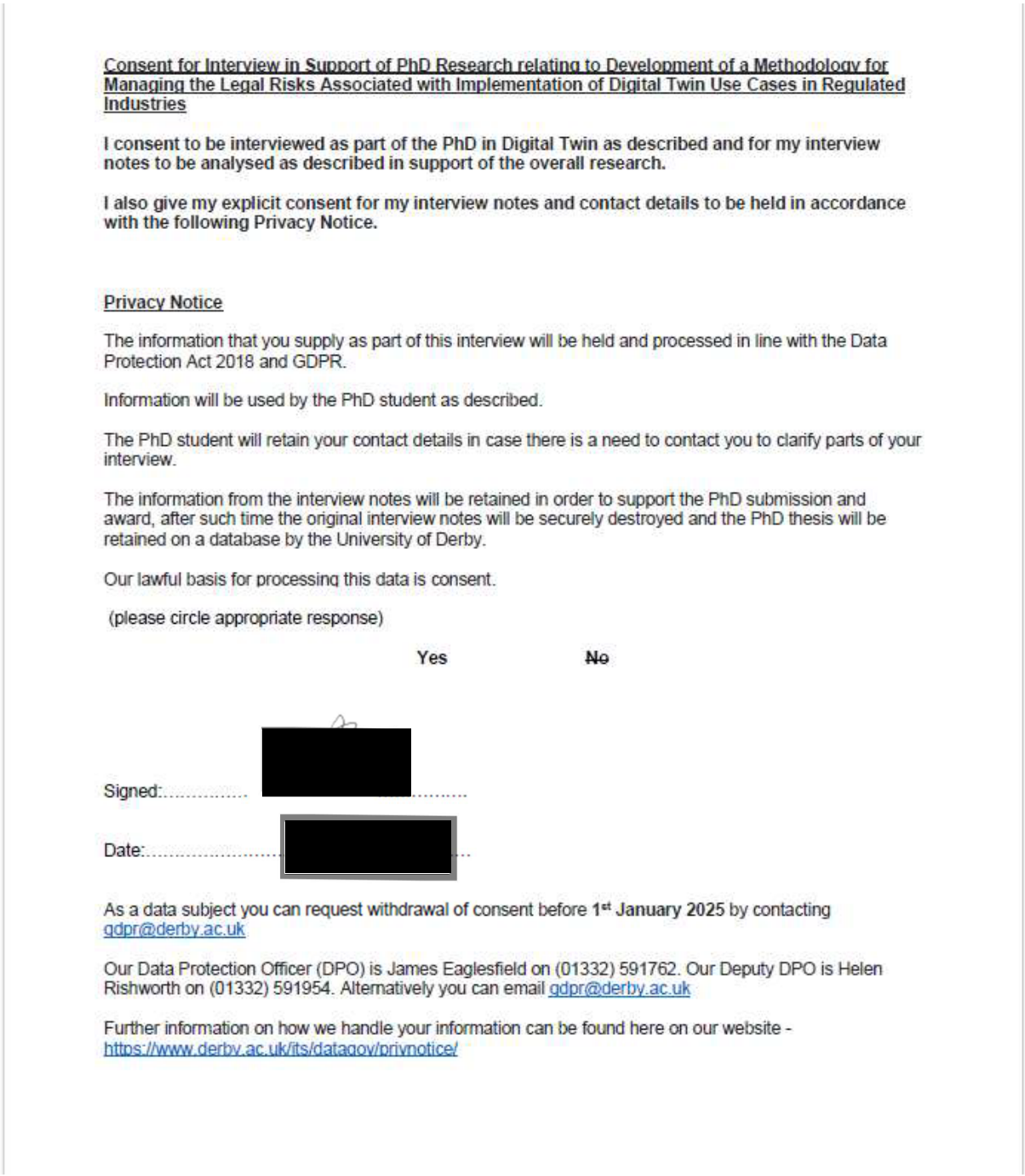
Your participation in these interviews is of great value to me. If possible, please could you provide your explicit consent to be interviewed and the notes to be held and processed as discussed above, by returning the consent form below.

If you have any questions, please do not hesitate to contact me at: j.clementson@derby.ac.uk

Many thanks for your time and I look forward to hearing from you. Once I have your consent I will be in touch to arrange a convenient interview time for you.

Yours Sincerely,

Jenny Clementson
PhD Student and IISE Senior Project Manager
IISE, The University of Derby



Consent for Interview in Support of PhD Research relating to Development of a Methodology for Managing the Legal Risks Associated with Implementation of Digital Twin Use Cases in Regulated Industries

I consent to be interviewed as part of the PhD in Digital Twin as described and for my interview notes to be analysed as described in support of the overall research.

I also give my explicit consent for my interview notes and contact details to be held in accordance with the following Privacy Notice.

Privacy Notice

The information that you supply as part of this interview will be held and processed in line with the Data Protection Act 2018 and GDPR.

Information will be used by the PhD student as described.

The PhD student will retain your contact details in case there is a need to contact you to clarify parts of your interview.

The information from the interview notes will be retained in order to support the PhD submission and award, after such time the original interview notes will be securely destroyed and the PhD thesis will be retained on a database by the University of Derby.

Our lawful basis for processing this data is consent.

(please circle appropriate response)

Yes No

Signed:.....

Date:.....

As a data subject you can request withdrawal of consent before 1st January 2025 by contacting gdpr@derby.ac.uk

Our Data Protection Officer (DPO) is James Eaglesfield on (01332) 591762. Our Deputy DPO is Helen Rishworth on (01332) 591954. Alternatively you can email gdpr@derby.ac.uk

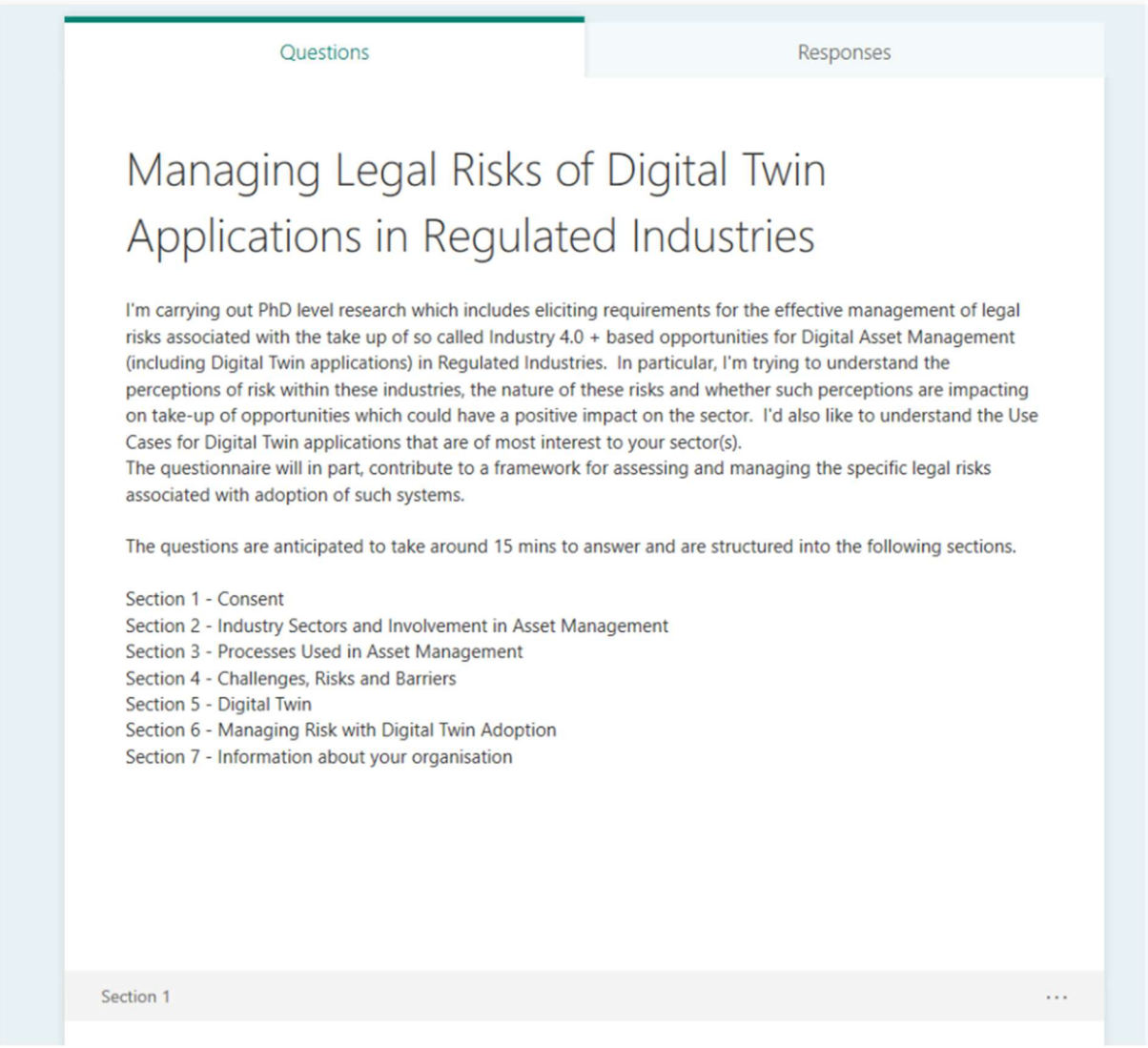
Further information on how we handle your information can be found here on our website - https://www.derby.ac.uk/its/dataqov/privnotice/

Figure A3.2 - Invite and consent for semi-structured interviews

Appendix 4: Data Collection Forms

Screenshots of the Microsoft Forms questionnaire are identified in section A4.1 and the form for guiding and capturing semi-structured interview notes is identified in section A4.2.

