Signalling and Cyber Security: Closing the gaps that prevent comprehensive security solutions

John Boss, BE, MBA, FIRSE

SUMMARY

Cyber security is an issue that needs to be addressed in signalling systems. There are however, no cyber security standards for signalling. Cyber security is a multi system problem, and further complicated by the fact that signalling and security disciplines are different in nature.

The critical issue is the potential for misalignment of context. – in particular, how the signalling engineer views 'the problem' may not align with the actual cyber security challenge that needs to be addressed. Simply encrypting some data channels does not make for a comprehensive solution. This paper examines that potential misalignment of context, by reflecting on three paradigms of signalling, viewed through a cyber security prism.

Firstly, the definition of a system that is used by signalling engineers is compared with security architectures currently defined in cyber security standards for industrial applications. Secondly, the definition, and process of risk analysis is compared to reveal underlying differences between signalling and security concepts - but also highlight areas of commonality. Finally, the signalling approach to updating safety code is compared with the IT practice of updating (patching), and examples are discussed that attempt to address the issues that result.

The conclusion is that close collaboration is necessary between the safety engineers and the security engineers to ensure comprehensive cyber security solutions for railways are developed.

1 INTRODUCTION

Railway signalling systems were traditionally closed systems using proprietary equipment. Current developments are increasingly using more digital networks, open standard protocols (e.g. IP) and more COTS (Commercial Off the Shelf) equipment. The digital attack surface is increasing. These developments are happening in an environment where cyber threats to railways are becoming more real. Cyber security is an issue that needs to be addressed.

There are no cyber security standards for the railway environment. Signalling engineers have a responsibility to address cyber risks but have limited tools and guidance to do so. The critical issue is the potential for misalignment of context. – in particular, how the signalling engineer views 'the problem' may not align with the actual cyber security challenge that needs to be addressed. Simply encrypting some data channels does not make for a comprehensive solution.

The first objective of this paper is to close the gap caused by that potential misalignment of context, through reflecting on three paradigms of signalling, viewed with a cyber security prism.

Cyber security is a multi system problem and requires a multi discipline approach. The second objective of this paper is to help facilitate the interaction between signalling engineers and security engineers: by using the language of both disciplines, by pitching discussions at a system level and by providing a broad set of references.

The term "signalling system" is used generically through this paper, it is intended simply to identify a system that is the responsibility of a signalling engineer, and therefore differentiate it from other business systems. Business systems include, enterprise systems (that deliver corporate functions - finance, HR etc.), operational systems (that control equipment and production processes – e.g. signalling), building systems (air-co, fire, heating, access etc..) and engineering back office systems (design, planning, maintenance terminals) etc.

2 CYBER SECURITY AND RESILIANCE

We hear a lot about cyber security in the media and the industry press. It is normally coupled with references to the "usual collection" of cyber attacks and an underlying implication that there is evil out there, lurking in the ether. There is a lot of hype, and even more scare mongering. Cyber threats are real [1] – there is a need to address cyber security, but in a systematic and controlled manner, not as a knee jerk reaction to scary press stories.

Cyber threats mean different things to different people. It includes phishing emails, fraud, theft (of intellectual property, goods, money and identities), spam, taking over industrial installations, money laundering, privacy infringements, knocking out power stations, identity theft, espionage (state and industrial), DDOS (Distributed Denial Of Service), malware, ransomware and child pornography. It is a broad concept. For the purpose of this paper we will consider cyber security only in the context of deliberate malicious attacks. Whilst this context excludes a significant part of cyber security (for example accidental acts[1]), it is sufficient basis.

2.1 Vulnerabilities

In the language of cyber security, a threat actor looks to exploit a vulnerability. Threat actors range from script kiddies to criminals and nation states. Some threat actors are so proficient they are classified as Advanced Persistent Threats (e.g. APT 10 [2]).

Vulnerabilities are weaknesses in a system and can be due to software, but also people, procedures, controls architectures etc. A vulnerability does not necessarily have to be a fault in the software (a bug), but it does provide an opportunity for an attacker to use code in a manner for which it was not intended, examples include cross scripting attacks or the teardrop attack[2]. The CVE database [3] contains a dictionary of publicly disclosed vulnerabilities. This database does not contain vulnerabilities that have not yet been discovered, nor vulnerabilities that have been discovered, but not disclosed.

2.2 Anatomy of a cyber attack

A cyber attack is often characterised by a series of actions over a longer period of time. Forensic analysis of cyber attacks has revealed that, in many cases, the attackers had been in systems for months prior to an incident occurring. The Cyber Kill Chain © is a model developed to demonstrate what a “typical” cyber attack looks like. There are several variations on the kill chain [4], but the basic idea is that an attack is not a singular event, rather a series of actions that work through a phased progression. The concept of the kill chain in cyber attacks is well reflected in industry publications [5].

