
Cybersecurity

Sarabjit Purewal

Head of Operations

BSc ACGI PGDip CEng MIET

What we will cover

- Why cybersecurity is an issue
- How cyber threats can impact on safety of people and harm the environment-links to MAH
- The current H&S Regulations in MH and how they are applied.
- CNI industries regulated by HSE
- CA operational guide for MH sector
- Next steps

Why cybersecurity is an issue

- Functional safety and independent layers of protection concepts.
- Common cause failures are by far the main cause of accidents in the MH industries.
- Inadequate functional safety management systems, and competency of staff are the two most common causes of failure leading to accidents.

Why cybersecurity is an issue

- Nearly all new control and safety instrumented systems are programmable
- Open standardised protocols allowing interconnectivity between different systems
- Increasing interconnectivity between Operational Technology (OT) e.g. control/protection systems, Information Technology (IT), and Internet
- Control and protection being merged into the same system
- Cyber security is another potential common cause of failure

Why cybersecurity is an issue

- Multiple failings can result. A dangerous state and failure to protect against it can occur at the same time.
- Layers of independent protection no longer a valid assumption.

Links to MAHs

- If a threat (deliberate or accidental) occurs it can lead to:
 - Mal-operation of a control system leading to an unsafe state- an initiating event
 - Mal-operation of a safety system such that it does not operate- protection layers fail
 - Both can occur at the same time
 - Common cause failure
- Both the above will lead to:
 - Increased risk of a MAH
 - An actual incident

CNI Industries regulated by HSE



- Electrical supply and distribution
- Oil production, refining, storage and distribution
- Gas (incl. LNG) production, refining, storage and distribution
- Water treatment

Relevant H&S Regulations

- Control of Major Accident Hazards Regulations (COMAH) 2015
- The Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations 2015
- Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995
- Specified Animals Pathogens Order (SAPO)
- Pipelines Safety Regulations 1996
- Gas Safety (Management) Regulations 1996

Approach to Regulation

- Means of compliance with the law- goal setting not prescriptive
- Standards and guidance is not the law- may be one means of complying with the law
- Duty holder obligation to demonstrate ALARP.

Guidance applicable to process sector



- Very good guidance is available, but it can be overwhelming, and it's not all limited to safety and environmental risks.
 - ISA-TR84.00.09-2013- Security Countermeasures Related to Safety Instrumented Systems (SIS).
 - The Centre for the Protection of National Infrastructure (CPNI) – Security for Industrial Control Systems.
 - <http://www.cpni.gov.uk/advice/cyber/Security-for-Industrial-Control-Systems/>

What guidance is out there

- NIST Publication 800-82 – Guide to Industrial Control Systems (ICS) Security

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

- 10 steps to Cyber security available via link
http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/Relaunch-10-Steps-to-Cyber-Security.aspx
- EEMUA Information sheet 2. Cyber security assessment process for industrial control systems

Standards for process sector

- Functional safety. IEC 61511 Ed 2 has specific requirements for cybersecurity threats. This is the benchmark Standard HSE uses for safety instrumented systems.
- Security standards developing
- BS EN 62443. Note this is not limited to functional safety.
 - Part 1: Framework and threat-risk analysis
 - Part 2: Security assurance
 - Part 3: Security requirements
 - Part 4 Relevant to system integrators.

HSE Operational guidance (OG)



- Why is this needed
 - It provides for proportionate risk reduction and one means to demonstrate ALARP
 - For specialist HSE C&I specialist inspectors
 - It is targeted at MH regulated industries and one means of compliance with the requirements of IEC 61511 Ed 2.
 - It is specific to relevant regulations covering safety and the environment
 - Consistent with the wider available guidance

Current status of HSE OG

- Published on HSE website in March 2017
- Consultation with industry, trade bodies, institutions, other Government departments and other interested parties
- Plan to run pilots and apply the guide at selected establishments across the sector.

Risk level

- We know many systems are vulnerable but don't know the extent of those vulnerabilities
- The extent of the threat level is being developed by the national cybersecurity centre which will inform risk assessment.
- The pilots will inform whether the extent of controls and systems are adequate

Next Steps

- Key issues for CA/HSE are:
 - To raise awareness of Industry so they start to address the issues.
 - *Ensuring staff is competent and become an intelligent customer*
 - *Develop adequate safety management systems that address cyber risks*
 - Assess current installed systems and identify gaps
 - Put programmes in place to close those gaps.

Thank You Questions