A4.1 Questionnaire template



Section 1 ...

Consent

This section records your consent to take part in the questionnaire and optionally to be contacted post-questionnaire for follow-up.

Privacy Statement
The information that you supply in this questionnaire will be held and processed in line with the Data Protection Act 1988, GDPR and subsequent legislation.
Information will be used by the PhD student to identify patterns across the data as a whole and to compare and contrast subsets of questionnaire responses in order to draw observations and conclusions.
Where personal information is supplied and consent given to be approached about follow-up questions this will be carried out by the PhD student directly and will not be passed on to anyone else or for any other purpose.
The overall aggregated results and observations will be presented in a PhD thesis and may be included in academic publications. In publications, there will be no reference to individual contributors to the questionnaire and conclusions will be made in relation to aggregated groups of responses with a list identified of the companies and industries that supported the research. If it seems relevant to include quotations from individuals in potential publications explicit consent will be sought from that individual.
The data will be held for six years to inform the PhD thesis, after such time it will be securely destroyed. Our lawful basis for processing this data is consent.

1. I give my explicit consent for my responses to the questionnaire to be used as described. *

- ○ Yes
- ○ No

2. I am happy to be contacted directly by the PhD student for clarification on any responses given ? *

- ○ Yes
- ○ No

3. If answered "Yes" to Q2 please provide contact details (name, email and phone below - thanks !) *

Enter your answer

Section 2 ...

Industry Sectors and Involvement in Asset Management

Categorises the industry sector and asset activity to enable responses from a specific sector to be related and compared with other sectors.

4. Which industry sector(s) do you operate in ? Please tick all that apply. *

- [ ] Rail, airline and pipeline transportation
- [ ] Oil and Gas
- [ ] Electric power and transmission
- [ ] Water
- [ ] Other

5. Does your organisation have responsibility for the performance (including reliability, availability, maintainability, safety) for a significant asset(s) for a part or all of their lifetime ? (including via any contractual relationships.) *

- ( ) Yes
- ( ) No - As we are a supplier of Asset Management Tools and Solutions
- ( ) No - As we are a consultancy without direct responsibility for assets
- ( ) Other

6. What type of assets do you have responsibility for ? (tick all that apply)

- [ ] Vehicles and their subsystems
- [ ] Infrastructure: Buildings, stations, control and maintenance depots
- [ ] Linear Infrastructure (Civils): Roads, Paths, Rail Tracks
- [ ] Linear Infrastructure (Amenities): Electricity, Gas, Water, Communications
- [ ] Other

7. What aspect of the asset lifecycle does you business focus on in its day to day operations? (Tick all that apply.)

- [ ] Design (includes commissioning design and tenders)
- [ ] Build/ Manufacture/ Systems Integration/ Assembly
- [ ] Use and Operation
- [ ] Maintenance, Repair and Overhaul
- [ ] De-Commissioning
- [ ] Training
- [ ] Other

8. Typically how long is the asset in the care/responsibility of your company (either through ownership or contract)

- ○ 0 - 5 years
- ○ 5 - 10 years
- ○ 10 - 20 years
- ○ 20 - 30 years
- ○ over 30 years

Section 3 ...

Processes used in Asset Management

Identifies the types of asset activities carried out and perceptions of the degree to which digital tools are used to assist manage these assets.

9. To what extent does your organisation utilise digital processes and techniques in asset management activities.
Consider the degree to which the processes and records are digital and integrated as opposed to paper based and manual or a mix eg technical drawings (paper) versus CAD and 3D scanned assets (digital), manual measurements recorded on paper versus in-line scanning and automatic checking.
'Partial' may be where there is a mix of traditional and digital within an organisation process.
'Widespread' may be where there is extensive use of digital records, digital process integration and with stakeholders interacting with relevant information via tablets/phones etc in the field.

	Manual and Paper Processes only	Partial Digital and Paper Based Processes	Pilots and Trials of Integrated Digital Solutions	Widespread Digital Processes with Some Gaps	Widespread Integrated Digital Processes (Effective)	Not Applicable
Lifecycle Management (evidence of digital could be PLM,PDM/ERP)	○	○	○	○	○	○
Design and Simulation - Physical, Interfaces (including human), Functional, Data and Performance	○	○	○	○	○	○
Design Compliance/ Assurance	○	○	○	○	○	○
Manufacture and Assurance	○	○	○	○	○	○
Systems Integration and Assurance	○	○	○	○	○	○

System Operations - Normal, abnormal and emergency (integrating assets and human roles)	○	○	○	○	○	○
Maintenance (Time/condition/ predictive)	○	○	○	○	○	○
Training	○	○	○	○	○	○

10. Add any comments to explain your choices.

Enter your answer

11. Is your organisation utilising the technologies of Industry 4.0 to support effective asset management solutions? If so, how well in your opinion.

	Not Adopting and No Clear Need (OK)	Not Adopting and Missing Opportunities (Not OK)	Adopting but not effectively (Could Improve)	Adopting and very effective (OK)	Adopting and Industry Leader
Cloud Computing	○	○	○	○	○
Internet of Things	○	○	○	○	○
Artificial Intelligence	○	○	○	○	○

3D Printing	○	○	○	○	○
3D Scanning	○	○	○	○	○
Data Analytics	○	○	○	○	○
Robotics	○	○	○	○	○
Cyber-Physical Systems	○	○	○	○	○
Digital Twin - Physical and virtual asset models linked by data	○	○	○	○	○
Virtual/ Augmented / Immersive Reality	○	○	○	○	○

12. Please describe the digital asset management Use Cases that could benefit the Sector and what the potential benefits could be. *

Enter your answer

Section 4 ...

Challenges, Risks and Barriers

The next set of questions explore the challenges, risks and barriers to digital asset management solutions.

13. What do you feel are the main challenges to effective digital asset management solutions in your business sector? *

Enter your answer

14. What do you perceive are the most significant challenges or barriers to effective adoption of digital asset management solutions? *

	Don't know	Most Important Challenge (Pick 1)	Significant Challenge	Moderate Challenge	Not a Concern at Present
Industrial Sector Structure	○	○	○	○	○
Organisation Structure eg Silos, Isolatory Thinking	○	○	○	○	○
Out of Step Regulation and Standards	○	○	○	○	○
Limited Resources	○	○	○	○	○

Lack of Digital Skills					
Lack of Understanding of Exposure to Legal Risks and Consequences (Cloud/IoT, Security, Data Protection, Data Access, Intellectual Property, Contracts with multiple stakeholders, AI decision responsibility, criminal activity)					
Uncertainty in implementation of legal protections from careless or malicious activity					
Demonstrating compliance with relevant legislation and regulations					
Ethics eg Extent of data gathering, monitoring and control					
Culture eg Risk Averse or not digitally aware					
Size of required organisational change required for implementation					

Inadequate knowledge management as a starting point					
Lack of current technical solutions for key considerations such as: decision assurance, data traceability, handovers from AI to human, interoperability, cyber-security, digital rights management obsolescence, data storage, data gaps/quality/ontology					

15. Please describe any other risks, barriers and challenges of concern to you. *

Enter your answer

Section 5 ...

Digital Twin

The term "Digital Twin" is increasingly being used across sectors in relation to Use Cases which closely relate virtual/digital and physical assets with data. The definition varies to some extent depending on the sector and application, and there are increasing levels of sophistication in the relationship between the digital and physical asset from exchange of sensor data, to applying data analytics to predict physical asset behaviour to real time control interactions.
This section explores your view on Digital Twin adoption in your sector.

16. To what extent are you currently seeing the adoption of Digital Twin terminology solutions in your sector at present ? *

- [ ] Basic Adoption - Physical and Digital Asset connected through real-time data eg from sensors
- [ ] With added control interation between the physical and digital asset
- [ ] Using predictive analytics to anticipate the behaviour of the physical asset
- [ ] Using predictive analytics to influence the behaviour of the physical asset
- [ ] Other

17. Please provide comments on the Digital Twin solutions that influenced your answer. *

Enter your answer

18. Please outline the Digital Twin Use Cases that you believe could benefit the sector and what the potential benefits could be. *

Enter your answer

19. What are the most significant risks that concern you with the adoption of Digital Twin ? *

Enter your answer

20. To what extent are these managed through existing sector risk management frameworks ? *

Enter your answer

Section 6 ...

Managing Risks with Digital Twin Adoption

This section seeks views on the risk management frameworks used to manage risks and the extent to which they support the adoption of Digital Twin solutions.

