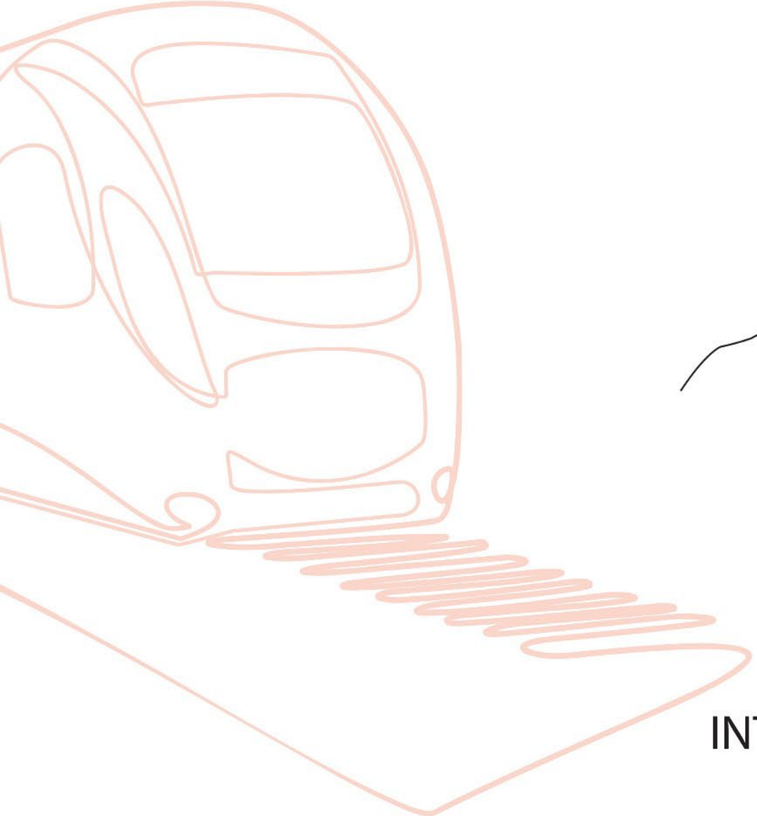


IRSc
INTERNATIONAL RAIL SAFETY COUNCIL
SOUTH AFRICA

ORR
OFFICE OF
RAIL AND ROAD

IRSC 2023

INTERNATIONAL RAILWAY SAFETY COUNCIL

"Reshaping Railways in an Uncertain World"

CAPE TOWN, OCTOBER 1 - 6, 2023

HOSTED BY RSR RAILWAY SAFETY REGULATOR
RAIL SAFETY ON THE RIGHT TRACK

James Walker
Office of Rail and Road

Health and Safety Regulation and the Cyber Security & Software Challenge

IRSC
INTERNATIONAL RAIL SAFETY COUNCIL
SOUTH AFRICA

HOSTED BY RSR RAILWAY SAFETY REGULATOR
RAIL SAFETY ON THE RIGHT TRACK

ORR
OFFICE OF RAIL AND ROAD

Contents

- ORR and Cyber Security
- IET Code of Practice
- Question set development and trial
- Future work

ORR & Cyber Security

- ORR's job is to regulate Health and Safety
- Achieved through preventative inspections, investigation of accidents and enforcement
- Expect duty holders to manage the health and safety risks arising from software and cyber security failures E.g. Overcrowding; disruption; signalling failures; etc.
- Software design, operation, maintenance and cyber security risk should be managed in the same way as any other risk. It should form part of their **Safety Management System**
- ORR is **NOT** responsible for advising & enforcing the Network & Information Systems Regulations 2018 around cyber security, which implement the requirements of EU Directive 2016/1148.

