# Towards Wireless Technology for Safety Critical Systems

# Towards Wireless Technology for Safety Critical Systems

**A B Johnston[1] CEng MIET, W Schiffers[1] CEng FIET, A H Kharaz[2] FInstMC**
[1]Rolls-Royce plc, Derby, DE21 7XX, UK, [2]University of Derby, Derby, DE22 3AW

E-mail: andrew.b.johnston@rolls-royce.com, werner.schiffers@rolls-royce.com, a.kharaz@derby.ac.uk

**Abstract.** Wireless technology provides an unprecedented level of design flexibility for new system designs and legacy system updates. However, there are several challenges which present themselves when adopting wireless technologies for use in safety systems. This paper elaborates on available design techniques which can resolve the implementation issues for a given application, to ensure data communication between nodes is safe (deterministic), secure, reliable and available.

## 1. Introduction

Product and service complexity is increasing along with additional demands on leaner engineering practices in order to reduce development time and manufacturing costs. Product design flexibility is essential to enable new features and help manage customer requirements. The implementation of new technologies in order to improve system capabilities so that product solutions continue to meet the ever increasing demands of the customer is paramount. Among other control system related technologies, wireless technology is considered as a key enabler in meeting growing customer requirements and expectations. In recent years, wireless technology has gained acceptance within industry based on the wide scale adoption through commercial product developments, in particular the telecommunications sector from which many other industrial sectors benefit [1]. The wireless sensor network market was valued at $29 Billion in 2016, and is predicted to be worth $94 Billion by 2023 [2, 3]. Industrial control systems form a large share of this market.

Significant benefits through the introduction of wireless technologies and wireless sensor networks may include [4,5,6]: System simplification through the reduction in cables and connectors, system cost reduction, system size and mass reduction, reduced maintenance burden associated with the inspection and testing of cables, reduction in connector pin failures, improved system resilience to hazards through communication diversity, invulnerability to wider system hazards such as fire and force impact, providing galvanic isolation between equipment, minimising impact on extant infrastructure when incorporating additional functionality, and increasing system design flexibility. Additionally, wireless technology reinforces the ‘Industry 4.0’ and ‘Internet of Things’ (IoT) movement, and enables the possibility for fully autonomous unmanned systems and platforms.

## 2. Wireless Technology Examples

There are several different methods of wireless communication, including: electromagnetic waves (e.g. radio, microwave frequency or free-space optical) and acoustic. These are augmented by energy harvesting technologies (for example thermoelectric generators), and energy storage, particularly in the case of a wireless sensor network, however, the focus of this paper is wireless data communication based

on electromagnetic wave technology. The aforementioned wireless technologies themselves are not novel at the time of writing, however, their application in a control system to provide safety critical functions is.

## 3. Wireless Technology Challenges

There are several safety and cyber security focussed challenges when considering the implementation of wireless technology, these can be summarised as [7]: Eavesdropping, data availability (interference, jamming), data reliability, elevation of privilege (unauthorised access to system though exploitation of design flaw), and safety (predicable communication behaviour). These problems are compounded by a cultural issue whereby designers and independent regulators alike typically raise concerns against a technology which is not yet well understood by the mainstream. Education is the proposed solution to the cultural problem. The former challenges are not unique to wireless technologies; such challenges should be considered irrespective of what data communication is employed for a given system. A robust design process is required to assess the credibility of wireless technology implementation and mitigate any safety and security hazards which may be present.

## 4. Proposed Risk Assessment Framework

There is at present limited guidance which supports the consideration of wireless technology in industrial safety applications [8-10], the available guidance provides no clear strategy or process to be followed to substantiate the use of wireless technologies in a safety system. It is proposed that system modelling and appropriate design assessments can resolve the credibility for wireless data communications for a given safety function. The relationship between safety and security is complex and can only be managed through suitable design practices, such as model based systems engineering and cyber security threat modelling. The proposed safety and security assessment framework is founded on a basic two-tiered approach; the first, and most important, is based upon processes and modelling mitigations, the second is based on design and technology mitigations.