The model in Figure 1 below, was proposed by Nachreiner. It is of particular interest as it shows not only reconnaissance, delivery, exploitation and infection phases, but also a phase of lateral movement. The lateral movement phase is described as the attacker obtaining access to other systems on the network.

Figure 1:Cyber attack kill chain by Nachreiner [4]

What this model helps us understand is that an attacker can use one system to reach another system: e.g. the way in could be by a back door in the HR system, but the target is the control centre. An attack vector (the approach to executing the attack) may define a strategy of entry, a path to the target, escalation of rights, delivery of the payload and finally manipulation of the system under attack (or extraction of the data). This makes a cyber attack not only a multi-step process, but also a multi system problem.

An attack should not always be viewed as someone in a hoodie taking control of a railway with the intention of crashing a train, something that Bruce Schneier refers to as “movie plot threats” [6]. An attacker could be using the

[1] Addressing accidental acts that facilitate cyber security issues is a necessary part of cyber security. The limitation on the scope has been solely for the purpose of readability. Cyber security requires attention in the technical sphere, the governance sphere as well as the socio-technical sphere.

[2]. Cross scripting works by inserting a command into a data entry field, thus instructing the code to operate in a manner not intended. The teardrop attack [42] worked by inserting a negative number in the IP header for packet length. The code responsible for reassembly of the message reserved memory for the message reassembly based on message length as advised in the IP header as an unsigned integer. A negative number (which is designated by having the most significant bit set to 1, e.g -200) was therefore interpreted as a very large positive number (in this case 2^{32} – 200 = c.a 2.4GB) which resulted in a memory reservation that overflowed available resource.

signalling system to gain entry to other systems, or using enterprise systems to get access to the signalling system. The signalling system could just be a step along the way to a final target.

The goal of the attack could also be hijacking system computing power to mine for bitcoins, or recruiting it as part of a botnet (for e.g. DDOS attacks on third parties or sending spam). The attack might look to use system components, like a sim card to make phone calls to Malaysia (which was an actual case involving components in a signalling system). The attack itself might not have any short-term effects on the operation of the signalling system (as would be the case with botnets). Having someone in the system but not doing anything might sound benign but two problems remains: first there is malicious code in the system that could have unpredictable consequences in the future and second, the performance of the system is under the influence of an unknown third party. There is also the possibility that the malicious activity is only masking another attack (e.g. make noise on the railway while the bank is robbed).

2.3 Resilience

Prevention has been described as a mode of control where efforts are made to stop an event impacting a system. Resilience is the capacity to continue operation after the event has impacted the system. The definition of when a cyber attack starts can be quite fluid. The quest for resilience therefore needs an understanding of when someone is already in the system – before they have a chance to do anything. This raises the question of Security Operations Centres (SOCs) and intrusion detection systems to monitor the cyber integrity of the operational as well as enterprise systems – a subject for a future paper.

The challenges of prevention and resilience are compounded by the changes in threats, unpredictability of attacks, difficulties in identifying vulnerabilities and developments in attack methods [1]. It may not be clear where a threat actor will try to gain entry, nor what the final target may be. This cannot be fully appreciated unless the business as a whole is taken into account, which leads to the first paradigm, being the definition of the system.

3 SYSTEM DEFINITION PARADIGM

The systems definition paradigm relates to the definition of a signalling system. “To a hammer, the world is a nail”, and this is the case when signalling engineers discuss cyber security. When signalling engineers discuss anything, it is, almost by definition, limited to the signalling system. There is however, a broader system definition necessary for the purpose of the security assessment / design. This broader system definition is referred to IEC 62443-3-3 [7] as the System under Consideration (SuC).

3.1 System under Consideration

There are therefore two system definitions that need to be agreed when discussing cyber security and signalling. The first being SuC (the subject of the security engineer), and the second being the signalling system, (a subsystem of the SuC, the subject of the signalling engineer).

The system definition paradigm starts cracking when applying cyber security to signalling systems. This is because the SuC is significantly bigger than just the signalling system. A railway business exists for the sole purpose of moving people and things. This purpose cannot be achieved with a signalling system alone. A railway business uses many systems to deliver the transportation product, including enterprise systems, operational systems, building systems and control systems. It is the totality of the systems required to run the business that should be considered as the SuC.

Business systems use both IT (Information Technology) systems, and OT (Operational Technology) systems (e.g. SCADA, Interlockings etc). IT is applied extensively in the enterprise systems whereas OT is applied in production processes and operational systems, however, as we will discuss later, this delineation is becoming increasingly blurred. The situation is further complicated if we include operators and rolling stock companies (Business to Business networks), rolling stock on board systems and IoT (Internet of Things) devices.

Defining security requirements from within the scope of a signalling system alone will miss a significant part of the cyber security challenges applicable to the business, and therefore a significant number of threats to (and potential solutions for) the signalling system.