21. What methodologies do you currently adopt to manage risks associated with the implementation of Digital Twin applications ? *

	Yes	No	N/A
Standards compliance	○	○	○
Risk management tools	○	○	○
Project and systems lifecycle methods	○	○	○
Compliance matrices	○	○	○
Checklists	○	○	○
Safety Cases	○	○	○
Contracts with Stakeholders for Data Access/Use/Sharing and IP	○	○	○
Other	○	○	○

22. Comment on whether you perceive there to be gaps in available methodologies or guidance to mitigate particular risks that the sector needs to address.

Enter your answer

23. Has your sector had any issues with illegal activity such as IP Infringement or Data Security breaches? *

- Yes
- No

24. If you answered 'yes' to the previous question please provide a summary of the issues experienced.

Enter your answer

Section 7 ...

Information About Your Organisation

Information about the organisation will further enable analysis of common themes and the range of responses for sectors and companies of similar type.

25. What is the name of the company that you work for ?

Enter your answer

26. Is the company that you work for an SME (less than 250 employees, not more than 25% owned by an enterprise that is not an SME and annual turnover less than 50million Euros with annual balance sheet not exceeding 43 million Euros) or a larger company ? *

- SME
- Non-SME

27. Please either identify your company registration number or provide a link to the company website. *

Enter your answer

28. Please identify the type of role you hold within the company ? (Select the closest where possible) *

- ○ Director
- ○ Senior Manager
- ○ Manager
- ○ Engineer
- ○ Technician
- ○ Other

29. Thank you for your patience in completing this survey. If you have any additional comments you would like to add please do so below.

Many thanks ! *

Enter your answer

A4.2 Semi-Structured interview notes template

PhD Titled A Methodology for Managing Legal Risks Associated with Implementation of Digital Twin Use Cases in Regulated Industries

Interview Notes

Interviewee	
Role	
Company	
Date of Interview	
Reference	

Question 1	How has the sector structured and where does your organisation fit within this?

Question 2	What are the key Digital Twin Use Cases of importance to your organisation? (step through how a particular one works or would be intended to work if not yet implemented)

Question 3	What frameworks/methodologies do you use to manage risks and legal compliance associated with the implementation and operation of Digital Twin and Asset Management systems that you use?

Question 4	How well do you feel these frameworks manage these risks and support the implementation and management of these systems?

Question 5	Where do you feel there could be improvements in the control of risks?

Question 6	What are the main challenges to the implementation and operation of Digital Twin?

Question 7	Do you have any concerns about legal risks such as IP/security/contractual issues or data sharing and protection and has your sector or organisation been exposed to such risks?

Appendix 5: Coding Factors from Literature

A5.1 Characteristics of Use Cases

The table below summarises the important characteristics of Digital Twin Use Cases identified from the literature which are considered important for legal risk management:

Characteristic	**Description and Importance for Legal Risk Management**	**Example Reference Papers**
C1: Purpose	Clearly defined purpose which tends to have associated productivity and quality requirements. For example, reducing verification and test duration, predicting when maintenance is due and scheduling before in-service failures occur. Ability to achieve the purpose will have direct legal risk implications, for example where the purpose contributes to regulatory or contractual duties. There are then legal risk implications from implementation of the solution to achieve the purpose, such as contracted performance obligations. Kritzinger *et al* (2018) states that a common Digital Twin target is to increase competitiveness, productivity and efficiency. Purpose in Manufacture included: • Defect free production • Shortening time between design and production • Lifecycle part traceability Purpose in rail included:	Kritzinger *et al.* (2018) Madni *et al.* (2019) Aniruddha *et al.* (2019) Mukherjee *et al.* (2019) Kaldaldrin *et al.* (2019) Pombo *et al.* (2020) Kremers (2018), Digital Manufacturing Rasheed *et al.* (2020) Redlinghuys *et al* (2020) Kaewunruen *et al.* (2019) Knapp *et al.* (2017) Millwater *et al.* (2019)

Characteristic	Description and Importance for Legal Risk Management	Example Reference Papers
	• Optimised time schedule, cost and sustainability for a railway turnout • Achieving desired outcomes for congestion, economic growth, mobility, air quality, reduced incidents and financial risk exposure Purpose in pharmaceutical included: • Patient-centric performance and industry reduction.	
C2: Value Case (Cost-Benefit Evaluation)	The benefits of achieving the purpose are balanced against the lifecycle costs and this informs the implementation choices. Grieves & Vickers (2017) state that the cost of information resources will be less than the cost of wasted resources with value identified at each physical entity lifecycle stage. Considerations include implementation cost as a function of the number of system components and interfaces, the complexity of algorithms and knowledge and know-how required and dependencies between components. (Madni *et al* 2019) Legal considerations relating to Intellectual Property management, including the cost-benefit from protection of designs and data and access and related contractual obligations, will need to be part of this value case. Moyne	Grieves & Vickers (2017) Madni *et al*. (2019) Moyne *et al.* (2020)

Characteristic	Description and Importance for Legal Risk Management	Example Reference Papers
	et al, 2020 stresses that the financial benefit of correct operation of the Digital Twin in its environment also needs to be balanced against the costs of incorrect operation in the environment and that this needs to be ascertainable and quantifiable.	
C3: Models and Frameworks	Requirements based Frameworks such as that of Moyne *et al,* 2020 include: • Digital Twin Definition as a Purpose Driven dynamic driven replica of the Physical Entity • Digital Twin Structure that includes one or more modelling resources • Digital Twin Output that includes metrics that quantify the Digital Twin output as it relates to the Digital Twin Purpose. • Digital Twin Object Oriented Structure that supports both generalisation and aggregation. Feature Based Frameworks such as that of Autiosalo, J *et al* (2019) include elements such as: Data Link, Coupling, Identifier, Security, Data Storage, User Interface, Simulation, Analysis, Artificial Intelligence and Computation These frameworks may allow a systematic evaluation of legal risks, for example identifying the Intellectual Property and	Autiosalo, J *et al*. (2019) Moyne *et al.* (2020) Qi *et al* (2021)

Characteristic	Description and Importance for Legal Risk Management	Example Reference Papers
	licencing issues associated with the framework elements with traceability to Value Case and Purpose.	

C4: Architecture	Features included:
	• Modularity and Re-Use
	• Integration
	• Data
	  ○ Reference Data Library
	  ○ Foundation Data Model
	  ○ Information Template for data which considers ownership and sharing for Intellectual Property Management as well as data quality attributes.
	  ○ Shared repository of model based systems engineering information which supports systems engineering and data collection tools.
	• Data Connections and Information
	  ○ Connection Architecture in layers for example Redelinghuys *et al* (2019) 6 layer architecture:
	  ▪ Layer 1 & 2 – Physical Twin
	  ▪ Layer 3 – Local Data Repositories
	  ▪ Layer 4 – IoT Gateway
		Madni *et al.* (2019)
		Moyne *et al.* (2020)
		Qi *et al.* (2021) (Available in 2019)
		Rasheed *et al.* (2020)
		Redelinghuys *et al.* (2019)
		Wang *et al.* (2015)

Characteristic	Description and Importance for Legal Risk Management	Example Reference Papers
	▪ Layer 5 – Cloud Based Information Repositories ▪ Layer 6 – Emulation and Simulation • Services o Data access controlled by an authorisation layer (Lamb, 2018, cdbb) o Everything- as-a-service (Wang *et al,* 2015). Specific service platform examples include Konsberg Digital PaaS and SaaS for services to energy, oil and gas and maritime industries in partnership with cloud vendors such as Microsoft Azure and Cognite open source and customised permissions for clients (Rasheed *et al,* 2020) These architectures are linked to IP, contracts, liabilities and regulation.	
C5: Enabling Technology & Tools	Digital Twin Technologies require integration and many individual components have Intellectual Property protection such as patents covering areas such as:	Kritzinger *et al.* (2018) Lamb (2018) Qi *et al.* (2021) (available in 2019) Rasheed *et al.* (2020)

Characteristic	Description and Importance for Legal Risk Management	Example Reference Papers
	Data: Collection Technology, Storage Technology (e.g. Public Cloud, Hybrid Cloud, Private Cloud etc), Processing Technology etc **Services:** Architecture Technology, Algorithm Technology, Software and Platform Technology e.g. (XaaS, Pay as you go service model) **Connections:** Communication Technologies, Interfaces Technology, Interaction Technology, Collaboration Technology, Security Technology etc **Model**: Simulation Technology, Visualisation Technology, Model Evolution etc **Physical**: Sensing Technology, Material Technology, Process Technology etc	Wang *et al.* (2015)
C6: Stakeholder Collaboration	Shared Long Term Vision Joint Short Term Priorities Challenges of Different Values National Digital Twin Gemini Principles Failure to collaborate can have legal implications through contract in relation to Quality of Service or directly depending on the use case and impact on safety and security.	Enzer *et al*. (2018) The Centre for Digital Built Britain, 2018

Table A51.1: Coding of Digital Twin Characteristics

A5.2 Coding Legal Issues with Digital Twins

Coding of legal issues from the literature has identified the following of relevance to Digital Twin:

