Cyber Security Trial Inspections Summary Report

Executive Summary

The trial covered a range of industry groups, large and small COMAH Operators and a range of IACS technologies including new and old installations, control and safety systems and electrical power systems. A few of the Operators were also covered by NIS Regulations when they came into effect later in May 2018.

The Operators were a self-selecting volunteer group, and thus it was expected that the findings were likely to be optimistic compared to the sector as a whole. However, these Operators had systems in place and were addressing cybersecurity which allowed the OG 86 to be tested comprehensively. It is expected that with the findings of this trial and the outcomes from the 2018-19 inspection programme, a more detailed picture of the sector will emerge.

The findings of the trial are presented using the NCSC cybersecurity principles using a RAG (red, amber, green) rating for partial compliance and full compliance for each of the principles. The partial compliance was included to recognise that Operators may have started to address the issues but had not yet fully completed the work.

The findings show some encouraging signs that Operators had started to address the issues and were keen to know how to address the risks to their commercial operations proportionately to the level of risk and to demonstrate compliance.

The key findings show there are large gaps to close to reach full compliance and manage the risks to ALARP. However, progress was being made by all the Operators and the report shows areas of partial compliance.

Whilst progress was made on system type security issues which covered technical controls, there was less progress on other areas. These related to management systems including, procedural controls, governance, competency, detection and recovery, and supply chain issues.

There was some evidence in the newer systems that security through design was being built into the systems. However, this was not consistent. This is an area that needs to be addressed by the vendors and suppliers of systems.

There were also learning points for HSE which included, allowing sufficient time for the inspections, building in cybersecurity specific HF issues, and incorporating NCSC guidance into the HSE OG so that there is a single source of authoritative guidance for the sector.

It is recommended that industry addresses this risk at Board level and ensure that management systems are put into place that address governance, roles and responsibilities, procedural controls appropriate to cyber security, and competency of staff. Operators should become familiar and trained in cybersecurity and assessing risk so that they can act as the intelligent customer. This will allow significant progress to be made on quick wins as well as the more detailed technical controls that may be necessary and manage the risk on an ongoing basis.

HSE can support the above by working in partnership with industry and providing proportionate targeted guidance on how to assess and manage the risk and how compliance may be demonstrated. There is perceived to be a gap in appropriate training and HSE can fill this gap.

It is likely that it will take many years before the sector as a whole is managing the risks appropriately both for their commercial risk and to demonstrate compliance with the regulations.

Table of Contents

Background and Approach

Background

HSE published its operational guidance OG86 'Cyber Security for Industrial Automation and Control Systems (IACS)' in March 2017. Operational guidance is primarily aimed at HSE inspectors, providing them with guidance on the standards expected to facilitate a consistent approach to regulation. However, the OG is also freely available to COMAH operators, providing useful guidance on how compliance might be achieved.

In order to test the OG, the inspection approach and also get an early sense of where various industry sectors were compared to the OG, a series of trial inspections were carried out between November 2017 and May 2018.

Trial Inspection Approach

The Operators involved in the trial:

- Participated voluntarily
- Were all major hazards Operators, covered by COMAH or SAPO
- Covered a range of industry sectors including chemical manufacture, refining, fuel pipeline, gas terminal, industrial gases, microbiological (an explosives sector operator was initially involved put dropped out of the trial)
- Covered large and small COMAH Operators and a range of IACS technologies including new and old installations, control and safety systems and electrical power systems
- Included some Operators that would be covered by the (then proposed) NIS Regulations – although it should be noted that the scope of the trial inspections did not consider risks to essential services.

For each trial inspection the Operator was:

- Issued an agenda at least one month before the inspection (see example in appendix A)
- Requested to provide information to HSE about their cyber security management system, cyber security risk assessment and cyber security assets on site which was reviewed ahead of the inspection.
- Visited for a single day inspection (2 days for larger sites).
- Provided with a report of the outcomes of the inspection.

Two HSE Specialist Inspectors were involved with each trial inspection – one leading (focussed on the inspection itself) and one assisting and considering wider issues (e.g. inspection agenda, OG, etc.). Other HSE personnel and others (e.g. NCSC) also attended to observe the inspection process or for training purposes. It was noted that Operators sometimes also brought in wider audiences from their organisation who were interested in HSE expectations.

The trial inspections only considered MAH safety risk. There was no consideration of critical national infrastructure issues (i.e. loss of essential services).

