Oh Cyber Security doesn't affect me…right? Systems Integration and Cyber Security

Colin Hamilton-Williams, Eur Ing MEng CEng CSEP MINCOSE MAPM MIRSE, SNC-Lavalin Atkins

SUMMARY

We live in an unprecedented time of human connectivity and functionality. We have come to expect more and more functionality from our devices, our offices and even our homes. As system designers, we are being asked to design, retrofit and upgrade systems to modern standards. This means not just thinking about what the customer needs, but what the customer will need and even making passive provision for things we haven't imagined yet.

To do this we need connectivity, and by that I mean our systems need to talk to each other. Data is a rich resource that we can't get enough of. Mining this data and trending it, we get information which is used to improve our quality of service through functions, maintenance, or even the customer experience.

But all this connectivity comes at a price, and that price is vulnerability. By virtue of requiring access to the system for data, the system now has and access point that can be exploited which faces the outside world. Cyber-attacks have increased in complexity and frequency whilst system complexity connectivity as increased also. Risk mitigation techniques advise us that first we should avoid the risk, if at all possible. If not, transfer it elsewhere, mitigate, reduce or finally accept it. However, in order to do this we must first understand the system and how it interacts in the system of systems.

It's illogical to assume that all systems can be air-gapped and removed from networks as they once were, just as it's illogical to assume that a couple of firewalls will solve all your cyber related issues, the truth is much more complicated. Cyber security experts understand threats and vectors but without context, the effects are limited. Systems Integration gives us that context. Systems Integration is the discipline of ensuring that complex systems of systems are designed and integrated in such a way to deliver the high level functionality required by the concept. By merging this seamlessly from the concept stage with cyber security, decisions on architecture and protection can be better captured in the design process.

In this paper we talk about Cyber Security and Systems Integration. How effective Systems Integration and design, linked with cyber security can drive the overall solution and lead to a safer, more secure, and integrated solution.

1 INTRODUCTION

Cyber Security represents a growth area in the design of new and complex transport systems. As we move into the age of the digital railway, retro-fixing digital systems to protect them against cyber-attack is no longer enough. We need to put cyber security and cyber resilience both into new and existing projects in order to deliver systems that are safe, secure and efficient enough for today's transport needs and tomorrow's.

We're already living in an increasingly digital world, where advances over just the past five years have been staggering. Autonomous vehicles are being tested on our roads. Driverless trains are on the increase. Computer systems on aircraft are so advanced that planes virtually fly themselves. The broad perception is that the railways are finally catching up, with Network Rail's Digital Railway programme driving the modernisation of Britain's railways.

The rail industry cannot afford to stand still and is not. The digital revolution is enabling better connectivity, more data and functions than ever before but this connectivity comes at a price and that price is threats. The linking together of systems to create complex systems of systems combines many singular vulnerabilities or threat vectors into larger vulnerabilities to the functioning of the whole system. This also means that railway companies are being increasingly pushed to open-up their on-board networks to provide passengers with better, more reliable Wi-Fi and overall, a greater passenger experience. This new extra connectivity between trains, apps, Wi-Fi, websites and email to name but a few functions and this also means that the whole network, as an organism, is vulnerable in a way it never has been before.

However, the change is happening, the requirements and the need is there, whether it be through reducing operating costs or user demands to create these linked data rich systems and as such we need to find a way to embrace them whilst also maintaining strong Cyber Security and Cyber Resilience. While digital technologies

within our railway's operations aren't new, we are designing for them in way that we haven't in the past and this is where the connection to Systems Integration comes in.

As an industry it's our duty to protect that entire end-to-end digital ecosystem, the networks, the apps, the Wi-Fi, the control systems and much, much more. The whole system will only be as strong as its weakest link and sometimes, that weak link could have been avoided if we were using the right processes and mind set.

2 BACKGROUND

In the early days of railways, an effective means to signal rail vehicles simply did not exist. Not surprisingly, there were many disastrous collisions and loss of life. Similarly, there was a period in the history of the automotive industry when car manufacturers denied the importance of installing seatbelts. At the same time, the number of vehicles on the road grew rapidly. Again, there were many accidents and significant loss of life. Thankfully, things have moved on in both industry examples, but not without great sacrifice, and only achieved through a series of outcries, investigations, legislative initiatives, regulatory oversight and the passing of laws.

Then we had rudimentary electrical and electronic systems. They, by their design and definition were both air gapped because they didn't have the ability to be connected to anything else anyway and un-hackable because they either required changes in physical hardware or base logic that weren't possible unless you were there in person. At this stage Cyber Security was very much Physical Security; prevent the attacker from getting to the system and you prevent any potential malicious activity.

Unfortunately that was then and this is now, systems are no longer so rigid and separate. This has led to a confusing and potentially dangerous situations where cyber security is not taken seriously during design, or upgrades are made to a system that were once secure, placing them into potentially dangerous and open configurations.