Category	Sub Issue	References
L1: Intellectual Property Digital Twin Parts (Data, Services, Models, Connections, Digital Twin and Physical Twin)	**Data**: Data Ownership and Sharing, Data Use Agreements Legal Protection of Data: Applicability of trade secrets, contracts and database rights for protecting data and data sets Regulating web of APIs including governing ownership of the generated data and transparency in support. Link to governance stakeholders: Data Subjects, Data Controllers and New Service Providers (Nati *et al*, 2019)	The Gemini Principles (The Centre for Digital Built Britain, 2018) Conrado *et al.* (2017) Grieves & Vickers (2017) Madni *et al.* (2019) Moyne *et al*. (2020) Nati *et al.* (2019)
	Virtual Models Representing Protected Physical Assets and Processes Patents, Design Rights, Trade Secrets	Bird & Bird LLP (2020) Daly (2016) Mendis *et al.* (2020) Murray (2016)
	Digital Twin Infrastructure Ownership Digital Twin Infrastructure	Anwer (2017) Son (2018) Wang *et al* (2020)

Category	Sub Issue	References
	Patents, Design Rights	
	Licence Management	Bechtold (2015)
L2: Legal Compliance: Data Protection, Security and Information Governance	Usage Restrictions Privacy, Trust and Security Authenticity/ Traceability Information Governance	 Anwer (2017) Cohen *et al.* (2019) Daly (2016) Huang *et al.* (2020) Kerber (2016) Mandolla *et a*l. (2019) Redelinghuys *et al.* (2019) Enzer *et al.* (2019) Cdbb The Pathway Towards Information Management Framework Raptis *et al.* (2019) Sinclair *et al.* (2019)
L3: Liabilities and Risks	Guaranteed capability over defined period in a defined environment. E.g. Data Quality such as completeness, consistency and precision. 5Vs of Data(Volume, velocity, Veracity, Variety, Volume), access to computing	Cui *et al.* (2020) Kritzinger *et al*. (2018) Moyne *et al.* 2020 Rasheed *et al.* (2020)

Category	Sub Issue	References
	infrastructure (edge, fog and cloud computing)	
	Decision Making (Physical Realism/Accuracy and Reliable Future Projections) Risk of in-service product failure and liability. Decision making by automation and Artificial Intelligence – levels of autonomy should not undermine the ability to monitor, supervise and intervene. (RSSB 2017)	Bird & Bird LLP (2020) Mohr and Khan (2015) Moyne *et al.* (2020) RSSB (2017) WIPO Conversation (2019)
L4: International Dimension	Regulatory Interoperability Demonstrating safety, reliability of machine learning models Sharing and segregation of liabilities between stakeholders Internet Governance Who liable if a product or system fails or is unavailable?	Murray (2016)

Table A52.1: Coding of Legal Issues Related to Digital Twin from Literature

A5.3 Coding of Mitigations

The table identifies an early stage analysis of mitigations.

Mitigation Category	Reason	References
Technology: Cyber-Security, Smart Contracts and Technology Risk Mitigations	Ensuring data is managed and Intellectual Property is protected. Managing risk of malicious or accidental tampering with models which leads to product failures and unsafe states.	Cui *et al.* (2020) Huang *et al.* (2020) Lamb (2018) Mandola *et al.* (2019) Mohr and Khan (2015) Raptis *et al.* (2019) Rasheed *et al.* (2020) Wang (2015)
Stakeholders: Defined Types, Roles and Responsibilities, Minimise Contractual Interfaces	Contractual obligations within the supply chain. Competing interests of suppliers (limiting exposure and warranties) versus customers and users of the system (all trying to avoid liability) Types of stakeholder: Funding Agencies, Owners/Operators, Supply Chain, Customers, Regulators Designer, Assembler, Maintenance, Recycle, Customer, Manufacturer, Dealer, Logistics	Bird & Bird LLP (2020) Huang *et al.* (2020) HS2, 2022

Mitigation Category	Reason	References
Policy, Legislation (sector and area specific standards and guidance)	Extent to which protects information and supports ongoing collaboration e.g. Joint Rail Data Action Plan Challenges dealing with electronic evidence. Ensuring authenticity and integrity of electronic evidence.	Bird & Bird LLP (2020) Kalogiamno *et al.* (2020) WIPO (2019) Wu and Zhang (2020)

Table A53.1: Coding of Legal Risk Mitigation Issues

Appendix 6: Coding Participant Context

Participant views of digital implementation and use cases of importance were captured and coded to clarify the context for their perceptions of risks and issues.

A6.1 Coding of Perceptions of Digital Twin and Industry 4.0 Implementation

The interviews and questionnaire questions Q9 – Q11 predominantly contributed to the view of perceptions. The perceptions are coded as follows:

Coded Perception	**Example Response in support**
Currently patchy digitisation implementation over asset lifecycles.	"Asset use and maintenance still very manual in practice." "Company has areas where their digital records are excellent but they lack the ability to change and adapt quickly." Relating to design and development "We use a combination of digital and paper based processes." Mixed responses to Q9 and Q11 of questionnaire covering manual processes and low use of Industry 4.0 technologies to "industry leader" in some areas. "Not Adopting" response was particularly noticeable against robotics and cyber-physical systems."
Not implementing digital solutions across stakeholders and functions.	"designs are transferred between parties as 2D drawings. The only parts that are manufactured without paper drawings are a few CNC and 3D printed parts; design development and simulation is entirely digital but becomes paper once the design moves to production".

Coded Perception	Example Response in support
Opportunities for condition based maintenance recognised but not implemented yet	"maintenance activities still typically interval based and move towards risk based partially implemented."
Rail Sector and Gas Pipeline are on a very early stage adoption of Digital Twin	Interviews revealed engagement with the National Digital Twin but at the very beginnings of exploring implementation of asset Digital Twins. Asset owners were engaging on feasibility and pilot studies which are just starting late 2020. Quote from Q17 and Q18 of the questionnaire: "Many projects are still at ideation and PoC phases." "Lots of starts in terms of introduction of sensors but nothing comprehensive – basic implementations – shadow and basic condition monitoring."

Table A61.1: Coded Perceptions of Digital Twin and Industry 4.0

A6.2 Coding of Digital Twin Use Cases of Relevance to Participants

Use cases revealed through the interviews and the questionnaire which covered the Rail, airline and pipeline transportation sector are coded in summary as follows.

Coded Use Case	Source and Current Activity and Challenges
Goal: Predictive and Condition Based Maintenance for Rolling stock, wagon and	Source: Interview (Leasing Companies and Train Operator) and Q12 and Q18 Early stage of considering asset management decision support solutions. One respondent had just contracted with a

Coded Use Case	Source and Current Activity and Challenges
locomotive assets. (Moving away from periodic based maintenance) Actors: • Asset Owner • Train Operator (with interest in optimising maintenance too) • Maintainer • OEM (often with contract for maintenance) • Sub-System Suppliers • Digital Twin Owner (unclear at present which stakeholder this will be) Use Case Actions: Not yet developed in detail.	supplier of services to explore the feasibility of creating a Digital Twin. Focus is on new Rolling Stock as legacy seen as challenging due to information ownership and legacy contracts. Current challenges relate to ownership of models and data (with OEM) and owner of procured asset (leasing company) and day to day needs of the train operator versus needs and value between stakeholders. OEM perceived as reluctant to share data and Intellectual Property for effective Digital Twin until the last decade of an asset's life when they are working with new product families. One respondent was involved in modelling internal combustion engines in trains to deliver predictive analytics that could be used to predict asset behaviour. This shows the complexity of the supply chains involved in a Digital Twin of a complex asset like a train. A questionnaire respondent identified their intention to: "*develop a best practice maintenance programme where we as manufacturers can assist the customer in 'decision making' comparing results across many territories and scenarios*."

Coded Use Case	Source and Current Activity and Challenges
Goal: Predictive maintenance of switches and crossings and plain track. Actors: • Asset Owner/Operator/Maintainer e.g. Network Rail • Asset manufacturer • Digital Twin Owner (unclear at present which stakeholder this will be) Use Case Actions: Not yet developed in detail	Early stage pilot through H2020/Shift 2 Rail Project. Aiming for 'Standards' for Interoperability and sharing of information. Currently finding the National Digital Twin disconnected and too 'high level' for development on the ground.
Goal: Management of infrastructure asset condition (Gas Distribution Infrastructure) Optimisation of intervention decisions and lower through life cost. Sub-Goals include: • Lower operational risks and costs • Model operational conditions and gain detailed insights on asset health and condition	Project GRAID (Gas Robotic Agile Inspection Device) for inspection of unpiggable pipelines. Effort to digitise and move to cyber-physical systems. Implementing The Security of Network & Information Systems (NIS) Directive (latest version is 'Council Directive (EU) 2022/2555' (2022))

Coded Use Case	Source and Current Activity and Challenges
• Preventative maintenance forecasting and avoid unplanned maintenance and downtime • Demonstrate regulatory compliance • Data-driven overview of options and asset investment priorities Actors: • National Grid/ Cadent • Consultant : Digital Twin Solution Use Case Actions:	Moving away from OEM controlled to Open Source Systems. Consultant supplier of Digital Twin solutions identified importance of ISO 27001 (British Standards Institution, 2023) framework for data security and ISO 44001 (British Standards Institution, 2024) for collaborative business relationship management, especially relating to sharing IT and sharing data.