However, during the trial period the NCSC issued its NIS principles and guidance and therefore the trial inspection agenda and inspection reports were gradually changed to align with the headings and content of the NIS principles and guidance. This change did not result in any significant change of the OG requirements.

Summary of levels of compliance

The level of compliance against the OG are summarised below, aligned to the NCSC NIS Principles.

Each of the NIS principles has been summarised as either: red, amber or green based upon the number of operators that had partly (i.e. started to address) or fully achieved the objectives as follows:

PART (P)	FULL (F)
Most Operators had started to address / partially achieved most objectives (≥6/8)	Most Operators had achieved most objectives (≥6/8)
Some Operators had started to address / partially achieved some objectives	Some Operators had achieved some objectives
Most Operators had not started to address / achieved most of the objective (≤2/8)	Most Operators had not achieved most of the objective (≤2/8)

A more detailed breakdown is provided in appendix B where each individual objective has been assessed.

A. Managing security risk		P	F
A.1	Governance		
A.2	Risk management		
A.3	Asset management		
A.4	Supply chain		
B. Protecting against cyber attack		P	F
B.1	Service protection policies and processes		
B.2	Identity and access control		
B.3	Data security		
B.4	System security		
B.5	Resilient networks and systems		
B.6	Staff awareness and training		
C. Detecting cyber security events		P	F
C.1	Security monitoring		
C.2	Proactive security event discovery		
D. Minimising the impact of cyber security incidents		P	F
D.1	Response and recovery planning		
D.2	Lessons learned		

Conclusions

Trial Inspection Operator Selection

The operators that volunteered for the trial inspections were recognised as a self-selecting group. Discussion indicated that the reasons for volunteering were:

- The operator believed that it was ahead of the industry in developing cyber security risk controls and wanted feedback from HSE on its progress to date without the potential cost and enforcement associated with a normal inspection.
- The operator was making modifications (e.g. upgrades) to its IACS and therefore wanted to get early feedback on their approach rather than have to make changes later.

The operators were already aware of cyber risks and that something would need to be done to address these risks.

Therefore, it is likely to be the case that the level of compliance across the industry is likely to be overall lower on average than seen at the trial inspections.

Compliance against the OG

Compliance has been judged in general against the issued OG, although this was augmented with some of the emerging requirements of the NCSC NIS principles and guidance as the trial inspections progressed.

In summary:

- There were no Operators that had fully achieved all of the objectives. This was as expected – the OG was released just over one year before the trials and it would take time for Operators to fully comply. It is therefore useful to consider where progress has currently been made.
- There was good progress with some Operators starting to address requirements with respect to principle A (Managing Security Risk), i.e. setting up governance arrangements, risk and asset management. Note that part A4 (Supply Chain) requirements were not in the original OG and therefore it is not surprising that this topic had not been addressed by most sites.
- There was good progress with some Operators starting to address requirements with respect to principle B (Protecting against Cyber Attack). This section covers both managerial and technical cyber security protective countermeasures.
- However they had not fully met the required objectives, for example:
    a. Full roles and responsibilities and associated competence requirements not defined or met with particular reference to the supply chain.
    b. Risk assessment not completed to defined countermeasures proportionate to the MAH risk and inadequate asset management.
    c. Technical measures (such as network access controls, device hardening, physical logical and data access controls) not consistently implemented or managed.
- In particular the cyber security management systems (including competence management) were not well developed or formalised in most cases and therefore where cyber security measures were in place, they were often not well managed.
- It was also noted that management of cyber risks was in many cases placed upon the operator's control and instrument (or equivalent) team. Whilst it was agreed that this is probably correct, only a few Operators had provided additional resource to those teams.
- There was less progress on the mitigation countermeasures, i.e. detecting cyber events (principle C) and minimising their impact (principle D). Whilst there is clearly more work

required on these topics by Operators, it is not unusual (or unexpected) that Operators would first focus on preventative measures before addressing mitigation measures.

- Whilst there was some evidence of improved "security by design" in newer systems, issues associated with legacy equipment are likely to persist – for example it was noted that new systems installed were deployed with windows 7 which goes out of support in two years. This will be an issue that will need to be managed on an ongoing basis.