The scale of the vulnerabilities left open is truly startling and is best summed up by the mere existence of the search engine called Shodan. This search engine is dedicated to finding internet connected devices. In the presentation given by Dan Tentler at the Defcon 20 conference entitled "Drinking from the Caffeine Firehose we call Shodan", he goes on to show how with little knowledge you can find devices from CCTV cameras and printers, accessing their feeds using basic default settings. However, this quickly scales up to the major leagues, finding safety critical assets such as traffic lights and even the control system for a Hydroelectric Dam. This is an unacceptable level of vulnerability for critical industries and we must get stronger at both finding, designing for and plugging our Cyber Security gaps.

2.1 Cyber Security

What is Cyber Security? In simple terms it is the defence or defensive strategies employed by a system to resist against both remote and local malicious or accidental actions. If we did not have Cyber Security then it would potentially be possible to hijack and control a system or systems potentially putting them into dangerous configurations.

How does Cyber Security differ from Cyber Resilience? If we go back to our example of the seatbelt; Cyber Security is not crashing in the first place whilst Cyber Resilience is the seatbelt and airbag the prevent loss of life and injuries during the event of a crash. Thus, Cyber Security is the prevention of access to a system where Cyber Resilience focusses on recoverability and maintaining functionality, safety and integrity.

Cyber Resilience in transportation has unique challenges. Unlike in many commercial enterprises, where data protection and privacy is king, the values at the core of our transportation infrastructure are different. The focus instead centres around three key principles: Safety, Integrity and Operational Resilience.

Our current big challenge as an industry is the exponential growth and deployment of digital technologies, That is, both delivering these and doing do so in a secure way. Solutions are designed with good intentions in mind, but by their nature are vulnerable to exploitation and compromise. Previously, industrial systems were protected through a physical separation between the operational environment and the public domain. This air gap is closing, driven by a desire to harvest data and increase automation through greater distributed control across a network.

2.2 Systems Integration

Systems Integration (SI) according to INCOSE for the infrastructure industry is the integration of systems within a project, not just the electrical, mechanical, architectural and civil systems, but also all technical and human elements. Often used interchangeably, but incorrectly, with Systems Engineering; System Integration aims to deliver project outcomes through the visualising and managing of the concept systems of systems delivering higher level functions and project outcomes. Careful consideration is required to be given to the makeup of systems and sub systems in order to manage the interfaces where complexity and difficulty often lie between disciplines. The main constituent parts of systems integration through a multidisciplinary approach are:

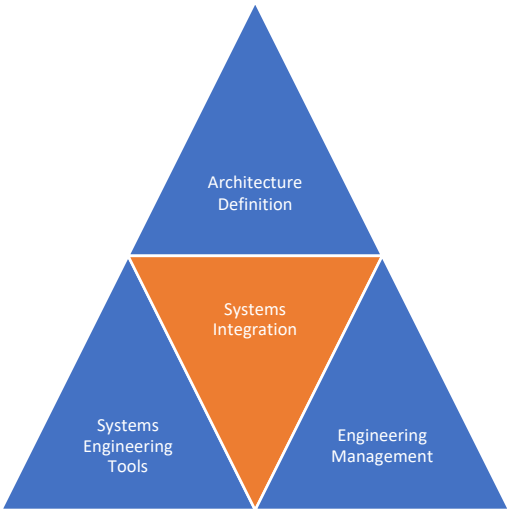

Figure 1: System Integration

Systems Engineering on the other hand is a toolset and methodology which can be used to deliver Systems Integration outcomes. The toolset focusses on the management of requirements and testable outcomes to ensure a system achieves its stated function.

A key tool in the System Integration toolset is the management of the Systems lifecycle. The Systems Lifecycle defines the expected phases of a project and the tools and actions to be used at each key stage. In systems integration, early intervention is key to reducing the cost of change and variation.

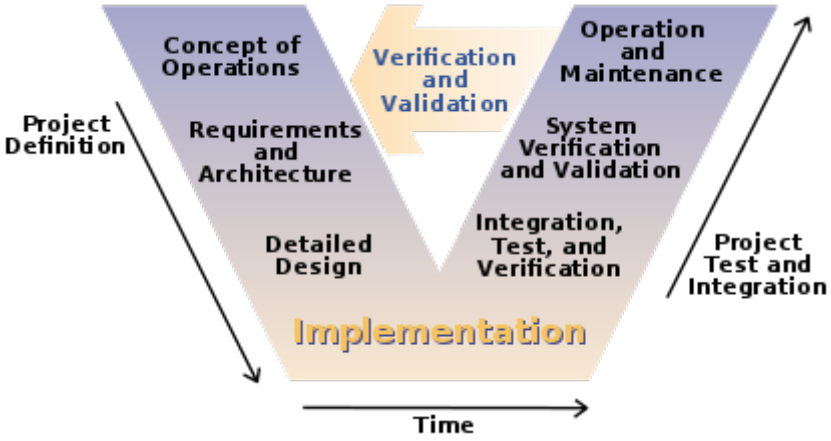

Figure 2: System Engineering Lifecycle

3 LIFECYCLE INFLUENCE ON CYBER SECUIRTY

Like many industry sectors across the globe, transportation is undergoing its latest evolution: boundless growth in the use of digital technology and widespread connectivity through the Industrial Internet of Things (IIoT).

