international Engineering Safety Management

Good Practice Guidance

Application Note pr7

Accounting for Security Threats within Engineering Safety Management

Published on behalf of the International Railway Industry
by Technical Programme Delivery Ltd
Issue 1.2, January 2017

TPD

iESM

We are grateful to the organizations listed who have supported iESM in various ways:

TPD

MTR

UNDERGROUND London Underground

BOMBARDIER
the evolution of mobility

RICARDO Ricardo Rail

EC HARRIS
BUILT ASSET CONSULTANCY
AN ARCADIS COMPANY

TCT

RSSB

ARBUTUS
TECHNICAL CONSULTING

Liv Systems
Human Factors Specialists

Transport
Sydney Trains

機電工程署
EMSD

Electrical and Mechanical Services Department
The Government of the Hong Kong Special Administrative Region

RioTinto

arc

CROSSRAIL

RATP

MiW Rail Technology

SYSTRA
CONFIDENCE MOVES THE WORLD

CERTIFER
RAILWAY CERTIFICATION AGENCY

WSP | PARSONS BRINCKERHOFF

PROVISIONAL

Cover pictures © 2012 Paul Cheeseman

© Technical Programme Delivery Ltd 2017

Disclaimer

Technical Programme Delivery Limited (TPD) and the other organizations and individuals involved in preparing this handbook have taken trouble to make sure that the handbook is accurate and useful, but it is only a guide. We do not give any form of guarantee that following the guidance in this handbook will be enough to ensure safety. We will not be liable to pay compensation to anyone who uses this handbook.

Acknowledgements

This Application Note has been written with help from the people listed below.

- S Bickley
- M Castles
- P Cheeseman
- Dr Chen Roger Lei
- J-M Cloarec
- A Cross
- Dr R Davis
- B Elliott
- S Hughes
- Dr KM Leung
- Ng Nelson Wai Hung
- G Parris
- Sen Paul HB
- Mrs Shi Lisa
- A Russo
- M Turner
- Dr Fei Yan
- Dr Zhang Simon

These people worked for the organizations listed below.

- Abbot Risk Consulting
- Arbutus Technical Consulting
- Beijing Traffic Control Technology Company
- Bombardier Transportation
- Certifer
- EC Harris
- Electrical and Mechanical Services Department, Hong Kong
- Lloyd’s Register
- London Underground
- MTR Corporation Limited, Hong Kong
- Systra
- Technical Programme Delivery Group
- WSP | Parsons Brinkerhoff

This guidance does not necessarily represent the opinion of any of these people or organizations.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

Contents

PROVISIONAL

© Technical Programme Delivery Ltd 2017

1 Introduction

This Application Note (AN) is a component of the international Engineering Safety Management Good Practice Handbook, or 'iESM', for short. The handbook as a whole describes good practice in railway Engineering Safety Management (ESM) on projects. It covers both projects that build new railways and projects that change existing railways.

The iESM handbook is structured in three layers:

- Layer 1: Principles and process
- Layer 2: Methods, tools and techniques
- Layer 3: Specialized guidance

The first layer comprises one volume, Volume 1. Volume 1 describes some of the safety obligations on people involved in changing the railway or developing new railway products. It also describes a generic ESM process designed to help discharge these obligations.

Volume 2 provides guidance on implementing the generic ESM process presented in Volume 1 on projects. Volume 2 belongs in the second layer. At the time of writing, Volume 2 was the only document in the second layer but further volumes may be added to this layer later.

The third layer comprises a number of Application Notes providing guidance in specialized areas, guidance specific to geographical regions and case studies illustrating the practical application of the guidance in this handbook.

The structure of the handbook is illustrated in the figure on the right.

This document is provisional[1] Application Note pr7. It supports the main body of the iESM handbook by providing guidance on considering security threats and vulnerabilities as part of ESM.

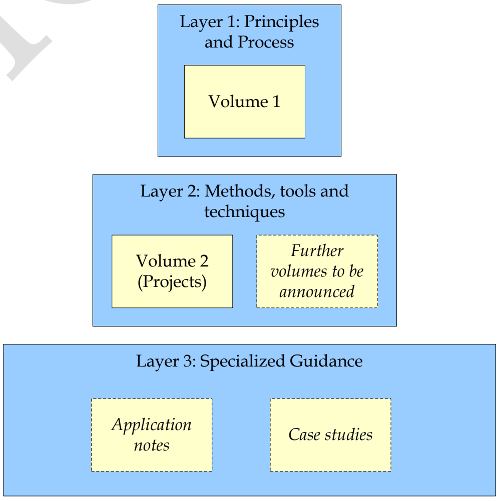
Layer 1: Principles and Process
Volume 1
Layer 2: Methods, tools and techniques
Volume 2 (Projects)
Further volumes to be announced
Layer 3: Specialized Guidance
Application notes
Case studies

Figure 1 The Structure of iESM Guidance

The role of iESM Application Notes is to develop more detail where required under the existing principles and guidance in iESM Volumes (layers) 1 and 2.