Table A62.1: Coded Perceptions of Digital Twin and Industry 4.0

Appendix 7: TACT Considerations for Qualitative Research Rigour

The considerations for qualitative research rigour described by Daniel, 2018 were applied to the development and evaluation of the research project. These considerations are documented in the following table:

TACT Category	**Dimensions of ascertaining quality from TACT (in bold) and considerations in current project under each bold heading**
Trustworthiness	**Sources and quality of data** Senior managers and engineers with responsibility for Physical Entity performance management at different points in a lifecycle, from design and manufacture to operations and maintenance, were sought for semi-structured interviews and questionnaires in the initial data gathering. Academic Literature included peer reviewed journal and conference papers. The evaluation was carried out by a set of IP legal experts and senior managers with responsibility for Physical Entity performance management. **Dependable Outcomes** Findings were documented and theory developed as the research progressed. Included both interviews and questionnaires to reflect on any similarities and differences to minimise bias. Documented observations were also related to literature. The evaluation stage was carried out by two diverse types of expert and application reflected against case scenarios. **Researcher experience** Researcher selected an application context (rail sector) that they were familiar with to assist identify target organisations, participants and case studies and to use this experience to interpret findings while also ensuring neutrality in capturing observations from participants in interviews and surveys.

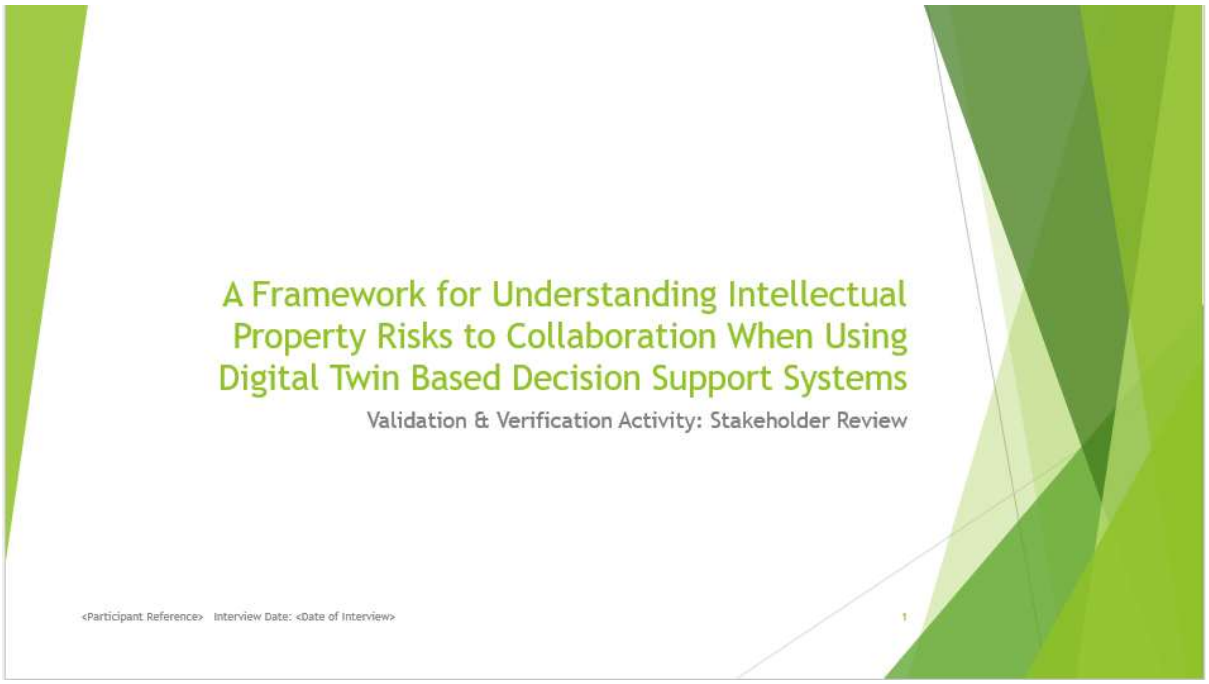
TACT Category	Dimensions of ascertaining quality from TACT (in bold) and considerations in current project under each bold heading
Auditability	**Transparent data collection** Records of interviews and questionnaires and collated responses were documented. Various memos and diagrams documenting analysis were recorded with samples in Appendices 2 and 4. **Systematic data analysis** Approach documented in Chapter 5 was followed. **Data verification** Approach as documented in Chapter 9 was followed with expert evaluation and application to case scenarios.
Credibility	**Triangulation** Questionnaires were related to interviews and to literature. Some questions were similar to relate responses. **Theory** Systematic approach followed as described and documented in Chapters 3, 5, 6 and 9. **Mixed Methods** Complex design with concurrent mixed methods in the phase that constructs the framework.
Transferability	**Acknowledging multiple realities** Expert review by 10 participants representing legal stakeholders and rail sector Physical Entity stakeholders which allowed views from their experience to be captured. Further considering the realities of three case studies. Evaluated predominantly in a rail context however the focus was on finding the common categories

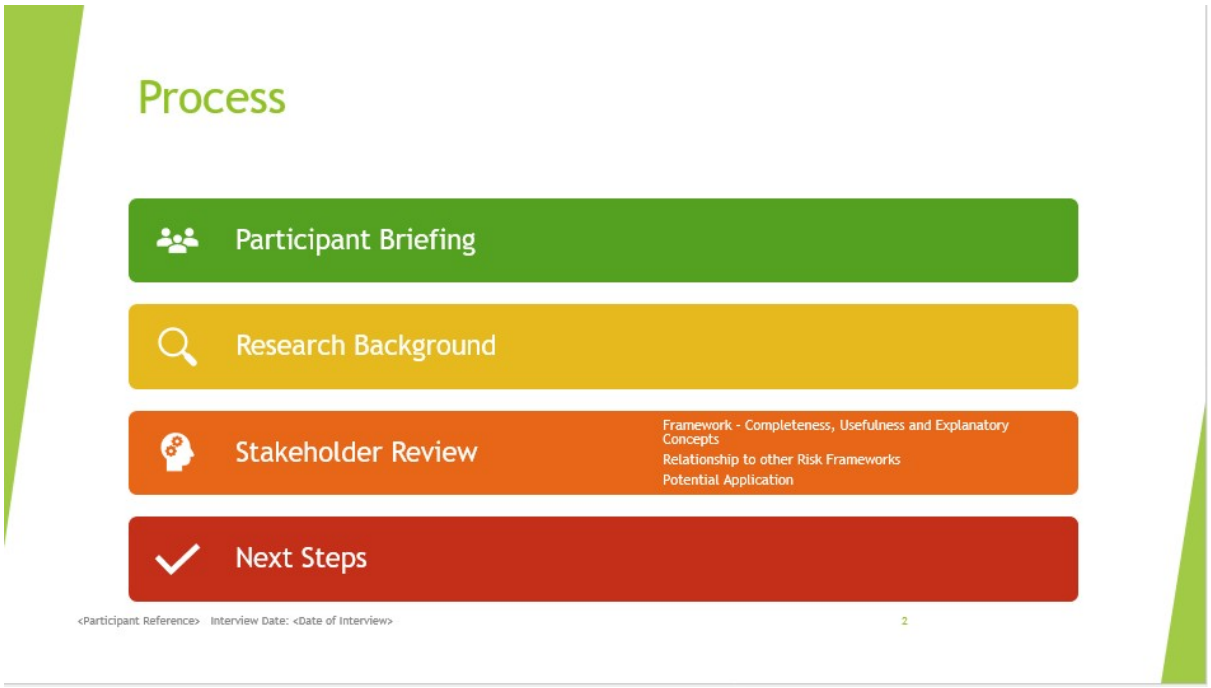
TACT Category	Dimensions of ascertaining quality from TACT (in bold) and considerations in current project under each bold heading
	and relationships for stakeholders to apply and develop in their context. **Delimitation of study** Focus on IP risk to collaboration using Digital Twins for decision support. Literature represented multiple industrial sectors, particularly the built environment and manufacture with participants predominantly from the rail sector although some had experience of other sectors such as aerospace and energy. As participants were predominantly from rail, the evaluation and case studies focussed on rail rolling stock examples. Although the legal expert review was broader and participants believed the constructed framework was generally applicable future further evaluation in non-rail contexts in future studies is recommended before confirming applicability more broadly. **Description of context** The context for the constructed risk framework is IP risk to multi-stakeholder collaboration using Digital Twins or digital systems for a decision support purpose. There was low maturity of adoption of Digital Twins during the research period. The evaluation represented the viewpoints of IP experts and the case studies applied were rolling stock maintenance decision support.

Table A7.1: TACT Considerations

Appendix 8: Expert Review Slides

Extract of the principal slides used to support the Expert Review. Some sub-title and Research Background slides removed.





Participant Briefing

- Scope: Follow-up to earlier stage interviews & questionnaires plus additional expert stakeholders
- Purpose: A V&V step in the research process
- Approach: Present findings and seek feedback
- Process & Consent

<Participant Reference> Interview Date: <Date of Interview>

UNIVERSITY OF DERBY

Consent for Participation in Review of Framework for Managing IP Risks Using Digital Twins for Decision Support

I consent to participate in this interview and any follow-up interview.

I also give my explicit consent for my interview notes and contact details to be held in accordance with the following Privacy Notice.

Privacy Notice

The information that you supply as part of an interview will be held and processed in line with the Data Protection Act 2018 and GDPR.