Differences between industry sectors

The differences between sectors was not analysed in detail (as this would reveal the participants and in any case there was only a small data set) but the following was noted:

- There were no major differences between the sectors
- There was overall better levels of awareness and compliance within Operator that have previously been considered as critical national infrastructure and therefore received guidance in the past.
- There was overall better levels of awareness and compliance for some of the larger multi-national Operators – this was attributed to them recognising the business and reputational risk and therefore taking measures to reduce this.
- There was overall better levels of awareness and compliance for Operators that had newer equipment – i.e. evidence that some of the control system vendors were building more security features into their equipment.

Inspection approach and OG

The following general learning points were identified during the trials:

- Planned inspection time: Apart from the very large sites, the trial inspections were planned to be one day on site plus associated preparation time ahead of the inspection and review and reporting time following the inspection. This was found to be insufficient to cover the agenda items and resulted in some of the aspects (typically CSMS) being addressed by correspondence. This was fed back at an early stage to the intervention planning process and additional time was allowed for inspections planned for 2018-19 work year – this should be reviewed following these inspections.

- Secure data transfer: It is necessary to receive significant amounts of sensitive data to prepare for the inspection. The inspection report and letter sent back to the Operator following inspection is also likely to be considered as sensitive. During the trials, temporary solutions were used such as removal of sensitive data, encrypted data and a secure email service that was used to send out inspection reports. A method of secure data transfer needs to be established for future inspections. This is being progressed, and HSE is reviewing security classification of such material.

- Human Factors: The topic of cyber security overlaps with a number of HF issues. Many of these (e.g. competence management, procedures etc.) are well known, already have HF guidance in place and could conceivably be addressed through existing inspection of these topics. However, some HF issues (e.g. insider threat and personnel screening and monitoring) are new topics and require development. During the trials (and consistent with the approach normally taken with other topics such as functional safety) these issues were addressed so far as they related to the EC&I discipline. However, there is a gap that needs to be addressed on these issues. This is being progressed by the HF team with support from the EC&I team.

- Duplication: The technical and managerial measures were split into different sections of the inspection agenda. Whilst this was appropriate in some cases, it led to repetition during the inspection (and report) in other cases. For example – there are both technical and managerial measures for logical access controls. It is recommended that where appropriate:
    a. Within the OG, there is clear cross-reference between the technical measures and associated managerial measures.
    b. In the inspection agenda template, the technical measures and managerial measures are discussed at the same time.
    c. In the inspection report template, there will need to be some consideration on how best to report on these measures to prevent duplication.

The OG, inspection agenda template and the inspection report template will need to be updated to address these issues.

- NIS Guidance: The NIS principles and guidance were released during the trial inspections. Compared to the NIS guidance, there were a few omissions within the HSE OG (e.g. supply chain). Apart from these, there was broad agreement between the NIS guidance and HSE OG on the technical and managerial security countermeasures required. However, the structure and breakdown of the requirements was different. The HSE OG provides a lifecycle management approach to managing cybersecurity in line with what Operators already do in managing functional safety. To ensure consistency between different government guidance, the HSE OG (since NIS guidance covers many different competent authorities) will be updated to take account of the NIS guidance but keeping the existing overall lifecycle management approach of the OG, thus providing a single source authoritative guidance that can be used to comply with both safety and NIS regulations.
- NIS Cyber Assessment Framework: NCSC has now released their cyber assessment framework (CAF) which can be used to assess (either self-assessment or by the regulator) Operator compliance against the NCSC guidance. NCSC does not expect all Operators to fully comply with all aspects of the NIS guidance, rather than the level of compliance will be different for different sectors. For regulation, HSE requires a benchmark that represents legal compliance. Therefore:
    - It will be necessary for HSE to establish the legal benchmark. This is largely completed through the existing OG and will be improved in the next version.
    - In judging compliance against the benchmark, HSE will require to assess the level of performance or risk gap in order to determine appropriate and proportionate enforcement outcomes. These will need to be appropriate for both NIS and COMAH. It is expected that this should be developed to closely integrate with the existing performance scoring (10-60 scores) and the EMM.
    - NCSC would prefer that it is possible to relate performance of Operators against their CAF profiles. This will require development to be able to equate the HSE performance scores (10-60) against the HSE benchmark (OG) that is linked to a CAF profile. This requires further development.