Given the many advantages brought about by digital transformation and the advent of Industry 4.0, organizations are understandably eager to reap the benefits and become early adopters. However, this digital evolution must be undertaken in a risk-averse and cyber-secure manner; otherwise, there is a high likelihood of creating more harm than good. Such pivotal change raises some key questions. Is the transportation industry on track to achieve an adequate level of cyber resilience? Are the right technologies, skillsets and frameworks in place to safeguard our nation's Critical National Infrastructure (CNI)?

Combining the lifecycle approach and systems integration thinking with Cyber security can not only reduce upfront design costs but also potential issues across the entire life of the system.

3.1 Concept

Business environments typically comprise of converging technologies that include Information Technology (IT), which communicates to enhance business processes via Network Technology (NT). What sets the transportation and industrial sectors apart is the addition of a third element namely operational technology (OT). Convergence of these three engineering disciplines creates a "technology trifecta" within which the industry domain knowledge resides. It is the translation of electronic signals in the virtual plane into physical outputs in the real-world plane that amplifies the cyber resilience challenge. In our now cyber-physical world, undesired events can directly affect public safety or the environment.

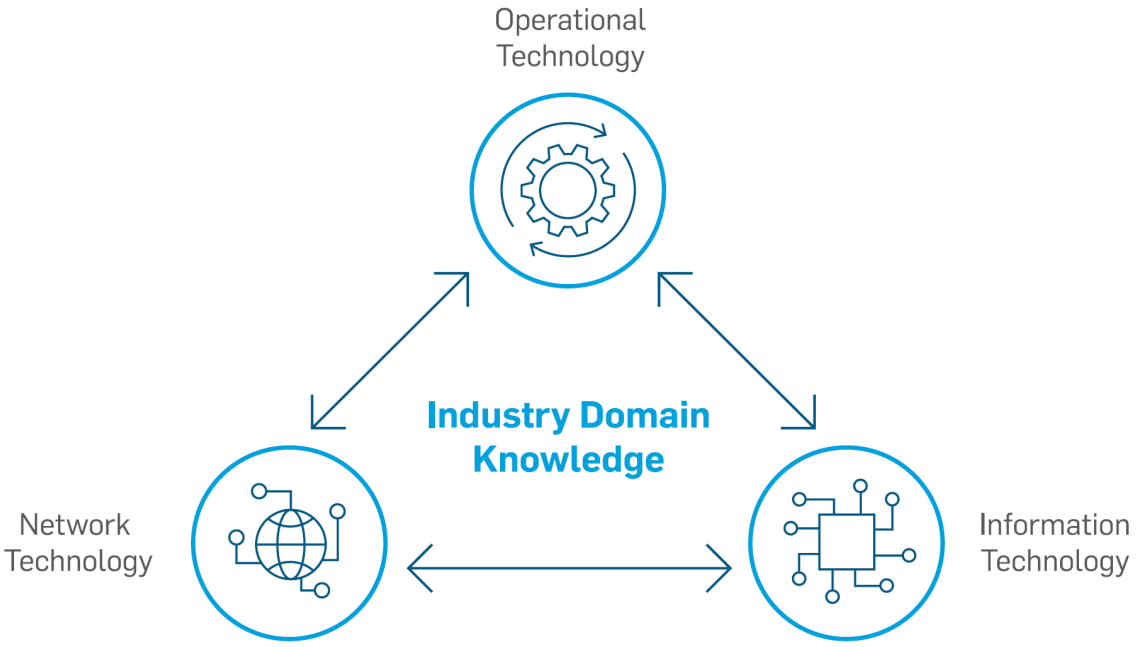

Figure 3: Industry Domain Knowledge

Rail systems comprise a complex array of network integrated systems and technologies, each with their own specific function and level of criticality. Rail-based transport systems are a melting pot for a multidisciplinary engineering base, where old and new technologies overlap and influence one another. Legacy and modern protocols, in every sense, must now coexist affecting interoperability and accountability. For this reason, addressing cyber resilience for transport infrastructure in greenfield or brownfield scenarios requires a unique approach.