Information will be used by the PhD student to progress and complete their PhD thesis and supporting journal papers.

The PhD student will retain your contact details in case there is a need to contact you to clarify parts of your interview.

The information from the interview notes will be retained in a restricted area of the University network in order to support the PhD submission and award, after such time the original interview notes will be securely destroyed (Assumed to be by 31st December 2027) and the PhD thesis will be retained on a database by the University of Derby.

Our lawful basis for processing this data is consent.

No – Interview does not proceed **Yes – Interview proceeds**

As a data subject you can request withdrawal of consent before 1st January 2025 by contacting gdpr@derby.ac.uk

Our Data Protection Officer (DPO) is James Eaglesfield on (01332) 591762. Alternatively you can email gdpr@derby.ac.uk. Further information on how we handle your information can be found here on our website = https://www.derby.ac.uk/its/dataguy/privnotice/

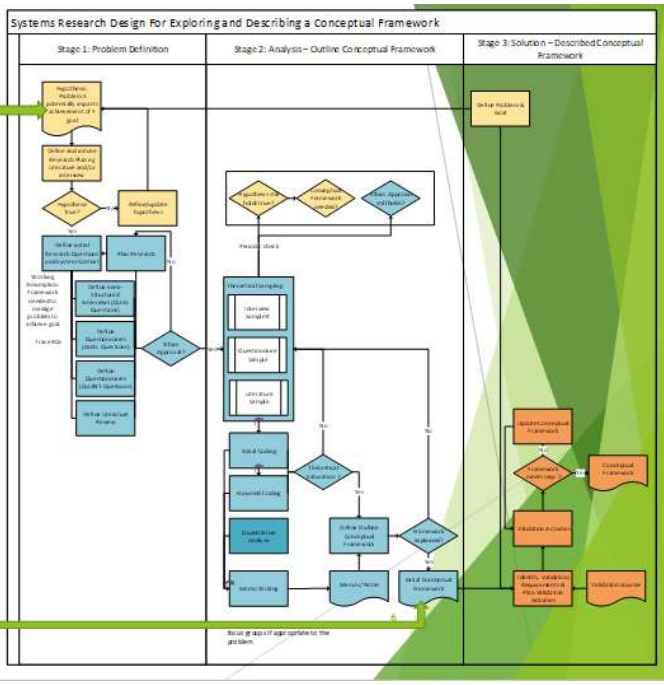
Stage 1 Hypothesis (H1):
Intellectual Property Risks potentially impact achievement of multi-stakeholder collaboration using Digital Twins for Physical Entity [lifecycle] decision support."

Research Approach

Stage 2 Hypotheses (H2, H3):
The described Framework explains how Intellectual Property Risks potentially impact multi-stakeholder collaboration using Digital Twins for life-cycle decision support.

Application of the framework could mitigate risks to achievement of multi-stakeholder collaboration using Digital Twins for life-cycle decision support.

<Participant Reference> Interview Date: <Date of Interview>



Verification & Validation

Verification - *consistency, completeness and correctness*	**Validation** - *confirmation by examination that the framework conforms to needs*
Stakeholder Review - This study	Case Studies
	National Digital Twin Legal Round Table H2020 'Leveraging Big Data to Manage Transport Operations (LeMo) Deliverable D2.2 Legal Issues, 1 November 2018

H2: "The described Framework explains how Intellectual Property Risks potentially impact achievement of multi-stakeholder collaboration using Digital Twins for life-cycle decision support."

H3: "Application of the framework could mitigate risks to achievement of multi-stakeholder collaboration using Digital Twins for life-cycle decision support."

Framework for management of Intellectual Property risks to multi-stakeholder collaboration using Digital Twins for life-cycle decision support.

<Participant Reference> Interview Date: <Date of Interview>

Verification & Validation - Stakeholder Review

- **Stage 1: The Framework Describes and Explains**
  - **How** Intellectual Property Risks potentially impact achievement of multi-stakeholder collaboration using Digital Twins for decision support (H2)
  - **Factors** for managing these risks and the relationship between them (RQ1, RQ2, RQ3, RQ4)
- **Stage 2: Application of the Framework**
  - Could potentially assure that Intellectual Property Risks are managed to support use of multi-stakeholder dependent Digital Twins for decision support through a system life-cycle. (H3)

<Participant Reference> Interview Date: <Date of Interview> 10

Stakeholder Review Process

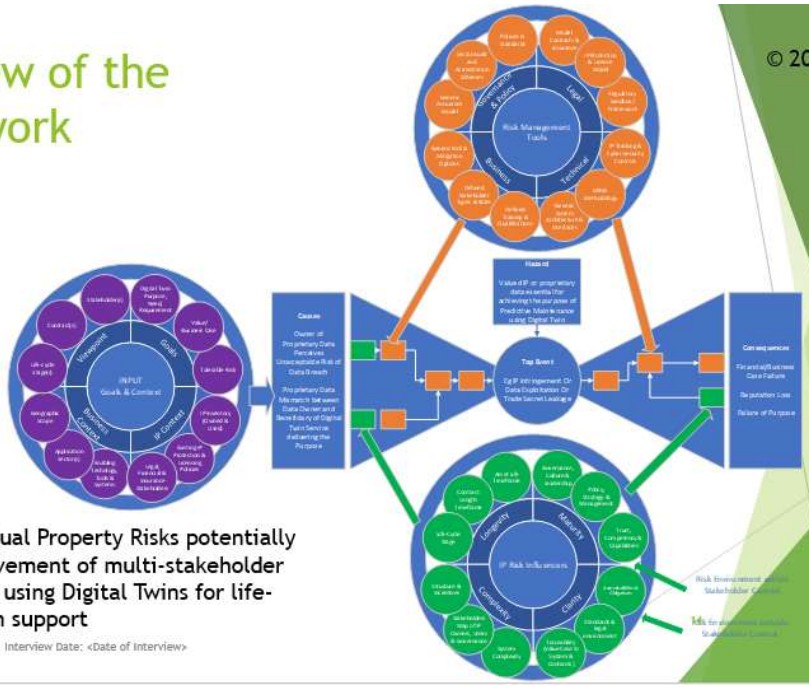
- Aspects of the framework will be shown and talked through
- I'll ask you questions to elicit your views relating to what you've seen
- I'll capture written notes of your responses
- I'll check with you that the notes are correctly captured.

- Once all stakeholders' views have been collated there will be some updates to the framework which will be presented back to the stakeholders.

<Participant Reference> Interview Date: <Date of Interview>

12

Overview of the Framework



How_Intellectual Property Risks potentially impact achievement of multi-stakeholder collaboration using Digital Twins for life-cycle decision support

<Participant Reference> Interview Date: <Date of Interview>

Overview - How IP Risks potentially impact

Q1.1: To what extent do you agree with the following statement:

"The framework forms the basis of understanding how Intellectual Property risks potentially impact achievement of a Digital Twin Purpose."

Criteria	Response
Strongly Disagree	
Disagree	
Neither Agree Nor Disagree	
Agree	
Strongly Agree	

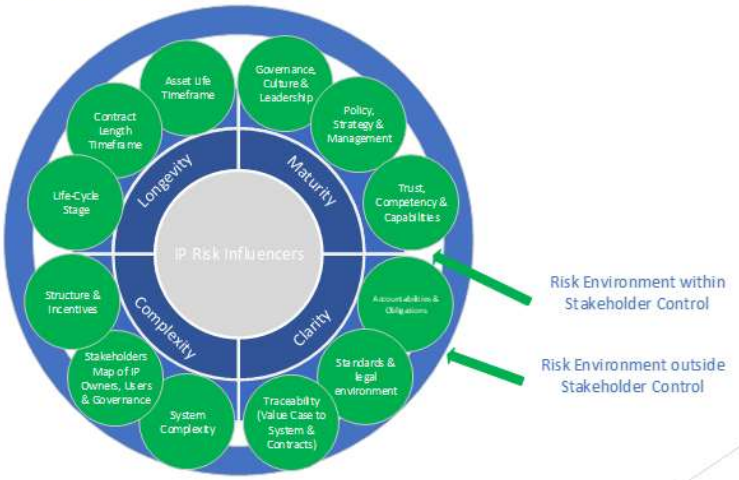
Q1.2: Please explain your answer

Comments

<Participant Reference> Interview Date: <Date of Interview>

15

Risk Influencers



<Participant Reference> Interview Date: <Date of Interview>

16

Risk Influencers - Clarity & Completeness

Q2.1 In your view are any Risk Influencer Categories missing or out of place ?

Criteria	Response
Yes	
No	

Q2.2: Please explain your answer

Comments

<Participant Reference> Interview Date: <Date of Interview>

Q2.3 In your view do the descriptions of Risk Influencers adequately convey their meaning ?

Criteria	Response
Yes	
No	

Q2.4: Please explain your answer

Comments

17

Tools - Risk Mitigation Categories

Legal Controls	Technical Controls	Business Controls	Governance & Policy Controls
IP Protections & Insurance	Standard Architecture & Interfaces	Defined & Assigned Skills & Capabilities	Reduce International / National Interpretations
License Agreements	Cyber-Security Measures	Apply Policies, Processes, Standards	Strengthen Sector Leadership, Governance and Assurance
Contracts - Data Sharing and Service	Access Controls	Roles & Responsibilities	Implement sector structures to minimise interfaces.
Regulatory Duties	Apply MBSE Methodology	Implement collaborative Practices and Constrain Opportunism	Certification
Regulatory Sandboxes		Insurance	

Risk Mitigation Categories

Q3.1 In your view are any Risk Mitigation Categories missing ?