Recommendations for Industry

Ahead of any proposed regulatory activity under COMAH or NIS, industry is recommended to address the following points:

1. At the management board level, recognise the cyber risk (both COMAH MAH and NIS essential service where appropriate) and establish formal governance arrangements, policy, identify relevant roles and responsibilities, risk management and decision making processes and provide appropriate resources (in terms of people and capital).
2. Identify competence requirements (based upon the roles and responsibilities) and put plans in place to improve competence. This should include general awareness as well as more detailed technical competences.
3. Become aware of relevant good practice – including the HSE OG86 edition 2 (now published in Dec 2018)
4. Develop a risk assessment approach that is sufficient to identify what cyber security countermeasures will be required and put a plan in place to address the gaps that are found. The risk assessment approach should consider the risk (both COMAH MAH and to essential services where appropriate) and result in countermeasures that are proportionate to the MAH or loss of essential services risk.
5. Outline the requirements for a cyber security management system (preferably as part of the wider management systems) and put plans in place to develop and implement the systems.

Recommendations for HSE

The OG (and associated inspection agenda and reporting templates) should be updated to bring these in line with the NCSC guidance and above findings.

HSE has already committed to completing some cyber security inspections in this current (Apr 2018 – Mar 2019) work year under COMAH. These should be done with the revised OG rev 2 and should cover risks from MAH risks and NIS, but without enforcements action on any NIS specific issues.

Since the completion of the trial inspections, it has been confirmed that HSE will be carrying out some of the regulatory activities for the Energy sector (oil and gas) for the NIS Regulations on behalf of the NIS competent authority (BEIS).

As a result HSE should be developing a common regulatory approach for both NIS and COMAH with respect to cyber security.

Joint Industry and HSE Recommendations

A high level guidance should be developed aimed at senior management to support the operational guidance. This work could be led by COMAH Downstream Oil Industry Forum (CDOIF) under the direction of COMAH Strategic Forum (CSF).

The high level guidance, aimed at senior managers should address the issues and risks to business, and raise awareness of cybersecurity so that senior managers can act on informed advice.

Appendix A – Example agenda

COMAH Control & Instrumentation (C&I) Inspection

Site:

Date:

Proposed agenda: Cyber security – baseline inspection against HSE Operational Guidance: Cyber Security for Industrial Automation and Control Systems (IACS).

Information to be provided ahead of inspection:

- Cyber security management system documents, to include:
  - Definition of cyber security roles and responsibilities
  - Competence requirements and how these are met
  - Relevant policy and procedures
- Simple network drawings and asset registers
- Cyber security risk assessment and countermeasures required including plans for implementation of any gap analysis e.g. for existing (legacy) systems
- Please ensure that any other relevant information / documentation is available for the inspection and you have suitably competent personnel in attendance to assist with the above agenda.

1. **Introductions and objectives of visit.**
2. **Site overview**
   - Company to provide a brief overview of site operations and processes (i.e. main operating units) and the control and safety systems in use.
3. **Governance**
   - Overarching cyber security policy and management commitment and ownership
   - Monitoring and oversight
4. **Personnel**
   - Organisation, roles and responsibilities in relation to cyber security including IACS Responsible Person(s).
   - Screening of employees – pre-employment checks, monitoring behaviour and conflict of interest
   - Competencies and competence management. To include:
     - Definition of competency requirements
     - Meeting these requirements – training, experience, third parties
   - Security Culture
5. **Definition of IACS:**
   - CSMS procedure for identifying IACS assets, zones and conduits.
   - Review of simple network drawing(s)
     - Equipment, technologies and connections installed for the safe operation and monitoring of the processes with MAH risks, for example: PLCs (Process/SIS), HMIs, PC stations (Operator workstations, Servers, Engineering workstations).
     - Network infrastructure for the IACS and connections to external networks (e.g. corporate LAN)
     - Temporary connections e.g. portable PCs for PLC programming,

    - Remote access
- Review of asset register
- Management of obsolescence

6. **Risk assessment**
    - CSMS procedure for identifying IACS risk assessment
    - Review of risk assessment findings
    - Application of risk rankings to zones
7. **Definition and Implementation of Countermeasures**
    - CSMS procedure for defining and implementing countermeasures.
    - Review countermeasures required
    - Existing (legacy) systems
    - Review additional SIS Considerations

8. **Procedural controls (as part of CSMS)**

A. Managing security risk

A.1 Governance – covered above

A.2 Risk management – covered above

A.3 Asset management – covered above

A.4 Supply chain

- Identification of third parties
- Security requirements and assurance of these
- Corporate networks

B. Protecting against cyber attack

B.1 Service protection policies and processes

- Security screening – covered above
- Configuration management (e.g. firewalls, VPNs, switches, WAP, VPN)
- Management of change (e.g. of firewall config, connections to IACS network)
- Auditing of policies and procedures.