3.2 Security Architectures

"Security architecture", as defined in NIST SP800-160 [8] is "A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected". Security architectures are useful mechanisms to achieve an overview of security aspects of a SuC – including the definition of the SuC and the place of the operational systems therein.

Operational systems have been addressed in security architectures for business systems for many years. The Purdu reference architecture [9] dates from 1994. It is somewhat dated and limited in application for rail systems but it acknowledges the need to move information between operational systems and enterprise systems. There are no defined models or standards for security architectures in railways. The closest that are available come from industrial control standards. Bastow [10] notes the similarities of signalling with SCADA systems.

A number of security architectures from industrial control standards are discussed below. The common aspect between them is that, when examining the security of the operational systems, they all take account of the enterprise systems as well as connections to the internet. In each, the approach is to address security in the context of the whole business, not isolated parts thereof.

The US Department of Homeland Security (DHS) model released a model in 2012 that was published by APTA [11] . The model presented an architecture of an industrial installation defining external, corporate, data, control and safety zones. The concept of security level was associated to the zone definition. This architecture included firewalls to separate zones and even recommended an air gap to separate production from non-production systems.

IEC 62443-3-3 [7] presents an architecture implementing the IEC 62443 general concept of security zones and conduits. This model includes enterprise zones and connections to the internet.

DHS released a model in 2016 [12] that maintained the security zone concept but reduced connectivity to the external world, it included specific provisions for patching and dropped the recommendation for the airgap present in the DHS 2012 model.

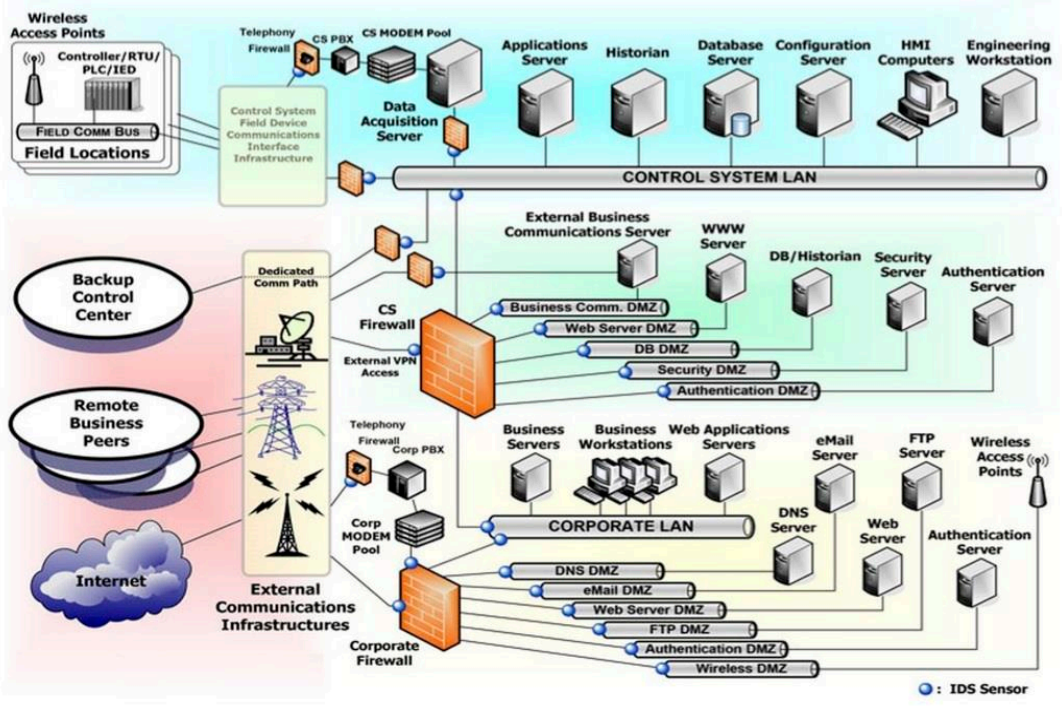

Figure 2: NIST architecture - NIST Special Publication 800-82 rev 2 [13])

NIST (the US National Institute of Standards and Technology) published a series of cyber security special Publications. NIST Special Publication 800-82 rev 2 [13] released in May of 2015 provided a recommended architecture for defence in depth for industrial control systems. This is shown in Figure 2 above. This architecture includes the entire business, with the operational control elements being only one small part (tucked away behind a series of firewalls in the top left hand corner). A point of particular interest is that this model includes intrusion detection devices spread throughout the network. This is an acknowledgement of the potential for an attack from within, and the possibility for attackers to gain access to the system by means other than via "the front door".

3.3 Signalling architectures

Recent development on signalling architectures demonstrate the application of COTS and common protocols. IP interlockings, for example, using IP to transmit data between the interlocking and the area controllers. Three examples of architectures of railway signalling applications are discussed below.

