Cyber Security for Industrial Automation and Control Systems (IACS) EDITION 2

Open Government status

Open

Contents

Target audience

Chemical Explosives and Microbiological Hazards Division (CEMHD) Electrical Control and Cyber Security (EC&CS) Specialist Inspectors and Energy Division (ED) Electrical Control and Instrumentation (EC&I) Specialist Inspectors.

Summary

The term ‘duty holder’ is used in this guidance to describe those having duties under relevant health and safety legislation and / or under the Network Information Systems (NIS) Regulations.

The first edition of this guidance was published in March 2017 and used as a basis for carrying out a number of field trial inspections at major accident workplaces. This second edition has been issued following the feedback from those field trials and to address some wider developments in this topic. This second edition is compatible with the first, in that the approach and countermeasures are broadly the same as edition 1, although additional guidance on how to apply them has been included.

Whilst edition 2 does not include many additional requirements, it includes some important changes. These include:

- Incorporation of feedback from the field trials to improve the usability of the guidance. This has necessarily increased the size of the guide.
  - more detailed content has been added explaining how some of the requirements should be met, particularly in relation to management systems and some of the technical countermeasures, most notably Network Architecture, Segregation and Access.
  - In addition, the process of assessing if a duty holder had selected appropriate countermeasures based solely upon zone criticality was not adequate. The risk assessment approach has also been changed in the latest draft of IEC62443-2-1. Therefore, edition 2 requires inspectors to also consider if countermeasures are appropriate considering threat scenarios.

- Inclusion of Network Information Systems (NIS) regulation requirements. These apply to Operators of Essential Services only. This change mainly impacts upon definition of IACS scope and risk assessment. Operators subject to both Health and Safety and NIS legislation should carry out risk assessment(s) that cover both major accident and loss of essential services consequences and then use the highest risk to determine the countermeasures to be applied. The approach and countermeasures are common to both sets of legislation.

- Alignment of the guidance with the National Cybersecurity Centre (NCSC) cyber security principles, which was published subsequent to the publication of the first edition of this guidance. This change is largely presentational since although the NCSC principles are related to NIS, they were found to be consistent and compatible with the requirements within Edition 1. However, some additional requirements were added, most notably management of supply chains.

- A managed approach to implementing the countermeasures. This edition of the guidance identifies a basic level of countermeasures only to address the lower

levels of risk based on the NCSC basic cyber assessment framework (CAF) profile. As these are adopted, and duty holders gain experience and NCSC CAF framework develops further, the basic countermeasures may need to be improved to address higher levels of risk. This guide will be updated in future to include the enhanced control measures that will address higher levels of risk when the NCSC CAF is updated.

This Operational Guidance represents the Health and Safety Executive (HSE) interpretation of current and developing standards on industrial network, system and data security, and functional safety in so far as they relate to major accident workplaces and relevant sectors of operators of essential services.

The Guidance will be applied by Inspectors to major hazards workplaces (as defined within the Relevant Regulations section of this guidance) only in so far as it relates to the control of major accident hazards by the duty holder.

Where such duty holders also have legal duties under The Network and Information Systems Regulations 2018 (NIS) as an Operator of Essential Services (OES), this guidance will be applied by Inspectors in so far as it relates to both control of major accident hazards and also loss of essential services.

Where an OES is not a duty holder for a major hazards workplace, this guidance will be applied by Inspectors only in so far as it relates to the loss of essential services by the duty holder as defined under NIS.

This guidance does not cover other data protection requirements, for example as required by data protection legislation, or other business data protection requirements, e.g. protection of intellectual property.

For the purpose of the enforcement management model, this guidance is an interpretive standard.

This Operational Guidance could contribute towards a suitable demonstration of compliance with relevant legislation, in order to demonstrate that appropriate and proportionate measures have been taken to control cyber security risks, but alternative equivalent means may also be used to demonstrate compliance.

Note that the requirement to address cyber security threats for SIS in clause 8.2.4 of BS EN 61511 (edition 2) may be met by following the process detailed in this Operational Guidance.

Introduction

Reducing the risk of a major accident, or operating an essential service, often requires the application of process control and safety systems and / or electrical supervisory / control systems. Therefore, major hazard risk reduction or continuity of essential service(s) may depend upon the correct functioning of these systems.