B.2 Identity and access control

- Definition of authentication methods
- Definition of users, devices and services requiring access (including device-to-device)
- Splitting access across roles
- Management – encryption key and password storage, distribution and revocation

- Physical access controls and management of these (key access or electronic access systems)

B.3 Data security

- Specification of data security is protected at rest and in transit and sharing requirements
- Identification of data required to safely operate and ensuring availability
- Data on devices
- Data not physically protected (e.g. Wi-Fi, radio)

B.4 System security

- Device hardening (vendor guidance, BIOS, disabling ports, services application management, default passwords etc.)
- Software / patch management on all IACSs assets including network devices.

B.5 Resilient networks and systems

- Validation testing of countermeasures
- Operation
    - File transfer and use (e.g. software patches, configuration data from vendors etc.)
    - Temporary / remote operational access connections.
- Maintenance
    - Updating of security software (AV, IPS etc.)
    - Temporary / remote maintenance access including third parties, laptops, connections.

B.6 Staff awareness and training – covered above

C. Detecting cyber security events

C.1 Security monitoring

- Awareness of threats (ICS-CERT, CiSP etc.)
- Aggregate, monitor, analyse and review security logs (windows, IPS, AV, networks etc.)
- Performance indicators
- Physical inspection to reveal tampering or physical access
- Management and oversight

C.2 Proactive security event discovery

- Penetration Testing
- Enhanced Monitoring

D. Minimising the impact of cyber security incidents

D.1 Response and recovery planning

- Backup, backup storage, restoration testing and restoration

- Incident response plant including
    - Roles and responsibilities
    - Identification, reporting and assessment
    - Initial mitigation measures
    - Data collection and analysis
    - Escalation and recovery strategies
    - End of incident
- Exercises
- Consideration of COMAH emergency response

D.2 Lessons learned

- Incident (real or exercise) investigation and review of incident response plan

9. Site inspection

Sampling of

- Accuracy of IACS network drawing and asset register
- Physical security controls
- Server / workstation countermeasures, e.g. hardening, software and patch management
- Software versions and patch management
- Incident response

10. Summary

- Feedback to site, any questions.

Appendix B – Detailed levels of compliance

The level of compliance against the OG detailed requirements are summarised below split according to the NCSC NIS Principles.

Each of the NIS principles has been assessed as either: red, amber or green based upon the number of operators that had partly or fully achieved each objective as follows:

PART (P)	FULL (F)
Most operators had started / partially completed the objective (≥6/8)	Most operators fully completed the objective (≥6/8)
Some operators had started / partially completed the objective	Some operators had fully completed the objective
Most operators had not started / partially completed the objective (≤2/8)	Most operators had not fully completed the objective (≤2/8)

A. Managing security risk

A.1 Governance

		P	F
A.1.1	Management aware of cyber risks to IACS		
A.1.2	Management recognise and own safety risks associated with cyber risks to IACS		
A.1.3	Policy for cyber security of IACS		
A.1.4	Policy includes decision making process for addressing cyber risks		
A.1.5	Monitoring / oversight of IACS cyber countermeasures by management		
A.1.6	Role of IACS Responsible Person identified		
A.1.7	All IACS roles and responsibilities identified and recorded / briefed		

In general it was noted that whilst there was general awareness, governance was not sufficiently developed or formalised as would be expected for a MAH risk topic. At least in part this was because of a failure to recognise the MAH risk due to cyber-attack – many only recognised a business impact only or not at all.

A.2 Risk management

		P	F
A.2.1	Risk assessment completed to appropriate standard considering MAH risk		
A.2.2	Risk assessment formally documented and review process in place		
A.2.3	Countermeasure requirements defined for zones to address MAH risk		
A.2.4	Suitable gap assessment / implementation plan defined and resourced		

Most operators had attempted some kind of risk assessment and identified some countermeasures. However in general, risk assessments, where completed, did not consider the MAH risk and were therefore not adequate. In many cases selection of countermeasures was based upon gap

assessment against a defined standard (typically internal) with no differentiation based upon MAH risk.

Many operators sought advice / guidance during the inspection on what a good risk assessment would look like.