The common aspect of these three examples is that whilst they all address aspects of cyber security (predominantly through encryption of communication links), the signalling system is treated in isolation of the rest of the business systems.

The EULYNX project implementation of DB [14] [15] presents a reference architecture including encryption and communications security. Whilst we see here an architecture for a signalling system that is incorporating security features, we still miss the enterprise level.

CY Rail Proposed an architecture with security zones and conduits (following the UIC 62443 approach) [16]. The extent of the architecture is limited to the signalling system.

A proposed security architecture for an interlocking [17] has a more elaborate collection of security devices but these remain limited to the signalling system.

What is missing in each of these three cases is the context of the business systems. There is evidence to support the adaptation of a broad definition of SuC at a transport agency and ministry level. The APTA transit agency network architecture [18] includes an enterprise zones and safety critical security zones. The Australian Rail Industry Safety and Standards Board (RISSB) recently released a rail cyber security standard [19] in which the little differentiation is made between OT and IT systems. The UK DoT Rail Cyber Security Guidance to Industry [20] acknowledges this point wherein it states: "Effective cyber security is reliant on full engagement at all levels of an organisation", a position endorsed by The Rail Cyber Security strategy [21].

The conclusions that can be drawn from this is that a comprehensive set of cyber security measures for a signalling system cannot be determined with reference to the signalling system alone. It requires consideration of the SuC.

It logically follows that a comprehensive set of cyber security measures for the railway business cannot be defined without reference to (amongst others) the signalling system. To do so would result in a sub optimised security architecture, ignorant of threats to, or emanating from, a major subsystem of the SuC. In essence, this means that the signalling engineers and the security engineer need to be working collaboratively with each other to define a comprehensive set of cyber security requirements – and most importantly, understanding where those requirements overlap different systems in the SuC.

3.4 The blurred line between IT and OT

Examination of the security architectures discussed above also shows a number of traditional IT components starting to find their way into the OT systems domains (firewalls, intrusion detection systems etc).

The worlds of OT and IT are galaxies apart, especially if it is safety related OT. Safety critical software is released only after completion of verification and validation in controlled stages defined by industry standards, e.g. EN50128. IT software is characterised by sprints, scrums and the concept of minimum acceptable functionality. As the saying goes, "it is released on Thursday because that is the day we ship". IT software brings with it a significant number of vulnerabilities. Bruce Schneier [22] makes the point most eloquently when he says "the software we use contains thousands of mistakes -- many of them security vulnerabilities". The use of COTS in signalling systems effectively imports these vulnerabilities, a point noted by Katzenbeisser [23].

If we accept that security considerations for the signalling system must be derived from the context of the SuC, then we must also accept that attacks on the signalling system may arise from vulnerabilities outside of the signalling system, and conversely, that attacks to systems beyond the signalling system may arise from within the signalling system. Assessing the risks resulting from the broader definition of SuC leads on to the next paradigm.

4 RISK ASSESSMENT PARADIGM

The risk assessment paradigm relates to the scope, definition and execution of a risk assessment for signalling. Risk assessment is a part of the safety system delivery process. It is also a part of cyber security. Risk analysis standards NIST SP800—30 [24] and ISO 27005 [25] produce artefacts for cyber security that look remarkably similar to the safety risk assessment matrices that are common throughout the signalling industry. A risk assessment for security, however is not entirely compatible with a risk assessment for safety.

The crack in this paradigm is best demonstrated by comparing the language used in each discipline to describe the risk assessment process. Key words from the risk evaluation process for safety and for security are shown in the table below. The sentence in the top row is how a safety engineer would look at determining risk. The sentence in the bottom row is how a cyber security engineer would look at determining risk. The sentences are divided into parts and a comparison of those parts is discussed below.

Hazard with probability of occurrence	causing consequences	producing safety risk
Likelihood of threat actor exploiting a vulnerability	causing impact	producing security risk

4.1 Hazard v Threat Actor exploiting vulnerability

Signalling focuses on hazards. Cyber security talks about threats. Threats and hazards are not the same. A hazard is the “source of potential harm” (ISO 31000) and is generally considered to be random in nature – it has a probability of occurrence. In the language of safety: hazards occur with a probabilistic distribution.

In the language of cyber security, there is a “likelihood” of a threat actor exploiting a vulnerability and causing an event resulting in an impact. The analysis is complicated by the identification of vulnerabilities.

The broader definition of a SuC includes IT (with all the associated vulnerabilities). The vulnerabilities that need to be considered might be within the signalling system, in the IT components protecting the signalling system, in other OT systems or in enterprise systems. This scope is significantly larger than just components of the signalling system itself.

Defining likelihood is somewhat less straightforward than determining hazard probability. IEC 62443-3-3 [7] defines threat as “circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service”. The point of interest in this definition is its inclusion of malicious intentional actions. Hazards can be modelled with a probabilistic distribution but threat actors have intent – and that is not probabilistic [26].