In the context of cyber security these systems are often termed Industrial Automation and Control Systems (IACS), or Industrial Control Systems (ICS) or Operational Technology (OT). This guidance uses the term IACS.

Cyber security is a term used to define measures taken to protect IACS against threats and through accidental circumstances, actions or events, or through deliberate attack. The threats can originate from the Internet, external networks (corporate or third party), maintenance activities, software upgrades, and unauthorised access etc. with the potential to result in incidents with major health, safety or environmental consequences and / or loss of essential services.

Duty holders may operate a range of IACS; these typically include basic process control and safety systems, electrical control / data acquisition systems and the associated information and business systems connected via an IACS network infrastructure.

IACS are now more accessible and 'open' than ever before with increasing use of commercial-off-the-shelf information technology (IT) solutions, allowing connectivity and exchange of data with other systems and with external (corporate or third party) networks. IACS are thus increasingly merging with networks and systems. This, together with an increased use of non-proprietary systems (e.g. Microsoft Windows, typically for operator interface and engineering workstations), and the associated increased functionality has led to modern IACS having an increased attack-surface and therefore becoming potentially more vulnerable to a cyber-attack, even if they are 'air-gapped' from other systems.

In major accident workplaces, prevention and mitigation of major accident risks is the responsibility of the major accident duty holder, defined in relevant health and safety legislation. This is normally achieved through the application of good practice, an assessment of the hazards and risks posed and application of appropriate risk reduction measures. However, normal risk assessment processes such as hazard and operability studies (HAZOP), process hazard risk analysis (PHR) etc. are not sufficient to address cyber security threats to IACS since they do not, in general, consider multiple contingencies (i.e. several dangerous events occurring at once) or know and understand the capabilities of those that have malicious intent that are typical of a cyber-attack.

Operators of essential services (OES) may also have previously considered disruption to these services as part of business risk assessments, e.g. from equipment failures. But, these risk assessments are unlikely to have considered the risk to loss of essential services with respect to the impact on UK infrastructure, or from cyber-attack.

Therefore, it is not possible to discount cyber security threats on the basis of traditional risk assessment processes or to assume that the risk of such threats will be addressed by existing risk reduction measures alone.

Duty holders may use IT and business cyber security solutions (e.g. firewalls, anti-virus software etc.) to improve cyber security of the IACS, but these need to be applied in the correct way as part of a holistic approach incorporating people, process, procedures and technology.

It may not be possible for existing IACS systems (which were designed prior to widespread cyber security threats) to comply with all the requirements of the quoted standards. It is expected however that duty holders should take appropriate and proportionate steps to reduce cyber security risks and where the required countermeasures cannot be applied to existing systems, other compensating countermeasures are considered instead.

The following guiding principles were used in producing this guidance:

- Protect, detect and respond. It is important to be able to detect possible attacks and respond in an appropriate and timely manner in order to minimise the impacts.
- Defence in depth. No single cyber security countermeasure provides absolute protection as new threats and vulnerabilities can be identified at any time. To reduce these risks, implementing multiple organisational, protective and detect and respond countermeasures in series avoids single point failures: i.e.
  Organisational Countermeasures – Governance, Risk Management, Asset Management, Supply Chain Management, Policy and Procedures, Competence and Awareness
  Protective Countermeasures – Identity and Access Control, Data Security, System Security and Resilience
  Detect and Respond Countermeasures – Security monitoring, Incident response

This guidance describes the required cyber security countermeasures to address low levels of cyber security risk based upon the NCSC basic CAF profile (see reference to good practice below). The topic of cyber security is rapidly developing and relevant international, national or industry standards have yet to be fully established. Therefore, this guidance will be updated in future as relevant standards are established and to address higher levels of risk as the NCSC CAF profiles develop further.

Action

Inspectors should:

- Use the high-level process described in Appendix 1, Figure 1 and the accompanying notes along with the associated Appendices 2-5 to verify, or otherwise:
  - the adequacy of a cyber security management system including competence management;
  - the adequacy of cyber security countermeasures;

  for (as appropriate):
  - Major accident workplaces;
  - Operators of essential services covered under the NIS Regulations.
- Refer duty holders to the high-level process described in Appendix 1, Figure 1 and the accompanying notes along with the associated Appendices 2-5.