A.3 Asset management

		P	F
A.3.1	Responsibilities and procedure for identifying and recording IACS assets etc.		
A.3.2	Adequate simple network drawing in place i.e. sufficient detail and coverage		
A.3.3	Adequate Asset register in place for assessment and ongoing management of IACS		
A.3.4	Suitable obsolescence process / plan in place		

Most operators had some sort of network drawing in place but this was often not sufficient to understand the extent of the IACS and review the cyber risk. Similarly with the asset register – most operators had a register but it was not sufficient for the purpose of assessment and ongoing management.

It was recognised that improvements should be made to the OG to more clearly define the purpose of these documents and improvements made to the example network drawings to make it clearer what is expected with respect to a hierarchical approach to network architecture and defence in depth.

A.4 Supply chain

		P	F
A.4.1	Identification of third parties with responsibilities for the IACS		
A.4.2	Specification of cyber security requirements		
A.4.3	Assurance that cyber security requirements met		

Note this requirement was not in the issued OG and therefore, not surprisingly, was not addressed by most operators. It was identified as a requirement from the NIS guidance and was discussed at some of the later trial inspections.

Summary for Part A

Some operators had awareness of cyber risks and how these might impact safety and had started to implement governance arrangements, policy, risk management and asset management but in general this was not fully implemented and / or to the necessary standards.

There was very little recognition of the risks from the supply chain, although this topic was not covered in the issued OG, and will be updated accordingly.

It was noted that most operators that had made progress in these areas had done so specifically because of the issue of the HSE OG and participation in the trial inspections.

B. Protecting against cyber attack

B.1 Service protection policies and processes

		P	F
B.1.1	Policy and procedures for cyber security of IACS documented		
B.1.2	Policy and procedures are implemented, communicated and reviewed		
B.1.3	Screening and monitoring of IACS responsible personnel (incl. 3rd parties)		
B.1.4	Configuration management is in place		
B.1.5	Management of change for the IACS is adopted incl. relevant risk assessment		
B.1.6	Periodic audit of the policy and procedures is completed		

The trial inspections were, in general, found to be too short to cover all the agenda items. Therefore, the section on the CSMS detailed procedures was often not completed in any detail, instead relying on the information provided before, during and after the inspection.

However, it was clear that CSMS needed to be more formalised: No operators had a full range of policy and procedure in place, but most operators had top-level policy in place and some operators had some or had started to put procedures in place.

Screening of personnel was generally carried out in general as part of pre-employment checks but not proportional to cyber risk.

B.2 Identity and access control

		P	F
B.2.1	Definition and review of users, devices and services based upon least privilege		
B.2.2	Authentication approach and management defined		
B.2.3	Removal of rights and return of equipment		
B.2.4	Physical protection measures and their management		

Some operators had role definitions (typically operator, supervisor, engineer, admin). It was noted that many operators had recognised the need to improve access control – for example operators were moving to unique usernames where common usernames were previously used. But most operators did not have adequate overall management in place especially with respect to revoking access no longer required.

Most operators had some physical protection measures in place but these were found to be inadequate or inadequately managed in most cases.

B.3 Data security

		P	F
B.3.1	Identification of sensitive data and specification of how it will be protected		
B.3.3	Protection of data on devices		
B.3.4	Protection of data moving over non-IACS networks		

There was in some cases recognition of data security requirements, although this was normally associated with loss of corporate confidential data rather than data linked to cyber security associated with MAH.

Note – the coverage of this topic was expanded during and after the trials to include data on devices.

B.4 System security

		P	F
B.4.1	Suitable network architecture in place		
B.4.2	Suitable network perimeter devices in place (e.g. firewalls)		
B.4.3	Suitable device hardening processes in place		
B.4.4	Operation & Maintenance - file transfer across IACS boundary		
B.4.5	Operation & Maintenance - temporary / remote access		
B.4.6	Operation & Maintenance - AV, IDS definition updates etc.		
B.4.7	Suitable patch management process documented		
B.4.8	Patch management process implemented		

This section largely deals with technical measures. Most operators had largely suitable network architectures in place with separate IACS networks and a hierarchical approach where appropriate. However, whilst control of the IACS network perimeter was in place it was often found to be inadequately controlled – for example there were unnecessary connections or poor management.

Many of the other controls for file transfer, remote and temporary access, malware detection and software vulnerabilities were often addressed in an ad-hoc manner, i.e. there were often no management systems and the controls were not consistently applied or subsequently monitored.