[1] This means that we actively encourage comment on and contribution to, the content of this AN and recognize that in this rapidly emerging field it may be not yet fully achieve our aim of promoting good practice.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

2 Background

It is a sad reality that there are individuals and organizations in the world who wish to deliberately harm people and infrastructure through attacks on transport networks. We must ensure that both safety risks and related security risks are appropriately mitigated to minimize the danger of harm, disruption, and economic loss, although iESM is concerned mainly with the first of these.

This AN describes the interface between the existing iESM guidance and what we call security engineering with reference to existing external guidance. The intention is to allow for a unified approach to safety (protecting people from the system) and security (protecting the system from people) but not to repeat guidance that is available elsewhere.

Security engineering is concerned with preventing harm to people[2] by identifying potential threats and vulnerabilities, then applying appropriate mitigations to demonstrably reduce the risk associated with the threat to an acceptable level. The motivation for accounting for security within ESM is that a system or product cannot be demonstrably safe if it is not secure.

Much guidance is online and links given were correct at the time of publication. If they cease working please let us know.

PROVISIONAL

[2] And other things too such as financial loss and loss of functionality but this AN is concerned with safety.

© Technical Programme Delivery Ltd 2017

3 Scope

3.1 Safety and Security

Safety and security are both emergent properties of a system or product. They are so interlinked that in some languages a single word is used for both. The iESM risk-based approach can be adapted to provide an effective framework for managing them together.

Accounting for security within iESM security covers three areas:

- **Cyber security** – to protect a system and its controlled processes against unauthorized access or attack e.g. malicious software or hacking.
- **Physical security** - to prevent a direct assault on assets and injuries that can be inflicted should an incident occur e.g. breaking into equipment and interfering with it.
- **Personnel security** - manage the risk of people exploiting legitimate access to assets for unauthorized purposes.

This AN does not address the last of these although it is important to note that cyber security attacks can start off by exploiting some kind of personnel vulnerability, e.g. free gift of an infected USB stick all the way through to blackmail, kidnap and violence. Nor does this AN cover other aspects commonly covered by business security measures such as continuity planning, establishing a security organization, developing a security strategy, financial or cash security or incident response except where these are intrinsically linked to the design and implementation decisions for an engineering system or product.

A lot of cyber security guidance is Information Technology (IT) centric and the main concern in the IT domain is often compliance with prevention of unauthorized access to data. This AN is more focused on preserving the dependability of the process under control, be it train movements, station environment or power supply. Secure management of data is part of this, but only part.

This AN does not relate to a single iESM principle but extends the consideration of Engineering Safety Management to include additional factors and requirements. An important difference between safety and security engineering is that, in security, one has an attacker. That makes it difficult to assess the risk of harm. A determined attacker may convert a very small vulnerability into an effective attack. On the other hand, there are counter-measures such as intelligence, surveillance and policing which do not appear in safety work.

The varied nature of security threats means that there is no single approach that is capable of addressing all the resultant risks. The rate of change of technology and the steady flow of serious vulnerabilities, means that any strategy needs to be kept under regular review

PROVISIONAL

© Technical Programme Delivery Ltd 2017

3.2 Cyber Security

Cyber security in railways is concerned with the technologies, processes and practices deployed to protect computer systems, networks and their operational processes from unauthorized access or attack. This includes the content of, and actions conducted through, digital networks. Protecting information, assets and processes and ensuring that they remain dependable in the face of misuse, should be at the heart of an organization's security planning.

Increasing use of networked Programmable Electronic Systems (PESs) for control and monitoring means railway systems are becoming vulnerable to cyber attack. This risk will increase with the move away from bespoke stand-alone systems to open-platform, standardized equipment built using Commercial Off The Shelf (COTS) components that can be accessed remotely via public and private networks. Whilst examples of wifi interference from passenger owned technology are known to have halted trains on metro railways, a bespoke system may have vulnerabilities and be quite easy to understand and attack, but the lack of access and relatively limited scope for disruption makes it an unattractive target.

Even some physical security measures can be dependent on IT systems and common networking protocols to support their operation. A door or gate lock remotely released from a central point or networked CCTV are vulnerable to attack even though the equipment itself is working correctly. Whilst centralization brings additional flexibility in deployment, the ability to use such centralized security control rooms for IT and physical security monitoring, will also expose users to risks that did not previously need to be considered.

3.3 Physical Security

Physical security measures are more familiar to us as they are visible deterrents or features designed to prevent or contain a security threat. Standards and good practice are better established and more obvious in this area.