Defining the likelihood of a threat actor being able to successfully exploit a vulnerability is difficult at best. NIST SP800-30 [24] suggests looking at the capability, intent and targeting of the threat actor to help assess the likelihood of a successful exploit. The approach used in IEC62443-3-3 [7] is to define Security Levels (SL) relative to the capability, motivation and resource of the attacker. With both SP800-30 and IEC62443-3-3, one is left wondering how to assess the motivation of threat actors – an exercise arguably more complex than determining a likelihood! This also raises a philosophical question - If railways are considered critical infrastructure, and the threat actor under consideration is a nation state, then, at what point does the risk analysis become an evaluation of national security? It should be clear that estimation of likelihood is by no means a simple matter, nor in any way empirically probabilistic.

4.2 Consequence v impact

Determining the consequences of a safety event or the impact of a cyber incident will in many cases (but not all) result in the same analysis. The operational impact of a system disturbance due to a component failure is

independent of that failure being caused by a defect of that component, or, an attacker shutting that component down (dependant on failure mode). This raises the issue of the security engineer and the safety engineer sharing artefacts from their analysis. The operational implications of failure modes will be of great interest to the security engineer. There are clearly cases where consequences of a failure and a vulnerability exploit will be operationally independent.

4.3 Security risk v safety risk

There are safety risks that do not impact on security, and security risks that do not impact on safety. It is, however worthwhile examining where safety and security meet (and overlap). There are safety scenarios that have security impacts (e.g. a fire in a control room that means the systems are unattended) and security scenarios that have safety impact (e.g. breach of encryption on safety critical communications, or an unlocked door to an equipment enclosure).

Safety assessment and functionality is based on an assumption that there are effective security measures in place [27]. If a system is not secure, then it cannot be safe [19] [28]. This statement may attract some criticism from the hardened signalling engineer who would argue that in a system with well-defined and engineered failure states, the biggest problem could only be availability. However, this argument fails on two points.

- Firstly, the defined failure states are precedented upon a logical interaction between a failure event and the system state. This logic does not hold true when there is deliberate interference with the system, (this is the modern-day digital equivalent of someone holding up a track relay).
- Secondly, the concept of safety within the context of railway operations extends beyond a single safety system. Unsafe situations can be created for the railway environment even though the signalling system has been forced to a safe state. Consider, for example, the consequences of stopping trains in tunnels.

If we accept the premise that an unsecured system is not safe, we must also accept that security requirements are necessary to assure safety. This is referred to in literature as “security for safety” and seems to be the major focus to date in addressing cyber security of railway signalling systems [29].

The case of “security for security” has been conspicuously absent in signalling industry literature – it seems to be a white spot in the cyber security thinking in signalling. There is a class of non-safety risks that are relevant for security, which are underrepresented in signalling design / research. This reflects the crack in the paradigm.

4.4 Risk assessment approach

Given the differences between security and safety risk analysis, and the multiple variables that need to be considered, one might be asking where to start? NIST SP800-30 [24] notes that the approach may differ in respect to orientation and starting point. Three approaches are presented being: Threat oriented (starting with the identification of a threat and then working out to vulnerabilities), Asset/impact oriented (starting with impact on critical assets then working back to threats), and Vulnerability oriented (starting with vulnerabilities and working back events that could exploit those vulnerabilities and consequences thereof).

Flexibility in the risk assessment methodology is demonstrated in Bloomfield et al [30]. The risk analysis on ERTMS is performed by identifying trust relationships between the components in the overall architecture, then identifying weaknesses in the ERTMS specifications. Bloomfield et al note that they made no attempt to rank the attack scenarios as they state that “is a matter for government and industry stakeholders”. This study then defines the capabilities required to launch the defined attacks. In this way, they have sidestepped the problems associated with understanding the capabilities and motivation of the attacker, changing the focus to capability required for defined attacks. Another good example is Rekik et al [31] with a security risk assessment for train control. This assessment broadens the system scope to include customer-oriented services on board i.e. WiFi.

The conclusion that can be drawn is that cyber security risk assessment of the signalling system must be broader than the signalling system itself, both in terms of system definition and the types of risks that should be considered (“security for safety” as well as “security for security”). The complementary conclusion is that the risk assessment of the SuC must necessarily include detail from the signalling system.

5 SYSTEM UPDATE PARADIGM

The system update paradigm relates to how often the systems, or safety code, in a signalling system can be expected to be updated. The signalling discipline understands a development lifecycle conform EN50126. After commissioning, systems (hopefully) settle down to decades of undisturbed operation – it is static. There is no need to change the safety code unless the track layout or operating requirements change. The system update paradigm starts to crack when patching requirements for IT systems are considered.