B.5 Resilient networks and systems

		P	F
B.5.1	Threat intelligence - awareness, analysis and review		
B.5.2	Disaster recovery strategy - defined and backups in place and secure		
B.5.3	Disaster recovery strategy - restoration testing		

Most operators did not have formal intelligence of cyber threats and were encouraged to join the NCSC CISP and other information sources and set up a process of formal review and analysis.

Most operators had some backup strategies in place although these often were targeted at the main control and safety systems and missed the wider IACS network scope. Often the backup strategies

were not formalised as part of a management system. Restoration testing was not specified or completed in most cases.

B.6 Staff awareness and training

		P	F
B.6.1	Competence management - competence requirements defined		
B.6.2	Competence management - competence requirements met		
B.6.3	Cyber security awareness and culture		

Some operators had identified some cyber competence requirements and completed training although this was often targeted at a few key roles and not formalised into the wider competence management systems. Note – since wider roles and responsibilities had not been defined, the complete range of competence requirements were also not defined.

Some operators had completed wider cyber awareness and although this was useful it did not specifically cover the IACS.

Summary for Part B

This section covers managerial and technical cyber security countermeasures.

Whilst some operators had developed some high level policy and some procedures there was not the full range of formal cyber security and competence management systems in place to manage cyber security MAH risk.

There were some measures in place to control physical, logical and data access but these were generally not adequate and not well managed.

The greatest level of compliance was associated with B4 (system security) which covers many of the technical security countermeasures. In many ways this is consistent with progress on the topic of functional safety historically - i.e. Engineers initially focussing on technical measures rather than a lifecycle approach with appropriate management systems.

C. Detecting cyber security events

C.1 Security monitoring

		P	F
C.1.1	Security logging requirements defined and logs securely stored		
C.1.2	Monitor, analyse and review logs		
C.1.3	Periodic inspection / monitoring to reveal tampering		
C.1.4	Review and carry out actions		

Some operators were collecting, monitoring, analysing and reviewing logs but this often did not cover all relevant assets in the IACS network – e.g. typically it covered the control system assets and was managed by the control system vendor.

Most operators did not do any physical monitoring of assets.

The underlying issue was that there was no recognition from the operators of the importance of monitoring and no strategy defined in the management systems.

C.2 Proactive security event discovery

		P	F
C.2.1	Enhanced testing where required		
C.2.2	Establishment of baselines and monitoring for abnormal situations		
C.2.3	Enhanced monitoring		

It should be noted that proactive security event discovery techniques should only be employed once more basic security monitoring (C1) has been established. Also, on many sites it may not be reasonably practicable to carry out proactive security event discovery techniques. Therefore, it is not surprising that there was very little progress on this topic.

It is expected that operator should define an overall strategy for monitoring and where appropriate consider the measures described in this section – this had not been completed.

Summary for Part C

Whilst there were some operators who had some basic security monitoring (C1) in place, there was not an overall monitoring strategy defined or management systems to ensure that the results of monitoring were routinely analysed and reviewed such that relevant action responses would be generated. Most operators did not carry out any inspection of equipment.

With respect to proactive security event discovery (C2), these techniques are only expected to be deployed once basic security monitoring is established and where it is necessary to address the risk (it will not be reasonably practicable in many cases). However, most operators had not considered what, if any would be required to reduce cyber risks.

D. Minimising the impact of cyber security incidents

D.1 Response and recovery planning

		P	F
D.1.1	Development of a cyber incident response plan for IACS		
D.1.2	Periodic exercise of the plan		
D.1.3	Consideration of impact on MAH emergency response		

Some operators had defined cyber incident response plans, but these were often generic requirements (in policy) and not developed for the specific operator's site. Most operators had not planned for incident response exercises or considered incident response with respect to MAH emergency planning.

D.2 Lessons learned

		P	F
D.2.1	Root cause analysis following incident or exercise		
D.2.2	Review of technical and managerial countermeasures following RCA		
D.2.3	Review of incident response plan following RCA		

Following on from D1 above, most operators had no processes in place to analyse and review incidents or exercises and learn lessons.

Summary for Part D

Some operators had defined cyber incident response plans, but these were often generic requirements (in policy) and not developed for the specific operator's site. Most operators had not planned for incident response exercises or considered incident response with respect to MAH emergency planning.

Most operators had no processes in place to analyse and review incidents or exercises and learn lessons.