
HSE Operational Guidance
Cyber Security for Industrial Automation and Control
Systems (IACS)

Gill Smart

Policy Advisor

Chemicals & Land Use Planning Team

HSE's role

- HSE is the UK independent regulator for workplace Health and Safety
- HSE sets the strategy, policy and legal framework for health and safety in Great Britain
- HSE provide targeted advice, information and guidance to help duty holders comply with health and safety law in a sensible and proportionate way
- HSE encourage broader ownership of health and safety by involving all those who have an interest

Background to HSE Guidance

- International Standards for analysing cyber risk and to specify the design, installation, inspection, maintenance and testing of cyber security countermeasures were being developed
- Practical guidance was developed for HSE's Inspectors in the field – HSE Operational Guidance note 86
- Guidance is publicly available – Operators are free to use it
- Operators do not need to follow the guidance to be able to comply with the law

What does it contain?

A flow chart covering process management for IACS:

- Recognising the Need to Manage Cyber Security Risk
- Defining IACS scope
- Risk assessment
- Control measures
- Security measures
- Audit, monitoring and review
- Change management

What does it contain?

Each step in the flow chart has further guidance under the following headings:

- Purpose
- Background
- Approach
- Output

Providing a step by step approach for Inspectors – ensuring clarity and consistency in Inspection

Trial Inspections

In order to test the suitability and robustness of the guidance trial inspections were conducted.

The Operators involved in the trial:

- Participated voluntarily
- Were all major hazards Operators,
- Covered a range of industry sectors
- Covered large and small Operators and a range of IACS technologies (old and new)

Findings

The trial found that:

- Insufficient time had been allowed for Inspections
- There were overlaps in some areas (e.g. Human factors)
- The guidance needed to be aligned with requirements under the Security of Network & Information Systems Regulations (NIS Regulations)

Next steps

- HSE worked with operators, industry groups and other Governments departments on the findings
- A revised OG86 was published to take account of the trial findings, and Operator feedback
- A further revision is currently in development

Any questions?