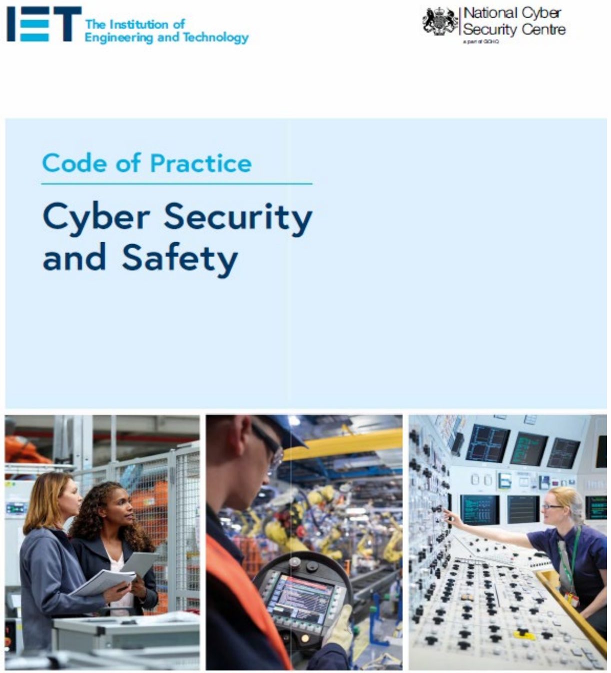
Building Capability

- Originated from the IET Code of Practice – Cyber Security and Safety

- Focused on developing Inspectors understanding of cyber security and digital software to test dutyholder arrangements

- Link to RM^3 to feed into dutyholder maturity assessment

- Trial did not involve RM^3 assessment



IET The Institution of Engineering and Technology

National Cyber Security Centre
a part of GCHQ

Code of Practice

Cyber Security and Safety

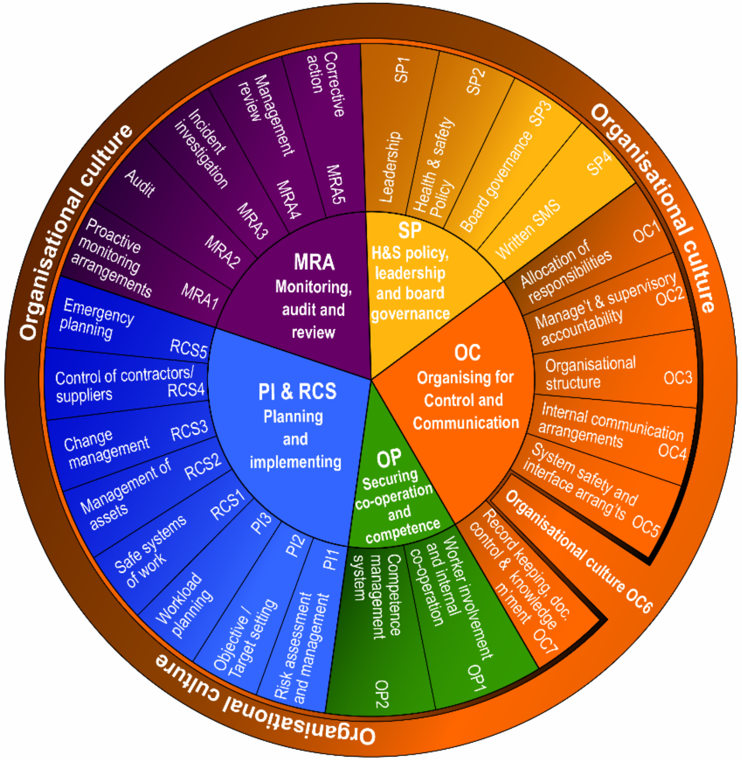
RM^3

- Safety regulatory framework based on the Safety Management System

- Five themes for excellence in Health & Safety Management Systems

- ORR's Risk Management Maturity Model, criteria around 26 Plan, Do, Check, Act elements:
  1. Ad hoc
  2. Managed
  3. Standardised
  4. Predictable
  5. Excellence

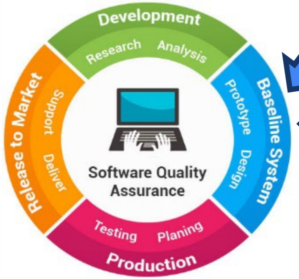
- Legal obligation to ensure continuous improvement of SMS and management maturity