Physical security measures aim to either prevent a direct assault on premises or reduce the potential damage and injuries that can be inflicted should an incident occur. For most organizations this will involve a sensible mix of good housekeeping alongside appropriate investments in CCTV, intruder alarms and lighting that deter as well as detect. These measures that will also protect against other criminal acts such as theft and vandalism and address general health and safety concerns.

Monitoring advances in technology and good practice, including good practice in other industries, becomes important even during the execution of a project.

In designing physical security arrangements the Guide to Producing Operational Requirements [OR] is suggested.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

4 Other Guidance

The effective management of security is a rapidly emerging field and standards and good practice are not always yet well established. Unlike system safety, the ability to share good practice is also limited by the need for secrecy of tools and techniques used to achieve the desired level of security. However the principle of following relevant standards and good practice, where it exists, forms the basis of this AN.

We recommend the guidance published by the UK Department of Transport available from RSSB on Cyber Security [RSSB] and therefore do not repeat it here.

Further guidance from the UK Department for Transport is specific to UK Light Rail security which includes material relevant to the scope of this AN [DFT]

The UK Centre for the Protection of National Infrastructure (CPNI) provides a different set of guidance on Good Practice Guide - Process Control & SCADA (Supervisory Control And Data Acquisition) Security [CPNI] which:

- Provides an overview of the necessity for process control and SCADA system security
- Highlights the differences between process control and SCADA system security and IT security
- Describes the key principles underlying the approach
- Identifies eight elements for addressing process control system security and for each, presents good practice principles.

CPNI also offer a SCADA Self Assessment Tool as do Industrial Control Systems Cyber Emergency Response Team (ICSCERT) with their Cyber Security Evaluation Tool in USA.

Other work has been performed as part of the European Union Secure-ED project which aimed to provide a set of tools to improve urban transport security. More information can be found here http://www.secur-ed.eu .

The security of engineering assets is also an implicit requirement of the CENELEC Standards for RAMS (EN50126) and software-based control systems (EN50128 / EN50129). The latest draft of EN50126 includes specifying a demonstration that misuse-based failures on external interfaces do not adversely impact on the safety integrity of the system. The emerging Part 5 also requires that the Software Technical Safety Report shall demonstrate that inputs via the external interfaces cannot bring the software to a hazardous state.

American Public Transport Association (APTA) has published recommended practice "Cyber Security Considerations for Public Transit Securing Control and Communications Systems in Rail Transit Environments" (Parts 1, 2 and 3A) available at http://www.apta.com/resources/standards/security/Pages/default.aspx

The National Institute of Standards and Technology (NIST) in USA publishes a series of NIST documents which are relevant:

PROVISIONAL

© Technical Programme Delivery Ltd 2017

- SP800-26 provides advice on how to manage IT security. This document emphasizes the importance of self assessments as well as risk assessments.
- SP800-30 “Guide for Conducting Risk Assessments”, supported by its application note SP800-37: "Guide for Applying the Risk Management Framework to Federal Information Systems" provide a risk assessment approach.
- SP800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", contains 194 security controls grouped into management, operational and technical / design that can be applied to a system to make it more secure. The security controls in this document have been incorporated into overlays of security control baselines in NIST SP800-82 Rev 2 (see below). This will make SP800-82 a more specific reference for interpreting the requirements of SP800-53.
- SP800-82 Guide to Industrial Control System (ICS) Security [NIST] provides a broad overview of computer security and control areas. It also emphasizes the importance of the security controls and ways to implement them. Initially this document was aimed at the federal government although most practices in this document can be applied more widely.

The US Centre of Strategic and International Studies (CSIS) have taken a subset (around a third) of the NIST 800-53 security control activities to focus on as the top twenty priority Critical Controls based on attacks occurring today and those anticipated in the near future. They are explained in detail here:

http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf

Recent guidance published by IET covers Cyber Security of Ports and Port Systems has some general material that could be relevant to railways, see

http://www.theiet.org/sectors/transport/topics/autonomous-vehicles/articles/cyber-security-ports.cfm

PROVISIONAL

© Technical Programme Delivery Ltd 2017

5 Project Definition

5.1 Defining the scope

Your organization must define the extent and context of any activity that it performs which affects security-related systems or products [iESM].

As when dealing with system safety it is important to capture, document and place under change control:

- The products or systems that exist or are proposed
- Their interfaces
- The nature of each system or product including:
    - where they are located
    - who the designated owner of each system is
    - who manages each system
    - who supports each system and how the systems interact
- Their business and safety criticalities
    -

5.2 Determining obligations, targets and objectives

Your organization must establish the obligations that are relevant to the security of its systems or products [iESM].

Your organization must define objectives and targets for security that are consistent with its obligations [iESM].