### *4.1. Design Process and Modelling Risk Mitigation*

A safety and security risk assessment process and framework should be developed. This should be 'model based', enabling the assessing of risks associated with each security and safety concern, supported by employing traditional Hazard and Operability (HAZOP) assessments, to understand the likely impact to a given system. The process will allow for system design, safety and security features to be identified which will eliminate or mitigate the risks identified. It may be possible to develop a more robust system-wide architecture to mitigate or remove the hazard in the first instance. For a given use-case, if the risk cannot be reduced to an acceptable level, then wireless technology will not be appropriate for use.

Due to its maturity, the proposed assessment process is based on the NIST generic risk model [11]. The risk assessment shall: Identify threat sources, events and vulnerabilities, determine their likelihood of occurrence, determine the magnitude of their impact, and determine their associated risk. Risk is a function of Threat, Vulnerability, and Consequence whereby the most complex attribute is Threat because it can be intentional, unintentional, natural or human initiated [12]. Attributes associated with human initiated threats are: Capability; the resources available to an attacker, Intent; the motive behind an attack and associated difficulty for a defence to impact against, and Opportunity; the conditions required in order for an attack to be successful. Risk is defined in equation (1):

$$Risk = (Capability + Intent + Opportunity) \cdot Vulnerability \cdot Consequence \quad (1)$$

The NIST guide [11] provides a taxonomy of definitions for threat sources; threat actors, threat types, vulnerability groups, and system access points. The most appropriate vulnerability group for this process is 'Communication and Network', which can be aligned to the Open Systems Interconnection (OSI) basic reference model [13]. Vulnerabilities associated with each OSI layer can then be identified, this could be done in accordance with the SANS Institute application [14]. The risk model is augmented

by an information security model; the three basic security concepts important to information security are: Confidentiality, Integrity and Availability. The risk assessment framework is proposed in Figure 1, the overall process is outlined in Figure 2.

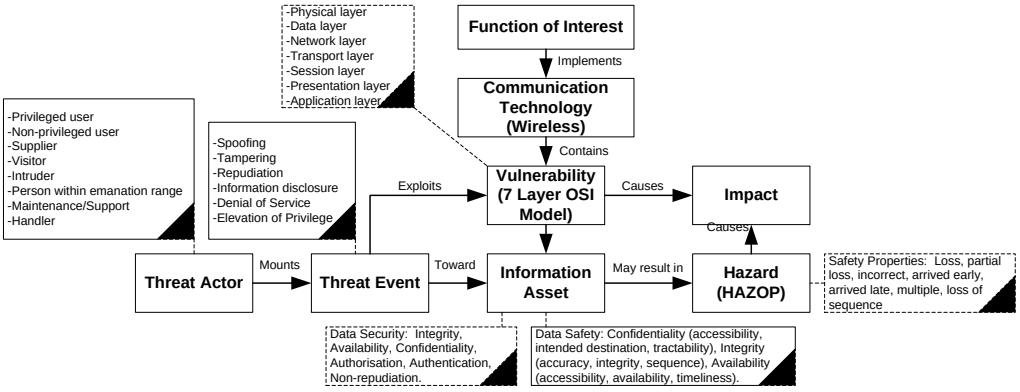


**Figure 1.** Proposed Safety and Security Risk Assessment Framework

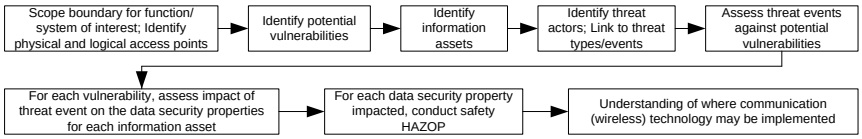


**Figure 2.** Safety and Security Threat Analysis Process

Where wireless communication may be found to be credible for use in a given safety function, modelling is to be used to demonstrate the propagation of the wireless signal path within its intended environment, quantifying a signal-to-noise ratio, providing the ability to eliminate or mitigate the effects of eavesdropping, interference, and to optimise the physical location of any wireless nodes within the system. From the model data, the credibility of signal jamming can also be assessed. Modelling of the protocol is then required to provide evidence as to the behaviour of the protocol, ensuring predictability in data packet handling, timing, and error management (data integrity and reliability). This design work should consider what network topology and protocols are to be used, and what standards they are to be assessed against. Prior to prototypic hardware development, measurements are to be taken in a representative environment to validate the model. Furthermore, identification of system operational policies and access controls will improve safety and security resilience for the intended system, but this should not be relied upon alone.