Organisational culture
SP H&S policy, leadership and board governance
SP1 Leadership
SP2 Health & safety Policy
SP3 Board governance
SP4 Written SMS
OC Organising for Control and Communication
OC1 Allocation of responsibilities
OC2 Manage't & supervisory accountability
OC3 Organisational structure
OC4 Internal communication arrangements
OC5 System safety and interface arrang'ts
Organisational culture OC6
OC7 Record keeping, doc. control & knowledge m'ment
OP Securing co-operation and competence
OP1 Worker involvement and internal co-operation
OP2 Competence management system
PI & RCS Planning and implementing
PI1 Risk assessment and management
PI2 Objective / Target setting
PI3 Workload planning
RCS1 Safe systems of work
RCS2 Management of assets
RCS3 Change management
RCS4 Control of contractors/ suppliers
RCS5 Emergency planning
MRA Monitoring, audit and review
MRA1 Proactive monitoring arrangements
MRA2 Audit
MRA3 Incident investigation
MRA4 Management review
MRA5 Corrective action

The Safety, Software and Cyber Security Triangle

Safety



Software Assurance: Critical process in software development that ensures the reliability, safety, and security of software products

Cyber Security

Core function is to protect the devices we all use and the services we access - both online and at work - from theft or damage.

Why and how have ORR addressed the challenge?

- We have seen several software-based systems fail in recent years e.g., Cambrian Line; Class 700; other new train failures

- We recognise that our capability in these areas needed to be improved, so we engaged a contractor to:
    - Provide fundamental software assurance and cyber security training
    - Build a tool to help inspectors
    - Train some of our inspectors to use the tool
    - Carried out an inspection to trial the tool
    - Have taken learning to improve training and question set application

Training

- Focused on developing a sufficient understanding of cyber security and digital software

- Introduction into fundamentals including:
  - Software assurance
  - Malware
  - Patching
  - Supply chain risks
  - V-lifecycle and importance of each stage

Inspection – topic areas

- Leadership, Governance and Safety Management System
- System Safety (Safety and Security) and Interfaces
- Risk Assessment
- System architecture – IT & OT
- Supply chain
- Competence

Inspection Tool

- 63 questions covering all elements of Plan, Do, Check, Act cycle
- Provides inspectors with examples of good practice and areas for improvement to inform decision making
- Covers all core RM^3 themes
- Shaping ORR approach to determine baseline maturity
- Identify good and bad practice

Example question – supply chain

- **Overarching Principle:** The organisation manages its supply chain to support the assurance of safety and security in accordance with its overarching safety/security strategy?

  - How does the organisation assess the relationship it needs with its suppliers to meet obligations to provide cyber security services (e.g. patching, incident response support) for the lifetime of their product and services

👍

- The CSMS and SMS explain how the organisations approach to complementary cyber security and safety extends to the supply chain.

👎

- There is no documentary evidence that describes the role of suppliers in a complementary approach to safety and security, particularly for safety related software based digital technology

Duty holder feedback

- Work in progress
  - Some questions felt out of place
  - Work in progress – questions set will work differently based on DH maturity
- Generally, a strong narrative, and an effective link between questions and assumed objective
- High value in having common representation in both parts of audit
- Very positive experience

Future challenges

- Security is not just about good cyber security processes, but significantly linked to strategic enablers:
  - Leadership and management
  - Culture
  - Competence Management
- Supply chain management – how far do you go!
- Change management – particularly software assurance
- Update of inspection tool based on inspection feedback

IRSC
INTERNATIONAL RAIL SAFETY COUNCIL
SOUTH AFRICA

HOSTED BY

RSR RAILWAY SAFETY REGULATOR
RAIL SAFETY ON THE RIGHT TRACK

ORR
OFFICE OF RAIL AND ROAD

www.irsc2023.com