Background

International Standards are being developed, such as ISA/IEC62443 to provide standards for analysing cyber risk and to specify the design, installation, inspection, maintenance and testing of cyber security countermeasures. However, these standards are yet to become established good practice.

Whilst it is expected that relevant standards for IACS cyber security will continue to be developed, this document provides guidance to Inspectors with a practical interpretation of the standards.

This guidance may also optionally be used as good practice by duty holders. However, duty holders are free to follow other good practice so long as it provides equivalent protection. Duty holders may need to work with IACS manufacturers / vendors and system integrators etc. to achieve the requirements.

Organisation

Targeting

Major accident workplaces where cyber security could pose a major risk to the health and / or safety of employees and / or members of the public and / or environment.

Operators of essential services, as defined in the NIS Regulations, in the energy sector where cyber security could pose a risk to loss of essential services.

This guidance will be applicable to duty holders who own / operate IACS and to IACS manufacturers and system integrators.

Timing

Ongoing.

Resources

To be used by CEMHD EC&CS and ED EC&I Specialist Inspectors during interventions at major accident workplaces or operators of essential services.

Recording & Reporting

No special requirements.

Health & Safety

No special requirements.

Diversity

No special requirements.

Further References

Relevant Regulations

Major Accident Workplaces

- Control of Major Accident Hazards Regulations (COMAH) 2015

- 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

Operators of Essential Services
- Network and Information Systems (NIS) Regulations 2018

Recognised Relevant Good Practice
- BS EN 61511 (Edition 2) – Functional safety – Safety instrumented systems for the process industry sector
- NCSC NIS Guidance Collection (including Cyber Assessment Framework - CAF) https://www.ncsc.gov.uk/guidance/nis-guidance-collection

Other Relevant Standards
- ISA-TR84.00.09-2013- Security Countermeasures Related to Safety Instrumented Systems (SIS).
- BS EN / IEC 62443; Security for Industrial Automation and Control Systems; 4 Parts.
- BS EN ISO/IEC 27001; Information technology – Security techniques – Information security management systems - Requirements

Other Relevant Guidance
These provide useful background and further information on cyber security:
- National Cyber Security Centre – 10 Steps to Cyber Security https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
- National Cyber Security Centre – Security for Industrial Control Systems https://www.ncsc.gov.uk/guidance/security-industrial-control-systems
- NIST Publication 800-82 – Guide to Industrial Control Systems (ICS) Security http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- ICS-CERT Recommended Practices https://ics-cert.us-cert.gov/Recommended-Practices
- EEMUA Industry Information Sheet 2 – Cyber security assessment process for industrial control systems https://www.eemua.org/EEMUAPortalSite/media/EEMUA-Flyers/EEMUA-Industry-Information-Sheet-2.pdf
- Purdue Model - Theodore J. Williams (1994) "The Purdue enterprise reference architecture." Computers in industry Vol 24 (2). p. 141-158
- SANS Twenty Critical Security Controls for Effective Cyber Defence https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download

Contacts

Chemicals, Explosives and Microbiological Hazards Division; Electrical, Control and Cyber Security team.
Energy Division; Electrical, Control and Instrumentation team.