IT works on a different cycle. Patching is a phenomenon that we are familiar with in this day and age. We (should) regularly download patches for our phones and computers as there is a constant stream of new vulnerabilities identified that need to be patched.

The idea behind patching is that when a new vulnerability is found, someone must "fix" the code to remove that vulnerability, or at least remove the possibility of exploiting the vulnerability. The "fixed" code is then distributed as a patch to all those people that use that particular code. Zero days are vulnerabilities that have been discovered in code but not yet used in an attack. A zero day[3] is particularly useful to an attacker as it usually means that it has not been patched. The ability to patch the software is a fundamental component of cyber security with dedicated standards in both IEC62443-2-3 [32] and NIST [33].

Patching is not the only issue. A similar challenge exists when replacing obsolete technology. The life cycle of computing devices is quite short. With the ongoing developments in technology, the most up to date chip today could be dropped from production tomorrow. If spare parts are not available then the system cannot be supported. The result is usually that alternate products and parts need to be used, which also has the potential to trigger a safety (re)certification.

The conclusion that can be drawn is that the use of IT and COTS within the SuC imposes additional requirements on the signalling system – in particular, the ability to patch. Careful consideration is required on systems architecture to limit impact of patching on safety certification. Regular patching is economically incompatible with the safety system certification requirements.

The challenge is being able to patch software without having to revalidate safety cases every time. If there is a vulnerability in the safety code that needs to be patched, then it is probably reasonable to revalidate the safety case during that patching process.

A number of approaches are being developed to allow devices for cyber security to be patched within the signalling system, whilst insulating the signalling system from the need for recertification. Some of these are discussed below.

5.1 Embedded security

The null option is to embed the cyber security within the safety critical systems. There are, for example, some cyber security requirements defined in the ERTMS specifications. Subset 26 [34], [35] and subset 37 [36] (in particular) require checking of certain aspects of messages prior to their acceptance. These measures however, are massively insufficient to address the most basic of cyber threats. The relevance of the null option is that embedded measures are insufficient. Furthermore, embedding security measures in the safety code means every patch requires a safety case revision, which seriously constrains the ability to keep defences in line with a developing threat environment.

5.2 Security Shell

The approach of the security shell is to encapsulate the safety functions to the greatest extent possible [23] [17] [37]. The shell proposal does not address the issue of vulnerabilities in the safety system, rather it provides a security layer around the safety systems. Encapsulation utilises firewalls and encrypted links. Encryption is not new to the railway signalling industry. It is, after all, the susceptibility of the ERTMS GSM-R encryption to attack that has been the subject of a number of cyber security papers [38] [39] [40].

[3] Zero days get their name from the fact that it is zero days since it was used in an attack. If a vulnerability has not been disclosed, then the first time industry will know about that vulnerability is when it is used in an attack. After the vulnerability is identified in the post attack forensics, work can commence on developing a patch for it.

An important point in the approach is that the security shell encryption is applied at OSI layer 3 (network layer) whilst the national communications protocols (compliant to EN50159 [41]) are applied at OSI level 7 (application layer). This means the safety integrity of the message is assured at the application.

This approach has been discussed with the German safety authorities. It has been advised, that agreement has been reached. DB Netz is proceeding with a rollout of the security shell on test sites.

The security shell approach provides protection to the safety functions, and allows updates to the security applications without affecting elements addressed in the safety case of the safety systems. It does not address issues of patches that may be required for the safety systems.

5.3 Dual Channel

The dual channel approach relies on a comparison of a protected safety system and an unprotected safety system [27] [29]. The theory is that the patches applied to the protected system can be confirmed to have no influence on the safety system by comparing the output of the protected system with the output of a non-protected system. As the non-protected system cannot have been affected by the patch then it can be used to ensure the validity of the protected system.

One issue with this approach is that two safety systems must be provided to allow for the comparison, which introduces a cost as well as a reliability issue. A second, more philosophical issue, is the validity of the output from the unprotected system. There is a logical incompatibility between the statements “If a system is not secure then it is not safe” and “use the not secured system to validate the safety of the secured system”.

5.4 Virtualisation

Virtualisation refers to the use of separate of programs operating on a single hardware platform. This approach is being addressed under the HASELNUSS project. The most common form of virtualisation would be multiple applications running on a desk top computer. Virtual Lans (Vlans) is another example, and these have been implemented extensively throughout IT application.

The theory with virtualisation is that the safety and non-safety programs can be run in segregated layers of a common computing platform. If the separation can be demonstrated sufficiently, then it would be possible to allow patching of certain programs without impacting the safety integrity of others.

6 THE DELIVERY PROCESS

The cracks in the aforementioned paradigms demonstrate that the traditional signalling perspective is too constrained to be able to fully identify and implement the requirements for a cyber secure system.