As with safety it is essential to identify in collaboration with your client and regulator which security guidance framework they expect to be used. This will vary by country and even by railway type. It may be that in the future regulators might require the demonstration of compliance with a particular framework.

5.3 Planning activities

Your organization must plan out a program of ESM activities that will deliver the security objectives and targets [iESM].

Your organization must carry out activities that affect security by following systematic processes that use recognized good practice. Your organization must write these processes down beforehand and review them regularly [iESM].

Like system safety, security cannot be bolted on at the end of a project. It must be considered as part of the lifecycle activities. You should design security requirements from the start of the design process and specify the security standards and good practice that shall be followed as part of the system or product specification.

A Security Management Plan may be produced or the System Safety Plan may be extended with additional material. These features are commonly captured in a Security Management Plan:

- What are the objectives

PROVISIONAL

© Technical Programme Delivery Ltd 2017

- What is to be protected
- Which are the critical components
- What is not covered by the policy
- What are the regulations to be complied with
- What are the criteria for risk assessment
- What is the risk appetite for the proposed activity
- What is required for approval before entry into service.
- Who is responsible for system security

The key elements of such a plan, linked to the EN 50126 lifecycle are shown in the table below:

iESM Principle	EN50126 Phase	Security-related activity
Definition	1: Concept	• Review current security policies and standards • Review current security vulnerabilities • Establish project security scope
	2: System Definition and application conditions	• Define security objectives • Define security constraints • Identify stakeholders • Consider security within preliminary hazard identification & risk analysis • Develop Security Management Plan
Risk Analysis	3: Risk Analysis	• Conduct risk assessment to understand threats, impacts, vulnerabilities & mitigations • Consider security within hazard identification • Include security risks within Hazard Log or any risk register or a specific Threat & Vulnerability Log
	4: System Requirements	• Specify System Security Requirements (SSRs) • Define acceptance criteria
Risk Control	5: Apportionment of system requirements	• Specify sub-system security requirements • Conduct sub-system risk assessment to understand threats, impacts, vulnerabilities & mitigations

PROVISIONAL

© Technical Programme Delivery Ltd 2017

iESM Principle	EN50126 Phase	Security-related activity
	6: Design and implementation	• Manage System Security Requirements • Justify any security-related design decisions • Prepare security inputs to Safety Case • Update Hazard Log / Threat & Vulnerability Log
	7: Manufacturing	• Update Hazard Log / Threat & Vulnerability Log
	8: Installation	• Implement System Security Requirements
	9: System validation	• Test security features • Monitor performance of security features during operational trials • Record any threats, breaches and security incidents in DRACAS • Prepare security inputs to Safety Case
	10: System Acceptance	• Review Hazard Log / Threat & Vulnerability Log • Review DRACAS
	11:Operation and maintenance	• Review adequacy of security features against new threats • Monitor performance of security features • Monitor arrangements for new or emerging threats and vulnerabilities
	12: Performance monitoring	• Analyse security features performance • Audit / test all polices, processes and procedures including supply chain
Re-apply iESM as appropriate	13: Modification and retrofit	• Assess system change impact on the security features
-	14: Decommissioning and disposal	• Consider security threats within decommissioning plan

PROVISIONAL

© Technical Programme Delivery Ltd 2017

6 Risk Analysis

6.1 Identifying threats and vulnerabilities

Your organization must make a systematic and vigorous attempt to identify all possible security threats and vulnerabilities related to its systems or products [iESM].

Your organization must assess the effect of its work on the overall risk on the railway [iESM].

It is important to note that we do not expect consideration of security threats and vulnerabilities to introduce new hazards at the boundary of the system. If the hazard identification is done thoroughly, all reasonably foreseeable situations that can lead to harm should be known. Consideration of security introduces additional ways that the hazards can occur and therefore needs additional mitigation measures to protect against them. This means that there is no hazard of the system under consideration relating to a security threat that cannot occur through failure, systematic error or other human action or inaction.

To ensure robust threat and vulnerability identification the following areas should be explicitly addressed throughout the lifecycle:

- Deliberate attack including viruses, malicious code installed on computers, worms or Trojan horse infections, denial of service
- Accidental attack through unintended infection with malicious software
- Accidental attack caused by the use of on-line hacking tools
- Accidental attack caused by unauthorised interrogation of systems
- Security breach through negligence or lack of knowledge
- Physical attack from munitions, rogue vehicles, chemicals, etc
- Perimeter and access control
- Lighting and intruder detection

PROVISIONAL

NIST SP800-30 “Guide for Conducting Risk Assessments” and NIST SP800-82 “Guide to Industrial Control System Security” [NIST] are recommended as useful help for threat and vulnerability identification.