Rail systems and assets are now dispersed, interconnected and remotely controlled in such a way that our infrastructure represents a complex nervous system with many moving parts and entry points. Modern-day rail solutions must be delivered with cyber security woven into the fabric of their design. As a result of this new digital facet, the execution of systems engineering and integration requires a fundamental re-think.

3.2 Design

A cornerstone of the Cyber Security workstream is the Threat and Vulnerability Assessment (TVA). Gaining a system-level understanding of all the assets included within a digital ecosystem, their criticality, function and architecture is required to identify and analyze the threat vectors present in an industrial environment.

A TVA is a key milestone when delivering greenfield infrastructure and is a fundamental element of cyber security engineering work in major projects. Periodic TVAs should be performed throughout the lifecycle of a system to ensure that the cyber security and resilience is maintained.

The goal of the TVA is to highlight the system's weaknesses and translate this analysis into a focused investment of time, effort and resources. Below is a description of the different stages of Cyber Security assessment and how they relate to the Systems Integration Lifecycle.

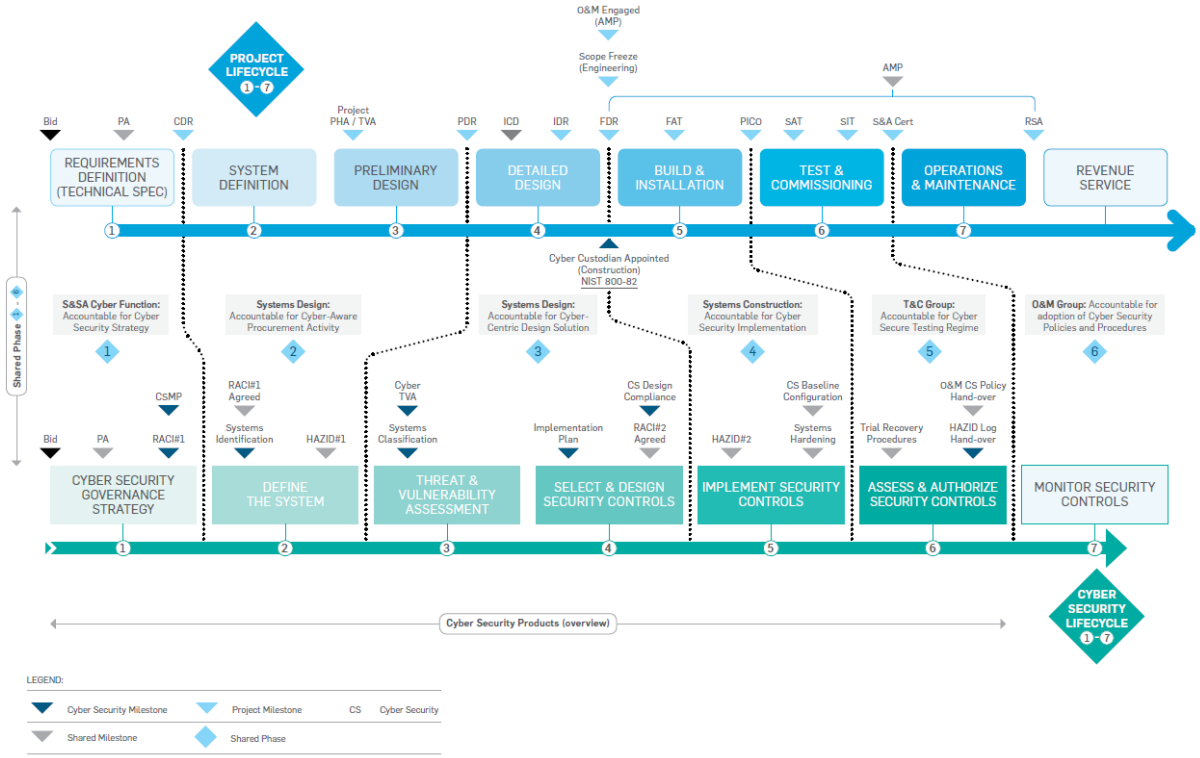

Figure 4: Stage of Cyber Security in relation to Systems Integration Lifecycle

Safety assets and systems, such as Rail Control Systems (RCS) or Tunnel Ventilation Systems (TVS), are essential to the safe running of metros and railways. Critical systems must be segregated and safe-guarded from malicious attack and accidental compromise. Operational resilience is concerned with maintaining availability of passenger services and business continuity of freight movements even in the event of a fault or failure in the underlying network or sub-system components.

These prioritized goals are achieved through pre-emptive secure-by-design and post-inception threat and vulnerability assessments. Cyber engineering must be undertaken by competent authorities who understand the industry domain, the way it operates and the embedded technologies, and can therefore emphasize where risk mitigation or enhancements are required most. Safety, availability, integrity and maintainability are the measures we use to gauge security posture in Critical National Infrastructures (CNI).

Critical systems must be segregated and safe-guarded from malicious attack and accidental compromise.