Appendix 1: Process for the Management of Cyber Security on IACS

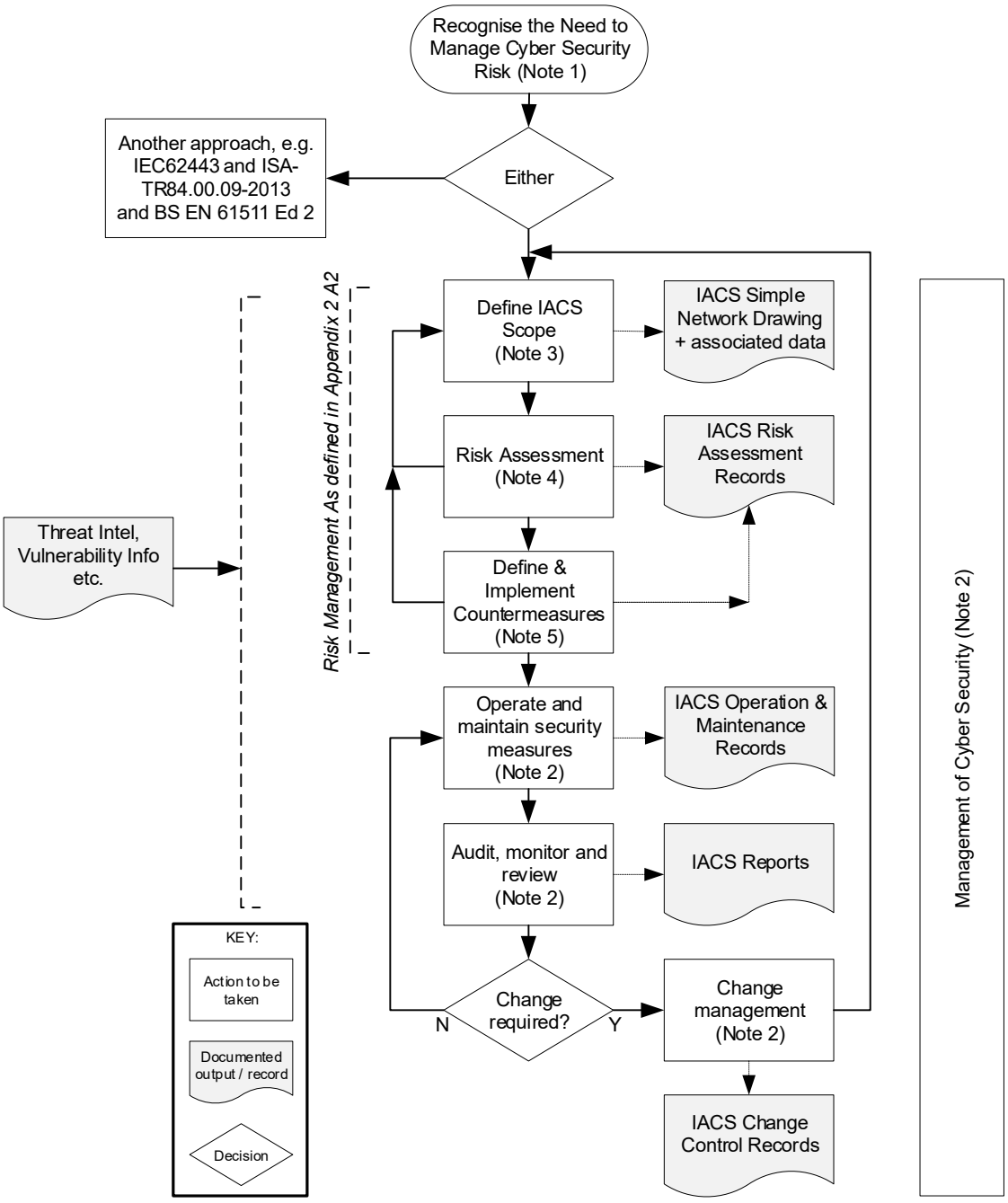


Figure 1: Process for Management of Cyber Security on IACS

Notes to Figure 1, Appendix 1

Note 1 – Recognise the Need to Manage Cyber Security Risk

Most IACS will be vulnerable to at least some cyber security risk. Even where the IACS is largely non-programmable or is physically separated from other networks, there will be cyber security risks from, for example, activities completed during maintenance, software upgrades, vendor support or by unauthorised physical access etc.

Resources will need to be applied by the duty holder to manage cyber security risks to build up competence in the subject, develop appropriate management systems and select and manage appropriate cyber security organisational and technical countermeasures.

The number and type of the systems vulnerable to attack and potential consequences that could be realised should be considered when deciding how much resource needs to be applied to ensure a proportionate approach is implemented.

Note 2 – Cyber Security Management System (CSMS)

Purpose

The purpose of this step is to implement a suitable CSMS.

Background

Appropriate cyber security risk management can only be achieved if the definition of the countermeasure requirements and the on-going management of the countermeasures is completed in a systematic way.