Criteria	Response
Yes	
No	

Q3.3 In your view do the descriptions of Mitigation Categories adequately convey their meaning ?

Criteria	Response
Yes	
No	

Q3.2: Please explain your answer

Comments

<Participant Reference> Interview Date: <Date of Interview>

Q3.4: Please explain your answer

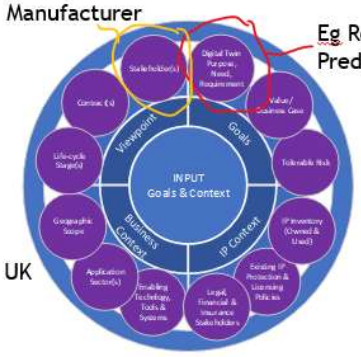
Comments

19

Relationship between: Risk Influencers, Risk Management Tools and "Goals & Context"

Manufacturer

Eg Rolling Stock System
Predictive Maintenance

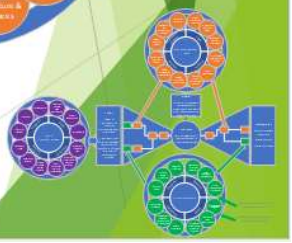


UK

Higher Risk - New design
Lower Risk - Old design

Risk Environment within Stakeholder Control

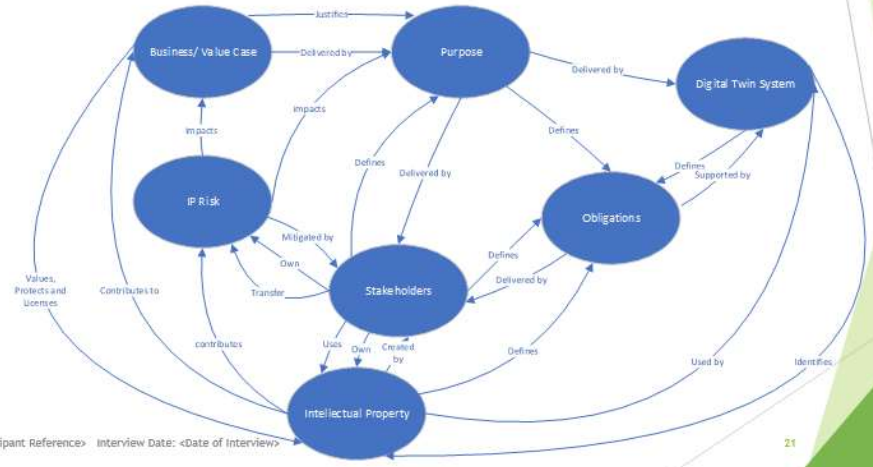
Risk Environment outside Stakeholder Control



Unclear Obligations eg for controlling use of data especially with 3rd party AI developers or system mitigated through standard contracts and reducing complexity
Low Maturity and Trust mitigated through System architecture design and sector accreditation and audit of third parties

20

<Participant Reference> Interview Date: <Date of Interview>



<Participant Reference> Interview Date: <Date of Interview>

21

Relationship between: Risk Influencers, Mitigation Tools and "Context & Purpose"

Q4.1 In your view are there any relationships between Tools, Context & Purpose and Risk Influencers that are particularly important ?

Criteria	Response
Yes	
No	

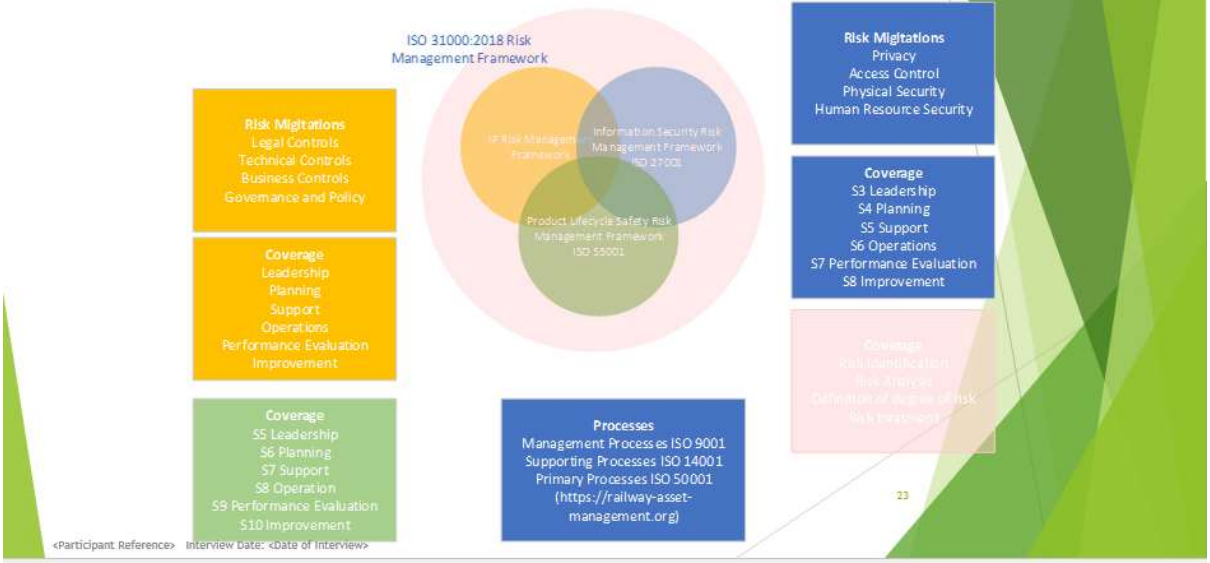
Q4.2: Please explain your answer

Comments

<Participant Reference> Interview Date: <Date of Interview>

22

Relationship between Risk Frameworks



<Participant Reference> Interview Date: <Date of Interview>

Relationship between Risk Frameworks

Q5.1: The research suggests a framework for IP risk management sits within the existing risk standards framework as shown. To what extent do you agree?

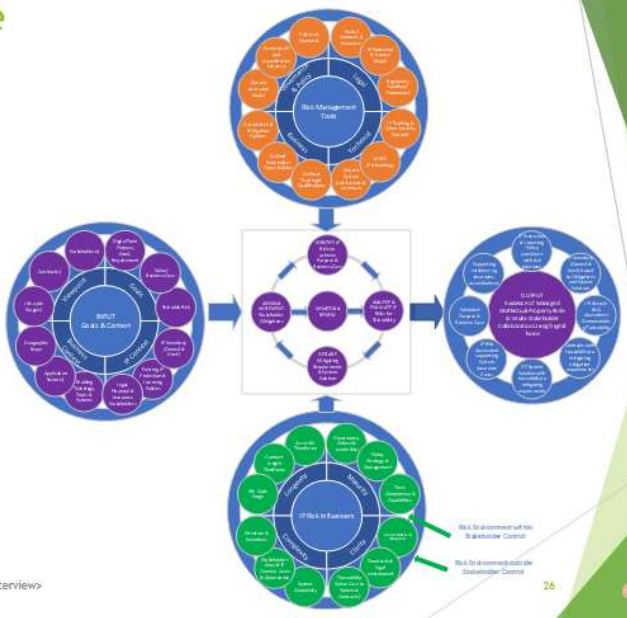
Criteria	Response
Strongly Disagree	
Disagree	
Neither Agree Nor Disagree	
Agree	
Strongly Agree	

Q5.2: Please explain your answer

Comments

<Participant Reference> Interview Date: <Date of Interview>

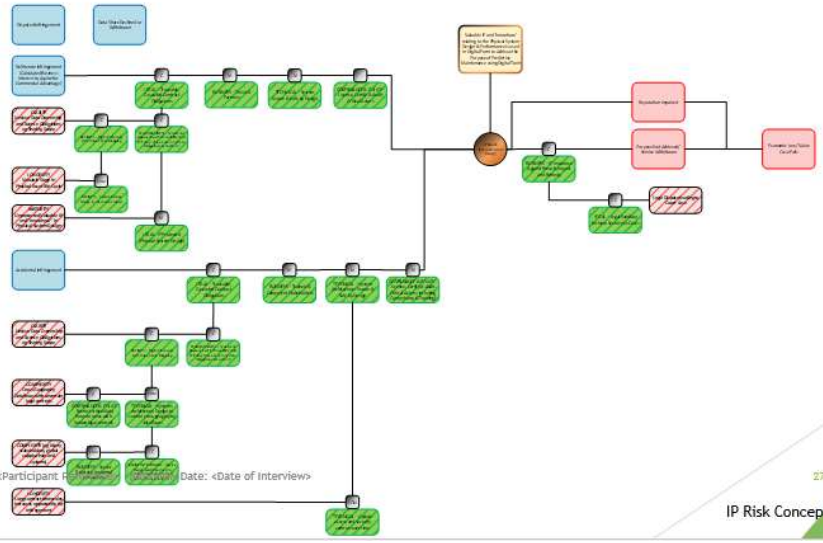
Application of the Framework - Risk Management Assurance



<Participant Reference> Interview Date: <Date of Interview>

26

Application of the Framework - Risk Management Assurance



<Participant Reference> Interview Date: <Date of Interview>

27

IP Risk Conceptual Framework.vsdx

Application of the Framework - Risk Management Assurance

Q6.1: To what extent do you agree with the following statement:

"This framework could be used as the basis, and developed, to assure that IP risks are managed to support use of Digital Twins for Life-cycle Decision Support in Regulated Industries."