3.3 Construction

When considering ICS digital architectures, there is more than first meets the eye. The Purdue Enterprise Reference Architecture was defined in ISA99 to capture Human-Machine-Interfaces (HMI) at the application level, through to the end-point assets, and "everything" in between. Originally conceived to depict the connectivity

between the enterprise zone and the industrial environment, this model is now a powerful tool when depicting cyber security concepts. Below is an introduction to the typical equipment which resides at each level. Overleaf, a variety of technologies are discussed to explore how our ICS architectures can be secured and depicted in a holistic diagram, comprising the Purdue model levels 5-0.

3.3.1 Enterprise zone (Level 5)

Information Technology (IT) infrastructure systems and applications are confined to levels 4 and 5. Web, accounting and e-mail servers reside in level 5. In terms of security, this level is least trusted and must remain strongly segregated from the operational and/or production environments.

3.3.2 Site business planning and logistics (Level 4)

Level 4 is an extension of level 5 and it incorporates IT systems responsible for reporting, scheduling, operations and maintenance management, e-mail and printing services. Access to the ICS environment is managed through a Demilitarized Zone (DMZ). There is an increasing appetite for transferral of valuable data from the lower levels of the hierarchy into level 4 to enable business and optimization decisions. This must be carefully enabled to protect critical systems.

3.3.3 Demilitarized zone

The DMZ operates as a buffer where services and data can be shared between the ICS environment and the Enterprise zone. The DMZ enables the effective segmentation and security control. High visibility of network traffic exchanged can be gained at this level of the Purdue model, which enables deep packet inspection, anomaly detection, prevention and many other security functions.

A Cyber Security Platform (CSP), comprising security tools and technologies may also reside in the DMZ. The functions are centralized and cascade down to serve the lower levels. The security tools, systems and servers depicted in the Purdue model represent only a sample subset of the potential options that could be implemented within the CSP. A quarantine area is defined in the DMZ where external removable media used for updates and upgrades can be manipulated securely.

3.3.4 Operations and supervisory control (Level 3)

The components in level 3 are typically the front-end interface of the end-point devices. Equipment at this level enables replication, supervision and operation of ICS assets, for example: SCADA, Distributed Control System (DCS), Access Control (AC), Telephony, CCTV, and the CSP. The HMI's and applications in level 3 communicate with level 4 systems through the DMZ. Direct communication between these levels is highly discouraged.

3.3.5 Area supervisory control (Level 2)

Level 2 is where the core systems, servers and hardware reside. Maintenance terminals here are operated by trained ICS domain engineers and enable configuration, interrogation and manipulation of systems. The Network Management System (NMS) monitors network behaviour, builds a topology and provides a portal for implementation of NMS security policies. The system backup and image servers are also depicted in level 2.

3.3.6 Local control (Level 1)

The DCS represents the control entity which could be a Rail Control Systems (RCS) in rail applications, an energy management system in power grids, or a parking management controller in smart cities. Process control equipment is included in level 1 and comprises non-

Safety Integrity Level (SIL) and SIL Programmable Logic Controllers (PLC), Remote Terminal Units (RTU) and DCSs which are responsible for continuous, sequence, batch and discrete control. These level 1 devices directly manipulate the behaviour of the physical assets at level 0.

3.3.7 Process (Level 0)

Level 0 includes the instrumentation elements which directly connect to and control the process. For instance, assets at Level 0 may include traffic signals, level crossing barriers, CCTV cameras, circuit breakers, sensors, smart meters, ventilation systems and fire detectors. In rail, many of these systems are safety critical.