Approach

A CSMS should be implemented for the defined IACS. This should be incorporated into the site's wider management system(s).

The structure of the CSMS doesn't need to be different to any other management system and could take a number of forms, for example:

- As described in relevant standards such as IEC 62443 and ISO 27001;
- the structure of management activities presented in IEC 61511;
- the plan / do / check / act structure of general management systems that is used in "Managing for health and safety (HSG65)", http://www.hse.gov.uk/pubns/books/hsg65.htm.

Similarly, technical aspects of cyber security management do not need to be different to any technical discipline, for example, in the way that Engineering projects are executed, or assets are maintained, modified and decommissioned.

Whatever form of CSMS is adopted, the following cyber security principles should be addressed (additional guidance is provided by the NCSC NIS guidance, IEC 62443-2-1 and 2-2 and appendix 2 of this guidance):

A. Managing security risk
    A.1 Governance
    A.2 Risk management
    A.3 Asset management
    A.4 Supply chain

B. Protecting against cyber attack
    B.1 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
    C.1 Security monitoring
    C.2 Proactive security event discovery

D. Minimising the impact of cyber security incidents
    D.1 Response and recovery planning
    D.2 Lessons learned

The documents of the CSMS should be maintained to be accurate (i.e. up to date and sensitive to changing threats / attack methods as they emerge over time), suitable for their purpose and site specific in setting out what is to be done, by whom and when; it is not necessary to include repetition of guidance when this could be referenced.

Output of this Step
The output of this step will be the implementation of formal policy, procedures and management systems which will be subject to ongoing management and review.

Note 3 – Defining the IACS Scope

Purpose
The purpose of this step is to identify the IACS scope and record it in a format that can be used for risk assessment and ongoing management of cyber security, i.e. an IACS Simple Network Drawing and associated data.

Background
In order to defend a system, it is first important to know what needs to be defended. Risk assessment, definition of the required countermeasures and on-going management of the countermeasures can only be achieved if the full scope of the IACS is understood and documented.

Approach
The IACS boundary should be defined to include all the IACS assets (computers and other devices etc. and the connecting networks) associated with major accident (MA) or loss of essential service (LES) consequences. In doing so the boundary of, and all logical (i.e. network connection) entry/exit points to/from the IACS should be

determined. Note – by definition, all IACS assets will be under the responsibility of the IACS Responsible person.

Defining the IACS scope should be based upon a clear understanding of the associated MA and/or LES processes and how they are controlled and managed by the IACS assets. This association will normally be clear from, for example, process descriptors and other risk management processes. However, it will be necessary to have this understanding clearly documented prior to defining the IACS scope.

Note that defining the scope of the IACS, risk assessment and selection of countermeasures is usually an iterative process. Therefore, it is recommended that initially all assets are included whether or not they are associated with MA or LES processes and then the non-MA/LES associated assets are subsequently identified as non-MA/LES IACS once this has been confirmed, typically during the risk assessment phase.

The IACS assets to be included in the IACS scope could include, but are not limited to:

- Basic Process Control Systems (BPCS). Including (but is not limited to) DCS, PLCs, SCADA, HMIs / operator interfaces, remote assets, and any other similar programmable controllers used for real-time process control or low integrity risk reduction.
- Safety Instrumented Systems (SIS) within the scope of BS EN 61511 and other safety critical protection / mitigation systems. Including logic solvers, remote assets, HMIs / operator interfaces, and other similar assets used for real-time active process plant risk reduction included.
- Electrical Control Systems (ECS) including electrical control or data acquisition systems, HMIs / operator interfaces, programmable switchgear, drives, protection systems, etc.
- Process plant / electrical system sensors, actuators or other similar devices. Note that those that are connected solely by discrete I/O (i.e. not by network) are within the scope of the IACS but could be considered part of the associated control system for the purpose of cyber security risk assessment and application of countermeasures.
- Assets that support the BPCS, SIS and ECS, including data historians, domain controllers, engineering workstations, application stations (e.g. recipe, asset, advanced control managers) and network infrastructure assets such as switches, routers, firewalls etc.
- Note that where assets (e.g. operator interfaces), are implemented in virtual machine environments both the server and the client assets should be included.
- All network connections within the IACS (both permanent and temporary) between all IACS assets and the other systems, including identification of the protocols that are used (e.g. TCP/IP over Ethernet, serial over RS485, proprietary, fieldbus, wireless instrument networks etc.)
- All network connections (both permanent and temporary) to systems outside the IACS boundary. This should include consideration of any connections made to other external networks such as corporate or third-party networks, dial-up / external access and any wireless connections used within the IACS.