Criteria	Response
Strongly Disagree	
Disagree	
Neither Agree Nor Disagree	
Agree	
Strongly Agree	

<Participant Reference> Interview Date: <Date of Interview>

Q6.2: Please explain your answer

Comments

28

Application of the Framework - Compare Options

Risk Category	Sub-Category	Criteria (Examples)	Weighting	Score
Maturity	Governance, Culture & Leadership			
	Policy, Strategy & Management	Effectiveness of risk management framework at managing IP Value and Risk throughout the process Lifecycle to achieve and maintain the Purpose and Business Case at Tolerable Risk. Standard Risk Management - degree to which Frameworks based on ISO 31000 are used. Sector mandates standards or provides guidance relating to IP risk management for defined Use Cases		
	Trust, Competency & Capabilities	Organisational competency is defined in Systems, IP, Risk and Digital Technology to ensure value flow of IP used by and generated by the system is understood to achieve and maintain the purpose. IP Risk Factors are understood by collaborating risk partners Is there sufficient Trust supporting collaboration between Stakeholders to achieve or maintain the Purpose? Is there mutual understanding of the value chain across dependent stakeholder? Is application of IP law to such systems well understood. How capable is the technical solution at protecting and managing IP while delivering the Purpose to stakeholders? How effective is stakeholder competency at mitigating Risk through system design choices?		

<Participant Reference> Interview Date: <Date of Interview>

Application of the Framework - Compare options

Q7.1: To what extent do you agree with the following statement:

"This conceptual framework could be used as the basis to compare relative risk between options."

Criteria	Response
Strongly Disagree	
Disagree	
Neither Agree Nor Disagree	
Agree	
Strongly Agree	

Q7.2: Please explain your answer

Comments

Thank you for participating in this review

We captured responses as we went through, are there any questions you'd like to revisit ?

I will send you an extracted copy of all your responses for your record. If you have any further comments or questions in the next few days please do not hesitate to get in touch.

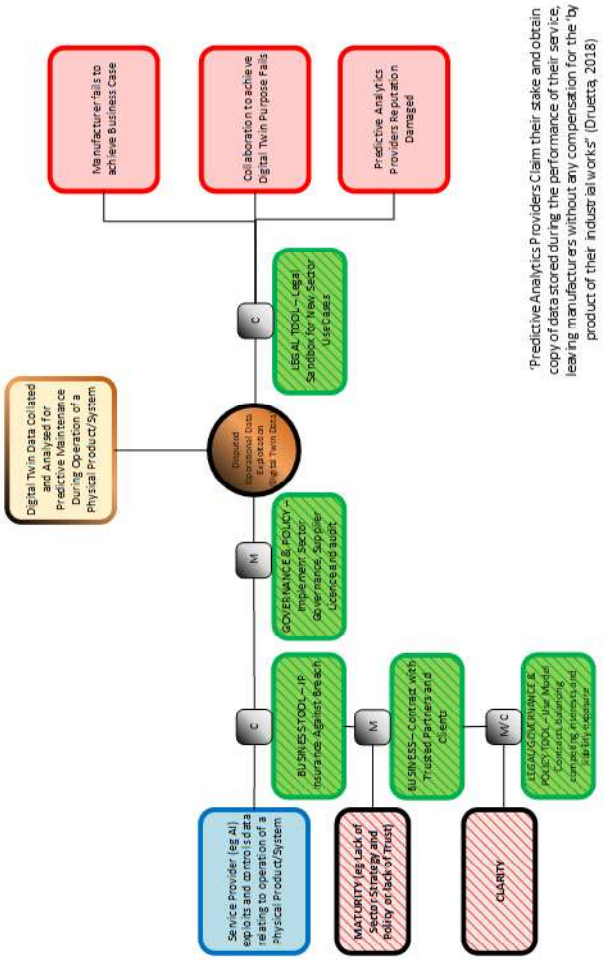
If the framework is materially updated following collation of the responses of all participants would you consent to being contacted again to run through the changes ?

Yes/No

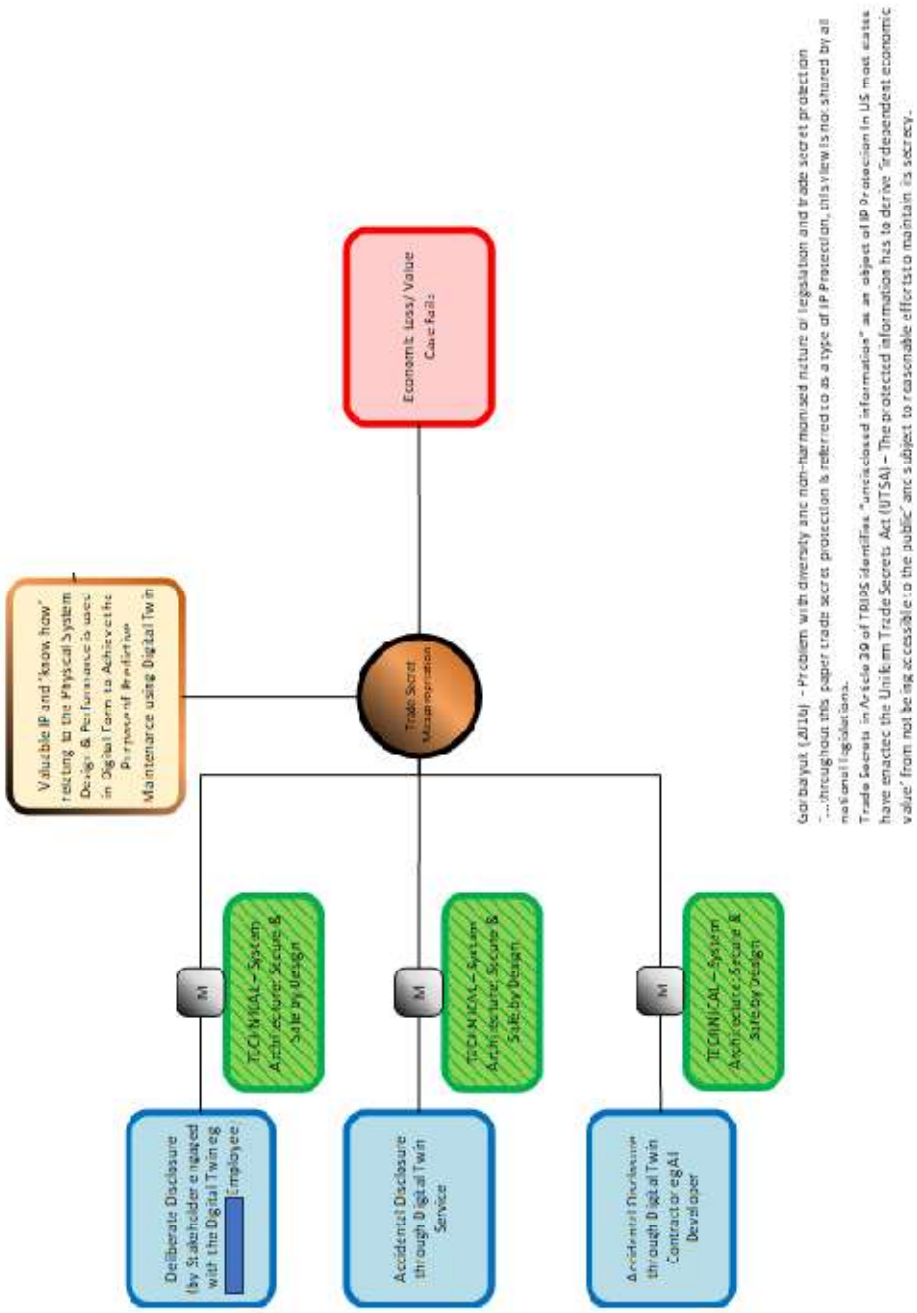
Appendix 9: Example Risk Bow-Ties

In addition to the example presented to Experts the following are examples of partially developed Risk Bow-Ties. These are used to illustrate application and are not intended to be complete. The green rectangles represent application of Tools to mitigate risks. The red hatched rectangles, outlined in black illustrate a Risk Influencer. For example, poor Clarity from low levels of traceability from stakeholders to obligations/requirements to contracts.

Example 1: Exploitation of Digital Twin Data Collated and Analysed, perhaps for Machine Learning, to support Predictive Maintenance During Operation of a Physical System



Example 2: Valuable IP and “know-how” relating to the Physical System Design & Performance is used in Digital Form to achieve the Purpose of Predictive Maintenance using Digital Twin but is misappropriated



Example 3: Access Declined to Valued IP or Proprietary Data Essential for Achieving Purpose of Predictive Maintenance using Digital Twin