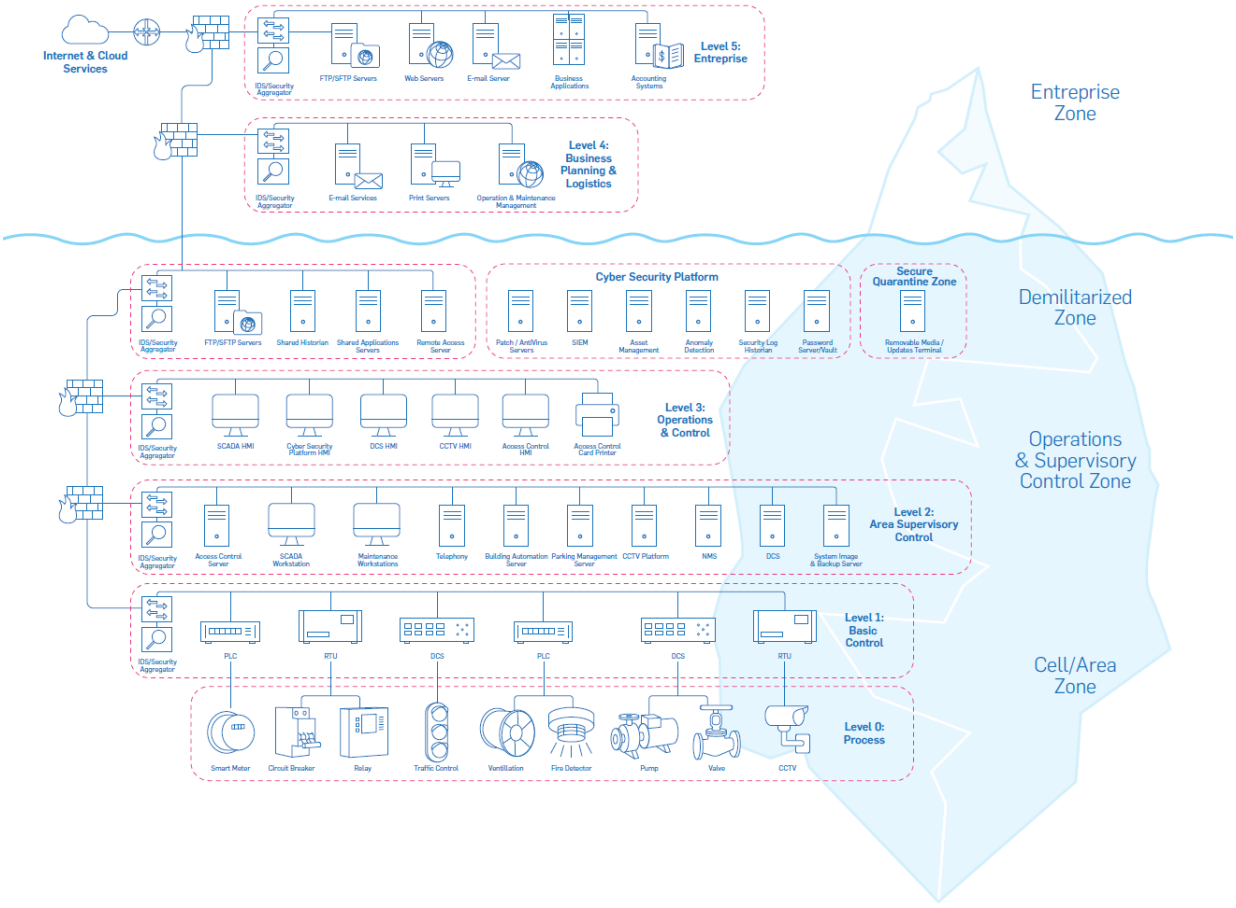

Figure 5: Cyber Security Level classification

Despite a similarity in the technologies used, there is a vast difference between typical data centres and industrial networks. Conventional ways of working in a traditional IT environment are often not possible due to the limitations and requirements of the industrial world as the requirements are different. This changes the way the systems must be designed, procured, built, tested, operated and maintained. Industrial devices and their functions are often proprietary in nature and may be sensitive to patching, updates or overlaid virus protection.

Thorough testing is a must, before deploying updates in a sensitive production or operational environment. The table below provides a summarized comparison.

Category	**Conventional IT**	**Industrial Control Systems**
Virus Protection	Widely Spread	Complicated, often impossible
Lifecycle	3-5 years	5-20 Years
O&M Outsourcing, Support	Widely Spread	Uncommon
Patch Management	Regular, Daily	Seldom, need approval by Systems Authority
Modifications	Frequent	Seldom
Time Dependency	Delays Accepted	Critical
Availability	8x5/260 – 24x7/365	24x7/365
Cyber Security Awareness	Good	Limited
Security Testing	Secured, by personnel	Seldom, problematic

3.4 Testing

Relying on firewalling is no longer sufficient to ensure cyber resilience based on the following:

1. Hackers have the resources and capabilities to circumvent a network perimeter to infiltrate critical infrastructure.
2. Insider threat actors may have access to equipment on the protected side of the Firewall.
3. The most common cause of cyber incident is human error – a Firewall in fact performs a very narrow security function and does not protect against the many sources of compromise.

Firewalls and endpoint protection remain the first line of defence and should be properly implemented and configured. A defence-in-depth approach consists of employing different levels of security and implementing different tools and technologies to achieve cyber resilience. The technologies below offer protection and enhancement beyond that of a Firewall.

Software Defined Perimeter (SDP) – SDP is a security solution which combines different security features to ensure that all endpoints attempting to connect to a network infrastructure are grouped, authenticated and authorized prior to being granted access. The SDP technology enables network engineers to define user groups efficiently, through a software driven tool and graphical user interface. This removes the overhead resulting from network reconfiguration and redesign, inherent to conventional mechanisms, e.g. Virtual Local Area Networks (VLAN), subnets and Access Control Lists (ACL). The result is a series of manageable and dynamic logical segments, as an overlay to the network fabric.