Not only do cyber security requirements come from beyond the limit of the signalling system. It should therefore be clear that application of EN50128 does not provide cyber security. Solutions for cyber security requirements may best be implemented (at least in part) outside the signalling system. This has implications for the signalling design process which can be demonstrated against specific phases of the “v model” from EN 50126.

Phase 2 (System definition & Application conditions): The signalling system should be viewed as a subsystem of the SuC. The definition of the signalling systems must take account of the environment into which it is to be placed. Cyber, it could be argued, is another dimension of that environment.

Phase 3 (risk analysis): Cyber risks should be identified address safety – the “security for safety” aspects as well as security risks associated with the SuC - “security for security”.

Phase 4 (System Requirements): Expect a number of additional requirements resulting from cyber threats in the risk analysis.

Phase 5 (Requirements apportionment): Apportionment of requirements to outside of the signalling system (export) should be considered.

Phase 6 (Design and implementation). This phase provides the most interesting opportunity for addressing cyber security requirements in the basic architecture of the signalling, but also in the security architecture. It is

entirely feasible, that addressing requirements may lead to a change in the system design and implementation. The secure shell approach, discussed above, is one manifestation of the cyber security requirement driving a rethink of the signalling architecture.

There is a second half of this discussion, and that is from the perspective of the security design process. The security engineer developing the security solution for the SuC will need the input and cooperation of the signalling engineer. A mapping of those requirements to the "v model" would be mutually beneficial.

7 CONCLUSION

The first objective of this paper was to close the gap caused by potential misalignment of context, through reflecting on three paradigms of signalling, viewed with a cyber security prism. Three paradigms were presented to examine signalling in the context of cyber security, and conclusions were drawn from each:

- The system definition paradigm demonstrated that a comprehensive set of cyber security measures for a signalling system cannot be determined with reference to the signalling system alone. It requires consideration of the SuC.
- The risk assessment paradigm highlighted that cyber security risk assessment of the signalling system must be broader than the signalling system itself, both in terms of system definition and the types of risks that should be considered ("security for safety" as well as "security for security").
- The system update paradigm highlighted that the use of IT and COTS within the SuC imposes additional requirements on the signalling system – in particular, the ability to patch. Careful consideration is required on systems architecture to limit impact of patching on safety certification.

The second objective of this paper was to help facilitate the interaction between signalling engineers and security engineers, which has hopefully been achieved. The overall conclusion that must be drawn from this discussion is that close collaboration is necessary between the safety engineers and the security engineers to ensure comprehensive cyber security solutions for railways are developed.

A further point of consideration is disclosure and information sharing between railway organisations. The definition of responsible disclosure is well embedded in the commercial IT world. ISACs[4] are common throughout industries. It would be of interest to examine the applicability, application and structure for similar arrangements in the rail industry.

Finally, this paper has limited discussion to engineering, which is only one part of the story. Threat actors utilise all manner of methods, including social engineering, phishing, dumpster diving, scattering infected memory sticks in carparks etc. The cyber security solution space must necessarily include training, processes and procedure as well as engineered solution. If you get a free memory stick during this conference, think about it before you plug it into your computer.

8 REFERENCES

[1] House of Lords and House of Commons Joint committee on National Security Strategy, "Cyber security of the UK's critical national infrastructure; Third Report of Session 2017–19."

[2] B. Barrett, "How China's elite hackers stole the world most valuable secrets," *Wired*, 2018.

[3] CVE Database, "Common Vulnerabilities and Exposures cve.mitre.org.cve. (visited on 28 May 2019). National Vulnerability database nvd.nist.gov (visited on 28 May 2019)." .

[4] P. Pols, "The Unified Kill Chain," *CSA Thesis, Hague*, pp. 1–104, 2017.

[5] National Cyber Security Centre (UK), *Common Cyber attacks: Reducing the impact (Cyber attacks white paper)*. .

[4] Information Sharing and Analysis Centre: an industry group set up to share computer security information with the aim of improving security for all members of the group.

[6] B. Schneier, *Click here to kill everybody*, First Edit. Norton & Company, 2018.

[7] IEC, "IEC 62443-3-3: Industrial communication networks — Network and system security," 2013.

[8] R. Ross, M. McEvilley, and J. Oren, "NIST SP 800-160v1: Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems."

[9] T. J. Williams, "The Purdue Enterprise Reference Architecture," *Comput. Ind.*, vol. 24, pp. 141–158, 1994.

[10] M. D. Bastow, "Cyber Security of the Railway Signalling & Control System," in *Aspect conference 2015*, 2015.

[11] T. Lawrence *et al.*, "APTA-SS-CCS-RP-002-13: Securing Control and Communications Systems in Rail Transit Environments Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones," 2013.

[12] Department of Homeland Security (USA), "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," 2018.

[13] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "NIST.SP.800-82r2: Guide to Industrial Control Systems (ICS) Security," 2015.