The following points, supported by links to the CPNI website, can be used on projects to ensure coverage of most possibilities:

Cyber security:

- Threat intelligence - a diverse array of products and services, classed as Threat Intelligence, are available to assist organizations with planning their approach to security. See http://www.cpni.gov.uk/advice/cyber/Threat-Intelligence/
- The 20 Critical Security Controls – as mentioned in Section 4, See http://www.cpni.gov.uk/advice/cyber/Critical-controls/
- Mobile devices - covering laptops, USB storage, smartphones and tablets. See http://www.cpni.gov.uk/advice/cyber/mobile-devices/

© Technical Programme Delivery Ltd 2017

- Log file management - Log files are historical records of the running state of hardware and software, storing information on how they are used, errors that occur and application specific events which detail how users interact with them. The use of log files can raise reliable alarms with low error rates. Good management of log files is also key to successful post-incident investigations and will assist an organisation in determining the source of problems and weaknesses with existing protective security measures. See http://www.cpni.gov.uk/advice/cyber/Log-File-Management/
- On-line reconnaissance - information about organizations from online sources can be used to identify gaps in their security which may compromise their systems See http://www.cpni.gov.uk/advice/cyber/online-reconnaissance/
- Denial-of-Service (DoS) - involves a malicious attempt to disrupt the operation of a computer system or network that is connected to the Internet. The most common form of attack is one which disrupts the operation of the computer system or network by consuming the bandwidth of the victim network or overloading the computational resources of the victim system. See http://www.cpni.gov.uk/advice/cyber/DoS-and-DDoS/
- Password management – passwords are widely used to prevent unauthorised access to systems and/or material. See http://www.cpni.gov.uk/advice/cyber/password-advice/
- Spear fishing – is a type of cyber-attack used by a range of adversaries to steal information or cause disruption to an organisation's business. See http://www.cpni.gov.uk/advice/cyber/spear-phishing/
- SCADA - almost all critical industrial infrastructures and processes are managed remotely from central control rooms, using computers and communications networks. These all use various forms of SCADA technology. See http://www.cpni.gov.uk/advice/cyber/scada/

Physical Security:

- Chemical, Biological and Radioactive (CBR) - since the early 1990s, concern that terrorists might use CBR materials as weapons has increased steadily. See http://www.cpni.gov.uk/advice/Physical-security/CBR-Attacks
- CCTV - should form only part of a whole security system; it should not be used on its own. It cannot replace security staff, although it may permit a reduction in their number or their redeployment to other security activities. Importantly it only has value if someone is empowered and equipped to take appropriate action based on what the CCTV shows. See http://www.cpni.gov.uk/advice/Physical-security/CCTV
- Explosives and ballistics protection - most terrorist bombs are improvised and so are known as Improvised Explosive Devices (IEDs). If you believe your project might become the target of a bomb attack, you should assess the threat and potential damage and plan how to prevent or mitigate it. See http://www.cpni.gov.uk/advice/Physical-security/ebp
- Hostile Vehicle Mitigation (HVM) - vehicle-borne threats range from vandalism to sophisticated or aggressive attacks by determined criminals or terrorists. The mobility and payload capacity of a vehicle offers a convenient

PROVISIONAL

© Technical Programme Delivery Ltd 2017

delivery mechanism for a larger explosive device. See http://www.cpni.gov.uk/advice/Physical-security/Vehicle-borne/

- Lighting and obscuration - lighting can be an important security measure, but may in fact assist an intruder if used incorrectly. See http://www.cpni.gov.uk/advice/Physical-security/Lighting
- Perimeters and access control - keep access points to a minimum and make sure the boundary between public and private areas of your building is secure and clearly signed. Invest in good quality access controls such as magnetic swipe identification cards or 'proximity' cards which are readable from only a short distance. See http://www.cpni.gov.uk/advice/Physical-security/Perimeters
- Secure destruction of sensitive items -destruction of sensitive items should be undertaken via a secure process. See http://www.cpni.gov.uk/advice/Physical-security/secure-destruction-of-sensitive-items
- Search and screening – explosives and weapons detection through search and screening measures to detect specific items and materials entering (or leaving) buildings and sites. Effective search and screening measures may additionally have a significant deterrent effect. See http://www.cpni.gov.uk/advice/Physical-security/Screening

As part of threat identification we suggest also recording any impacts identified (the equivalent of iESM consequences) which may include:

- Harm
- Loss of reputation
- Violation of regulatory requirements (e.g. health and safety, environmental),
- Inability to meet business commitments
- Financial losses
- Non-safety impacts.

PROVISIONAL

6.2 Estimating risk

Understanding the vulnerabilities is akin to estimating the safety risk. A vulnerability assessment of the system or product will help to focus effort where it is most needed. Such a review should include evaluation of the:

- Infrastructure
- Operating systems
- Applications
- Component software
- Network connections
- Remote access connectivity and processes and procedures
- The supply chain arrangements during manufacture, deployment and operation.