*4.2. Product Design and Technology Risk Mitigation*

Further risk mitigations are available during the product design stage; this should be underpinned by prototypic testing in a relevant environment with independent security assurance testing. The obfuscation of messages is a simple way to mitigate the effects of eavesdropping, data encryption further mitigates this risk, enhancing data integrity and confidentiality. Designing a receiver system to employ finite time listing periods will mitigate any external attempts of system overloading. Consideration of network scheduling and data synchronisation is required, as this potentially introduces the risk of common cause failure onto the network should the timing of the data within the network fall out of synchronisation. Employing unique message identifiers, which may be based upon a time stamp or an incremental transaction counter mitigates susceptibility to system overloading. Diverse signal propagation can be employed, using different carrier frequencies and protocols to mitigate common mode failure mechanisms. Indeed, it is considered that wireless technology can augment wired systems for safety critical functions to provide improved resilience to system safety and security hazards. Application of Commercial off the Shelf (COTS) solutions are recommended to support a proven-in-use argument; COTS solutions are subjected to a larger sample set of observations, thus providing more

accurate predictions on fault-free behaviour, safety and security robustness. It is often the case that the physical platform or environment can be used or modified to prevent data access outside of the system boundary. Finally, data encryption alone is not sufficient for system security or system safety.

## 5. Conclusions

It is considered that the introduction of wireless technology will not eliminate the need for wired functions for an industrial control system, this is particularly true for safety systems. Diligence is required to understand where wireless technologies can be adopted for safe and secure functionality. This approach should be no different to the consideration of safety functions deployed on wired solutions, and therefore, system safety and security robustness can be demonstrated via a robust design process. A simple yet robust design process for the consideration of wireless technology for use within a safety system has been presented. To date, the risk assessment process and associated electromagnetic modelling has been validated in a laboratory environment, supported by measurements in a relevant environment. Safety and security should be considered for 'IoT and 'Industry 4.0' applications. Connecting systems, including safety critical systems, to wider networks such as the internet is often cited in support of new technology trends such as 'big data' and Equipment Health Management (EHM). However, it is clear that this is a system level security risk and an indirect safety risk; one that needs to be addressed and very well managed as it may impact product safety and commercial credibility.

## Acknowledgements

The authors would like to thank Dr Robert Oates and Robert Barnes for their contribution to the development of the safety and security risk assessment framework.

## References

[1] Control Engineering Industrial Wireless Coverage Internet Page: www.controleng.com/wireless [Accessed March 2018].
[2] Wireless Sensor Network Market Worth, Internet Page: http://www.marketsandmarkets.com/PressReleases/wireless-sensor-network.asp [Accessed July 2017].
[3] Wireless Sensor Network Market by Offering - Global Forecast to 2023, Internet Page: http://www.marketsandmarkets.com/Market-Reports/wireless-sensor-networks-market-445.html [Accessed March 2018].
[4] Hope D C 2011 Towards a Wireless Aircraft, York University, ,
[5] Park P and Chang W 2017 Performance Comparison of Industrial Wireless Networks for Wireless Avionics Intra-Communications, IEEE COMMUNICATIONS LETTERS, VOL. 21, NO. 1.
[6] AVSI Future of Instrumentation and Internet Workshop, Wireless Avionics Intra-Communications (WAIC) Overview and Applications, May 2015.
[7] Chatham House Report, C S at Civil Nuclear Facilities, Understanding the risks, September 2015.
[8] BS EN 62734:2015 Industrial Networks – Wireless communication network and communication profiles – IAS 100.11a.
[9] PD IEC/TR 62918:2014 – Nuclear power plants – Instrumentation and control important to safety – Use and selection of wireless devices to be integrated in systems important to safety.
[10] Cyber Security Methods for Power Plant Equipment: Conceptual Small Attack Surface Characterisation – Tier 1. EPRI, Palo Alto, CA: 2015: 30002004999, 30/10/2015.
[11] National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1 – Guide for Conducting Risk Assessments, September 2012.
[12] Department for Homeland Security: 210W-06 Cyber Security for Industrial Control Systems – Current Trends (Threats).
[13] BS EN ISO/IEC 7498-1:1995 – Information Technology – OSI Basic Reference model.
[14] SysAdmin, Audit, Network and Security (SANS) Institute - 1309 - Applying the OSI Seven Layer Network Model To Information Security 21/11/2003.