[14] B. Elsweiler, "EULYNX A strategic project for DB," *IRSE EULYNX Semin. Braunschweig, Ger. 05 Nov 2015*.

[15] ERTMS User Group and EULYNX partners, "RCA Alpha – Architecture Overview," *Doc. id RCA.Doc.2 Version Alpha.1*, pp. 1–46.

[16] Members Cyrail Consortium, "CYRail Recommendations on cybersecurity of rail signalling and communication systems," 2018.

[17] C. Schlehuber, M. Heinrich, T. Vateva-Gurova, S. Katzenbeisser, and N. Suri, "A Security Architecture for Railway Signalling," in *Computer Safety, Reliability, and Security, 36th International Conference, SAFECOMP 2017 Trento, Italy, September 13–15, 2017*, 2017.

[18] Americian Public Transportation Association, "APTA SS-CCS-004-16: Securing Control and Communications Systems in Rail Transit Environments, Part 3b : Protecting the Operationally Critical Security Zone," 2016.

[19] Rail Industry Safety and Standards Board, "AS 7770:2018 Rail Cyber Security, V2.0 Public-Consultation." 2018.

[20] Department for Transport (UK), "Rail Cyber Security Guidance to Industry," 2016.

[21] Rail Delivery Group (UK), "Rail Cyber Security Strategy," 2017.

[22] B. Schneier, "The human side of heartbleed," *https://www.schneier.com/blog/archives/2014/06/the_human_side_.html (accessed 28 April 2019)*. .

[23] S. Katzenbeisser, "Challenges in designing secure and resilient railway command and control systems," *IRSE news*, vol. March, pp. 2–6, 2019.

[24] NIST, "NIST SP 800-30r1: Guide for conducting Risk assessments."

[25] IEC, "NEN-ISO/IEC 27005: Information Technology - Security Techniques - Information Security Risk management," 2011.

[26] T. W. Edgar and D. O. Manz, *Research methods for cyber security*. Elsevier Inc, 2017.

[27] J. Braband, "Functional Safety , Certification and SW Updating - How to balance ?," *IRSE Presentation*. 2017.

[28] UIC (International Union of Railways), *Guidelines for cyber-security in railway*. 2018.

[29] J. Braband, “Cyber Security in Railways: Quo Vadis?,” in *Reliability, Safety, and Security of Railway Systems Modelling, Second International Conference, RSSRail 2017 Pistoia, Italy, November 14–16, 2017*, 2017, pp. 3–14.

[30] R. Bloomfield, R. Bloomfield, I. Gashi, and R. Stroud, “How secure is ERTMS?,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7613 LNCS, pp. 247–258, 2012.

[31] M. Rekik, C. Gransart, and M. Berbineau, “Cyber-physical security risk assessment for train control and monitoring systems,” *2018 IEEE Conf. Commun. Netw. Secur. CNS 2018*, 2018.

[32] IEC, “IEC 62443-2-3: Security for Industrial automation and control systems: Patch management in the IACS environment,” 2015.

[33] K. Scarfone and M. Souppaya, “NIST SP 800-40r3: Guide to Enterprise Patch Management Technologies,” 2013.

[34] UNISIG, “Subset-026-7, System Requirements Specification, Chapter 7 ERTMS/ETCS Language 3.6.0,” 2016.

[35] UNISIG, “Subset-026-8, System Requirements Specification, Chapter 8 Messages 3.6.0,” 2016.

[36] UNISIG, “Subset-037, EuroRadio FIS 3.2.0,” 2005.

[37] C. Schlehuber, M. Heinrich, T. Vateva-Gurova, S. Katzenbeisser, and N. Suri, “Challenges and Approaches in Securing Safety-Relevant Railway Signalling,” in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris*, 2017, pp. 139–145.

[38] T. Chothia, J. De Ruiter, and R. J. Thomas, “A Formal Security Analysis of ERTMS Train to Trackside Protocols Chothia,” in *Reliability, Safety, and Security of Railway Systems. First International Conference, RSSRail 2016 Paris, France, June 28–30, 2016*, 2016, pp. 53–68.

[39] T. Chothia, M. Ordean, J. de Ruiter, and R. J. Thomas, “An Attack Against Message Authentication in the ERTMS Train to Trackside Communication Protocols,” in *AsiaCCS ’17, April 02 - 06, 2017, Abu Dhabi, United Arab Emirates*, 2017.

[40] F. Pepin and M. G. Vigliotti, “Risk Assessment of the 3Des in ERTMS,” in *Reliability, Safety, and Security of Railway Systems. First International Conference, RSSRail 2016 Paris, France, June 28–30, 2016*, pp. 79–93.

[41] CENELEC, “EN 50159: Railway applications — Communication , signalling and processing systems — Safety-related communication in transmission systems,” 2010.

[42] C. Doerr, *Network Security in Theory and Practice*. 2018.