© Technical Programme Delivery Ltd 2017

Typical vulnerabilities in a software system include:

- Insufficient validation or bounds checking on input data
- Allowing input data to be executed or interrupted
- Weak authentication (e.g. default passwords)
- User-friendly failures like "Autorun"

Note, where products or systems are critical elements of the supply of other key services, impacts may not be contained within the business but could have serious and potentially life threatening consequences elsewhere e.g. a railway station that also has substantial shopping or car parking facilities.

Experience to date shows that safety risk assessments can be quantitative if necessary but that security risk assessments tend to be qualitative.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

7 Risk Control

7.1 Evaluating risk, implementing and validating control measures

Your organization must evaluate the risk associated with each of its systems or products against the criteria for security that it is obliged to use. If the risk associated with a system or product cannot be reduced to an acceptable level, then it must be abandoned [iESM].

Your organization must design its systems or products to meet its security requirements and all control measures must be implemented [iESM].

7.1.1 Secure architectures

ISA/IEC-62443 [62443] is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to asset owners, system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

IEC 62443-3-3 2013 identifies Security Levels akin to System Integrity Levels. These can inform architecture decisions and allow validation of design decisions. They represent a measure of confidence that the ICS/IACS is free from vulnerabilities and functions in the intended manner:

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

CPNI guidance identifies three guiding principles [CPNI] which are "Protect, Detect and Respond". Addressing security threats and vulnerabilities is not just a matter of deploying protection measures. It is important to be able to detect possible attacks and respond in an appropriate manner in order to minimize the impact.

- **Protect -** deploying specific protection measures to prevent and discourage electronic attack against the process control systems.
- **Detect -** establishing mechanisms for rapidly identifying actual or suspected attacks.
- **Respond -** undertaking appropriate action in response to confirmed security incidents against the process control systems.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

Where a single protection measure has been deployed to protect a system, there is a risk that if a weakness in that measure is identified and exploited there is effectively no protection provided – the equivalent of a safety single point failure. No single security measure itself is foolproof as vulnerabilities and weaknesses could be identified at any point in time. In order to reduce these risks, implementing multiple protection measures in series avoids single points of failure.

In order to safeguard the system or product from electronic attacks (e.g. hackers, worms and viruses), it may be insufficient to rely on a single firewall, designed to protect the corporate IT network. A much more effective security model is to build on the benefits of the corporate firewall with an additional dedicated firewall and deploy other protection measures such as anti-virus software and intrusion detection. ISO/IEC 27002 [ISO27002] provides good practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems.

When implementing security there is a natural tendency to focus the majority of effort on the technology elements. Although important, technology is insufficient on its own to provide robust protection. For example, when implementing a firewall it is not just a matter of installation and configuration, consideration must also be given to associated procedural and managerial requirements:

- Procedural requirements may include change control and firewall monitoring
- Managerial requirements may include firewall assurance, standards, assurance and training.

The CPNI Guidance [CPNI] gives good practice design principles for possible security measures that may be used to form a secure architecture.

7.1.2 Open and closed transmission systems

Within the context of security EN50159 [50159] defines two types of transmission systems:

> **Closed Transmission Systems -** systems with fixed number or fixed maximum number of participants linked by a transmission system with well known and fixed properties, and where the risk of the unauthorised access is considered negligible.
>
> **Open Transmission Systems -** systems with unknown number of participants, having unknown, variable and non-trusted properties, used for telecommunication services and for which the risk of unauthorised access shall be assessed.

Railway control systems were traditionally closed systems designed for functionality, safety and reliability where the prime concern was one of physical security. Increased connectivity via standard IT technologies has exposed them to new threats and vulnerabilities (for example, worms, viruses and hackers but also new weapons or identified weaknesses in existing security measures). As these

PROVISIONAL

© Technical Programme Delivery Ltd 2017

process control networks continue to increase in numbers, expand and connect, so the risks to the process control systems from electronic threats continue to escalate. EN 50159 [50159] gives detailed guidance on design requirements for both types of systems.

There can be some confusion as to whether a transmission system is closed or open, for example provision of a firewall does not turn an open system into a closed one. Similarly the provision of condition monitoring facilities through for example a serial port can also allow the upload of data or viruses directly into the product.