Asset management – Employing tools that can perform automated asset discovery, classification, register and management is a surprisingly simple and an ICS-CERT top 10 security measure which provides full visibility into the ICS network. This also supports planning of maintenance projects, prioritizing upgrades, deploying patches, developing incident response plans and proposing mitigation strategies.

Data diodes – Where data exfiltration by the ICS operator or maintainer is sought, this must be achieved in a secure way to safeguard the operational assets generating the data. Unidirectional gateways, or data diodes, can provide a one-way flow of network traffic via a physical network component. Fibre optic technology is used to guarantee that the in-flow of traffic from the Purdue zone with a lower trust level is impossible via this conduit.

Security Information and Event Monitoring (SIEM) – ICSs are heterogeneous environments with a broad mix of operating systems, devices and systems. A SIEM tool should be selected to enable real-time event log monitoring and support of the various environments. The event monitoring plan employed should not only monitor the security event logs but also other logs which could be indicative of matters such as application, hardware issues or malicious software.

The selected technology should enable tracing all monitored events back to their origin.

- Patching – From adding new features to repairing security holes and fixing or removing bugs, regular updates and patches of ICS digital assets should be conducted. A systematic process is required to ensure robust testing and roll-back procedure is in place before implementing a new patch in the live production environment.
- Security logging – Every system within a network generates some type of log file which contains a wealth of important information that could be used to reduce the ICS's exposure to damage, loss, legal liability, intruders and malwares. Proper log management strategy and tools should be employed to automatically manage log information coming from different sources, in different formats and in massive volumes.
- Anomaly detection – Anomaly detection tools enable identification of all the changes to critical assets, whether performed over the network or directly on the physical devices. They generate real-time alerts based on early detection of malicious activity and unauthorized changes, facilitating the troubleshooting of operational problems and the quick discovery of their sources.

Embracing digital solutions brings inherent risks. To achieve cyber resilience – in transportation and other CNI's organizations must manage and mitigate risks in the following three key areas:

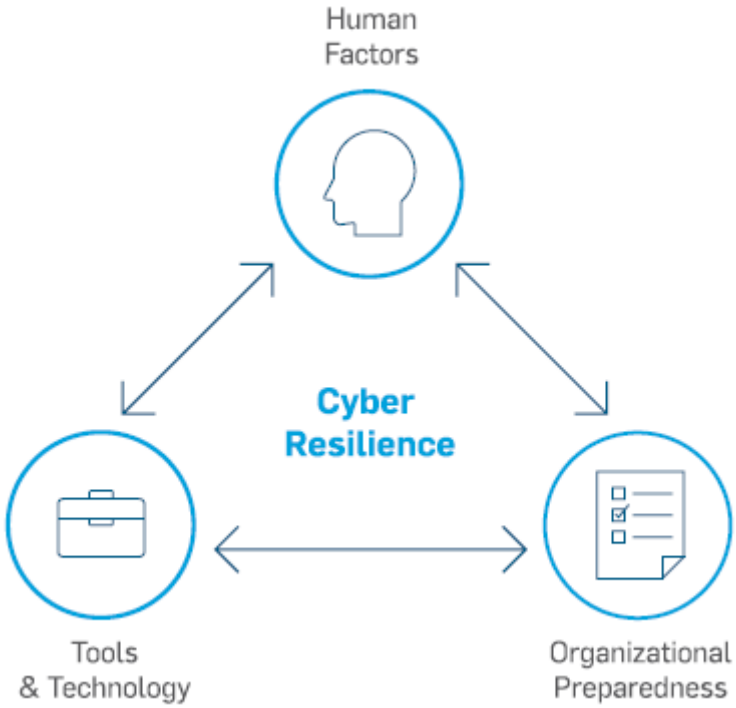

Figure 6: Cyber Resilience

A weakness or incident arising in any one of the three key areas can result in significant losses to a rail operator, including financial and reputational damages. Origins of compromise may include, but are not limited to:

- The supply chain
- Unsecure design architecture
- Unsecure legacy systems
- Lack of staff training
- Absence of contingency planning
- Weak physical security
- Incomplete asset registers
- Unsecure external network connections
- Increased connectivity and network access points
- Absence of system updates and patching regime

How can infrastructure owners, operators and suppliers address these unique challenges? Nearly three quarters of firms (74%) are currently recognized as being significantly underprepared in the key areas of cyber readiness [1].

Each scenario is different and will require its own unique starting point. For example:

Cities, municipalities and all levels of government should include cyber security as a fundamental part of any new transportation infrastructure project, through collaboration with a technical advisory group or subject matter experts.

Existing operators and maintainers should seek a security posture assessment to understand their current, real-world exposure to cyber compromise, associated financial losses and non-conformance to legislation, and also to understand where to best invest next as part of their digital transformations.