7.1.3 Secure by design

There are eight design principles promulgated by Saltzer and Schroeder:

- Economy of mechanism - keep the design as simple as possible
- Fail-safe defaults - base access decisions on permission rather than exclusion
- Complete mediation: every access to every object must be checked for authority
- Open design - the design for widely distributed systems should not be secret but instead protected by keys that should still be secret and be able to be changed easily
- Separation of privilege - two keys are better than one
- Least privilege - every program and every user of the system should operate using the least set of privileges necessary
- Least common mechanism - minimize the amount of mechanism common to more than one user and depended on by all
- Psychological acceptability - design for ease of use

These principles should be read in conjunction with the authors' paper at http://www.cs.virginia.edu/~evans/cs551/saltzer/

Insecure design might include features such as the ability to upload code to a system without it being digitally signed. Another might be a message protocol with no authentication or authorization components, or where defined field and message lengths are not validated via a message parser.

PROVISIONAL

7.2 Setting security requirements

Your organization must set security requirements which are sufficient to meet its safety obligations and targets [iESM].

In this case we will identify System Security Requirements (SSRs) or countermeasures as the equivalent of a Safety Requirement. There are many different types but they will address the threats and vulnerabilities we have identified by:

- Avoiding the threat
- Implementing design decisions to manage the vulnerabilities

© Technical Programme Delivery Ltd 2017

- Applying appropriate controls or mitigations including post event
- Transferring the threat to someone else
- Knowingly and objectively accepting the threat or vulnerability.

The SSRs may consist of a combination of:

- Deterrence
- Avoidance
- Prevention
- Detection
- Recovery
- Correction.

The table below shows examples of typical SSRs.

Requirement	SSR	Implementation
Protect from Unauthorized User Access	The System shall grant access to Users through a single User authentication process.	Authentication of a unique user identity and password. User's functional scope and privileges are made available on successful completion of the authentication process.
Protect from remote malicious access	The System shall be protected against unauthorized and mal-intended access. Protection to cover all applications, servers, networks including air gap interfaces, gateways and all other appropriate devices and links.	Protected electronically by: - Firewalls - Virus checking
Protect from Unauthorized Access	The System shall be protected such that neither hardware nor any other physical content can be accessed or tampered with by unauthorized persons, devices or materials.	Control Centre and trackside equipment rooms physically protected and alarmed against unauthorized access. Alarms annunciated to the control Centre and /or to an appropriate person at the site.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

Requirement	SSR	Implementation
Ensure secure communication paths	Any electronic communication paths used for operation or maintenance purposes shall be secure.	Remote transmission of data, particularly control information must not be accessible to outside parties.
Mitigation and recovery	Measures shall be defined to reduce impact and aid recovery	Incident response plans. Communication plans to reassure and inform stakeholders. Disaster recovery and business continuity plans which are able to afford the same level of security as the processes and systems in use on a day-to-day basis.

PROVISIONAL

7.3 Compiling evidence of safety

Your organization must demonstrate that risk has been controlled to an acceptable level. Your organization must support this demonstration with objective evidence, including evidence that all safety requirements have been met [iESM].

Claims about safety must be informed by security considerations. Security and safety are different but interrelated concepts. Security is related to deliberate and malicious acts. Safety is related to accidents, including those caused by lack of competence or negligence. A "Security-informed" Safety Case would show that security threats and vulnerabilities have been properly considered during the project lifecycle. Further information on this can be found in DfT Code of Practice for Cyber Security Informed Safety Cases for the Rail Industry [FNC]

It has rightly been said that if a system or product is not secure then it cannot be demonstrably safe. The "Security informed" Safety Case shall justify, where relevant, the:

- Technical choice of any cryptographic techniques
- Technical choice of cryptographic architectures
- Supporting dependencies (e.g. storage, distribution, revocation of keys)
- Choice of physical security measures
- Supporting dependencies on maintenance, inspection and testing
- Threat monitoring arrangements.

The presentation of evidence of security may take several forms, for example:

© Technical Programme Delivery Ltd 2017

- Statements from Subject Matter Experts on generic product or applied product security.
- Claims arguments and evidence showing "it is acceptably secure" or "the safety functions are acceptably secure"
- Goal Structuring Notation approach to "it is acceptably secure" or "the safety functions are acceptably secure".

Security "decays" faster than safety. The Safety Case must allow for reasonably foreseeable changes to the environment, not just changes to the system or product. Ideally such changes would not violate the Safety Case, but in some cases it may be necessary to repeat some iESM activities and update the Safety Case to reflect the new or modified properties of the system. It is good practice for the system definition in the Safety Case to encompass a process for applying patches, without the need to revise the Safety Case or at least without the need to obtain further approval.

PROVISIONAL

7.4 Obtaining approval

Your organization must obtain all necessary approvals before placing a system or product into service [iESM].

No additional guidance is offered apart from noting that in the event of a security threat requiring a change to a system or product, it may be necessary to approve a system or product change rapidly and processes need to facilitate this.

7.5 Monitoring risk

Your organization must take all reasonable steps to monitor and improve the management of risk. Your organization must identify, collect and analyze data that could be used to improve the management of risk, as long as it is has responsibilities for safety [iESM].

Your organization must take action where new information shows that this is necessary [iESM].

Any changes to parameters (e.g. system modification) could change the security risk. Consequently, an ongoing risk management process is required to identify any of these changes, re-evaluate the risk and initiate appropriate security improvements.

As with safety, there is an obligation to identify and control new security threats and vulnerabilities. Unlike safety, emergent security threats can arise suddenly through previously unknown vulnerabilities or attackers, changes in attractiveness of targets or change in capability of an attacker. It is probable that external factors will be the most likely change detected.

There is guidance in ISO/IEC27001 [27001] on measuring and evaluating how well an organization's Information Security Management System (ISMS) is performing and also requirements for establishing, implementing, maintaining and continuously improving that system.

© Technical Programme Delivery Ltd 2017

8 Technical Support & Team Support

These groups of iESM supporting processes apply as described in Volumes 1 and 2 of the Guidance.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

9 Glossary

Terminology can be a problem in considering the effects of security on safety. In this AN we introduce some additional definitions[3].

Compromise

The equivalent of an error within a system or product. Under certain conditions that error could lead to a hazard. It can be considered as a cause of that hazard.

Engineering Safety Management (ESM)

The activities involved in making a system or product safe and showing that it is safe.

Note: despite the name, ESM is not performed by engineers alone and is applicable to changes that involve more than just engineering.

Hazard

A condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product definition and exists at its boundary.

Impact

The consequences of a threat taking place.

Likelihood

The probability of a specified outcome.

Project

The planned change to the railway or development of a new product, system or process.

Risk

Possibility of an event occurring that will have a negative impact on the system or product. The event may be the result of one threat or a combination of threats.

Risk appetite

The level of risk, used to determine what an acceptable risk is.

Security

The state of being free from danger or threat.

System

A set of elements which interact according to a design, where an element of a system can be another system, called a subsystem and may include hardware, software and human interaction.

System lifecycle

A sequence of phases through which a system can be considered to pass. A product may also pass through some of these phases.

PROVISIONAL

[3] CPNI (Centre for the Protection of National Infrastructure) definitions in relation to assessing business security risks are in **bold**

© Technical Programme Delivery Ltd 2017

Threat

Any external circumstance or event with the potential to deliberately or accidently exploit a vulnerability in system or product through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Vulnerability

An emergent property of a system or product that reflects the degree to which it is open to unauthorized access, change, or disclosure of information and is susceptible to interference or disruption of system services.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

10 Referenced Documents

This section provides full references to the documents referred to in the body of this document.

[CPNI] Security for Industrial Control Systems Framework Overview a Good Practice Guide http://www.cpni.gov.uk/Documents/Publications/2015/12-May-2015-SICS%20-%20Framework%20Overview%20Final%20v1%202.pdf

[DFT] Light Rail Security Recommended Best Practice https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316816/light-rail-security-best-practice.pdf

[FNC] Code of Practice for Cyber Security Informed Safety Cases for the Rail Industry https://www.fnc.co.uk/media/284816/Code-of-Practice-Cyber-Security-Safety-Cases-web-version-.pdf

[NIST] Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, National Institute of Standards and Technology, US Department of Commerce http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[OR] Guide To Producing Operational Requirements For Security Measures, February 2010, CPNR http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf?epslanguage=en-gb

[RSSB] Rail Cyber Security, Department for Transport http://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf

[27001] Information Security Management System requirements, ISO/IEC 27001:2013 (formerly ISO/IEC 17799 or BS 7799 Part 2)

[27002] Code of Practice for Information Security Controls, ISO/IEC 27002:2013 (formerly known as ISO/IEC 17799 or BS 7799 Part 1)

[50126] EN 50126, Railway applications – The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS). Also issued as IEC62278.

At the time of writing the current issue of EN 50126 was dated 1999 but the standard was being revised to cover the scope of EN 50128 and EN 50129 and other railway systems. As far as we can, we have aligned this guidance with the emerging issue. If an issue of EN 50126 dated later than 1999 is available at the time of reading then this issue should be consulted. If no issue of EN 50126 dated later than 1999 is available then the reader may find it useful to consult the current issues of EN 50126 and EN 50129 but may not find the information referred to in any particular citation of the standard.

PROVISIONAL

© Technical Programme Delivery Ltd 2017

[50159] EN50159:2010 Railway applications, Communication, signalling and processing systems, Safety-related communication in transmission systems

[62443] ISA/IEC 62443:2010 Security Technologies for Manufacturing and Control Systems (formerly issued as ISA99:2007)

PROVISIONAL

© Technical Programme Delivery Ltd 2017

international Engineering Safety Management

Good Practice Guidance
Application Note pr7

Published on behalf of the International Railway Industry
by Technical Programme Delivery Ltd