Suppliers and vendors of any magnitude should invest in cyber resources and skillsets to ensure they develop their products, solutions and services in keeping with the ever-evolving and ever-stringent cyber requirements and cyber legislation.

3.5 Operation and Maintenance

During the operation and maintenance period, you may be forgiven for thinking that if it was all done well during design then there is nothing left to do, however this couldn't be further from the truth. The paradigm now shifts to patching, updating and remedial works. In reality with an ICS there should be no large scale works required unless a new vulnerability is detected however with every change of function, additional system added new vulnerabilities and vectors can expose themselves. Doubly difficult, because of the shelf life of such a system is that the original knowledge used to create it is no longer available.

Any in service patching will require taking out of service of the asset which could lead to costly and expensive downtime thus, it is necessary to consider and plan for this eventuality both during the design and concept phases of the project.

Through lifecycle management the following can be achieved:

- The cyber landscape can be daunting. Establishing a starting point to assess your current cyber security risk level and exposure to compromise is essential.
- Developing a bespoke roadmap for the proper governance of cyber security, which fits your organization.
- Adopting cyber security principles throughout all echelons of your business.
- No stone left unturned in the following key areas: human factors, tools & technologies and organizational preparedness.
- Ensuring your organization's cyber-readiness enhancement is through focused investment and in the areas which need it most, to maximise your benefit.
- Applying the basics to ensure your organization is employing the fundamental measures to protect itself.

4 CONCLUSIONS

Cyber Security and Cyber Resilience are often after thoughts in complex multidisciplinary projects. Systems Integration, whilst often focussing on how a system should work, can be used to understand how a system may not work. It is therefore in the best interests of all major projects to actively engage these specialisms and combine their relative strengths to reduce costs, the risk of later rework and schedule delays and the overall risk to the system.

In order to deliver the most cost effective Cyber Security and Resilience, the earlier the engagement from the project, the more likely actions are to be taken and problems are either avoided entirely or mitigated. Engaging later in the project lifecycle leads to increase cost for remedies, the potential for a less secure system or even baked in problems that require additional resource to manage. In some cases, the cost required to rectify or deal with a Cyber incident are significantly higher than they would have been if design considerations were incorporated at earlier project stages.

The above represents conventional wisdom for addressing problems early rather than in the eleventh hour. However a further consideration is to employ both Systems Integration knowledge and Systems Thinking to help shape the outcome. Through a multidisciplinary appreciation of the system construction, the communications channels required and potential threat vectors, systems integration tools can help to visualise the system early in the lifecycle, highlighting potential avenues of threat and enabling corrective action to be taken as early as possible in the System Lifecycle. This can lead to fundamental changes to architectures to remedy issues with the potential t0 entirely change designs to increase resilience and reduce costs.

The railway industry needs to consider Cyber Resilience not just Cyber Security. In the joined up digital ecosystem, with data driving our daily lives, new interdependencies will cause threats, opportunities, and the need for action. We're already in that world now, and it's no surprise that issues are occurring with more frequency and Cyber Security is becoming a hot topic. In 2018, estimates by Cybersecuirty Ventures

- Sonicwall just reported a 300 percent year-over-year growth in ransomware, according to KnowBe4.
- Global damage costs in connection with ransomware attacks are predicted to reach $11.5 billion annually by 2019.
- A previous report from Cybersecurity Ventures predicted ransomware damages cost the world $5 billion in 2017, up from $325 million in 2015 – a 15X increase in just two years.
- Cybersecurity Ventures predicts there will be a ransomware attack on businesses every 14 seconds by the end of 2019, up from every 40 seconds in 2016. This does not include attacks on individuals, which occurs even more frequently than businesses.
- Ransomware attacks on healthcare organizations are predicted to quadruple by 2020
- 91% of cyberattacks begin with a spear phishing email, which are commonly used to infect organizations with ransomware.

But when so much is at stake, if our rail networks aren't fully protected, and train companies face potential malicious attack like never before, how can we afford not to be resilient? The joined up approach to managing Cyber Security and Cyber Resilience through Systems Integration needs to consider and address the following challenges:

- Concept
- Maintainability
- Whole lifecycle costing
- Future threats

5 REFERENCES

1. Tentler D. *Defcon 20 - Dan Tentler - Drinking from the caffeine firehose we know as shodan* [Online]. https://www.youtube.com/watch?v=5cWck_xcH64 [04/2019].
2. UK Government. *The Network and Information Systems Regulations 2018* [Online]. http://www.legislation.gov.uk/uksi/2018/506/contents/made [04/2019].
3. National Cyber Security Centre. *NCSC NIS guidance* [Online]. https://www.ncsc.gov.uk/collection/nis-directive?curPage=/collection/nis-directive/nis-objective-a [05/2019].
4. Morgan S. *Global Ransomware Damage Costs Predicted To Exceed $8 Billion In 2018* [Online]. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/ [04/2019].