- Supporting services necessary for the above systems, e.g. fire and gas detection, power, HVAC, and VoIP communications etc.
- Associated software services such as business systems, databases, cloud services etc. that are required for control of major accidents and / or loss of essential services.
- Standalone or 'air-gapped' systems
    - The term 'air-gapped' is often used for systems that have no physical network connections to other systems. For example, an IACS would be considered 'air-gapped' from another network if there were no network connections between the IACS and any other device that was connected to that other network. This does not however eliminate the risk, as for example, malware can still be imported via USB drives and maintenance laptops, and therefore countermeasures need to be applied. Therefore, the IACS scope should include any air-gapped systems so that these countermeasures can be selected and managed.

Once the IACS assets have all been identified, they should be organised into zones and conduits (for further guidance IEC/TS 62443-1-1).

Definition of the number of zones and how assets are grouped into zones should be considered on a case-by-case basis depending upon relevant factors, such as: the size and scope of the IACS, criticality and function with respect to the MA and/or LES process, geographic or logical location, required access (for example, least privilege principles), corporate standards or the department or organisation responsible for particular assets.

The zones should be defined in a hierarchical structure such that a defensive architecture can be achieved i.e. connections to external systems at higher levels in the hierarchy and more critical control and safety zones lower in the hierarchy (therefore least susceptible to cyber threats from the external systems).

The grouping of assets into zones should minimise the need for real-time data communications between the zones, i.e. each zone should be self-sufficient as far as is practicable, to facilitate the application of the countermeasures (e.g. network segregation) without compromising operational needs and minimising communication paths that span the IACS network.

Zones should consequently be defined (in part) to include assets where the same cyber security countermeasures will be required. The zone definition may need to be adjusted following the risk assessment or definition of countermeasures as part of an iterative process.

Typical zones include:

- Control systems zone(s). The control systems zones should be defined to include all BPCS systems.
- Safety systems zone(s). The safety systems zones should be defined to include all SIS and other safety-critical protection / mitigation systems.
- Electrical system zone(s). The electrical systems zones should be defined to include all ECS.

- Other zone(s). Other zones that include relevant assets may be defined, for example packaged systems etc.
- Plant information zone(s) (PIZ). The plant information zones should be defined to include assets that support the BPCS, SIS and ECS
- IACS Demilitarised zone (IACS-DMZ). It is sometimes good practice to define a top-level in the hierarchy as a DMZ (sometimes also referred to as a perimeter network) used to connect to external networks such as the corporate network to allow access to specific services (typically historian data etc.).
- External zone(s), e.g. Corporate / Third Party. These zones are normally (but not always) outside the IACS. External zones that are connected to the IACS are normally shown on the simple network drawing so as to clearly show the connections between these zones and the IACS.

Once the zones have been identified, conduits can be defined where ever there is communications between zones:

- Internal conduits(s), i.e. communication connections between IACS zones.
- External conduit(s), i.e. communication connections to external systems outside of the identified IACS boundary.
- No conduits are to be defined within an individual zone.
- Conduits should include any network connections that are not physically contained within a zone, for example wireless connections.
- Conduits should include non-network communications between zones, for example using portable media or devices (such as USB media, laptops) that are used to allow data to be transferred between zones.

For most sites where there is at least one external connection (e.g. to the corporate network) then it is expected that there will normally be at least a control system zone, a safety system zone and a plant information zone.

Examples of definition of zones and conduits are shown in
Appendix 3: Example Simple Network Drawings. There is also further guidance in IEC/TS 62443-1-1.

Output of this Step

The definition of the IACS should be documented as the IACS simple network drawing(s) showing the IACS zones and conduits. It may also be necessary to capture basic information about some of the assets and conduits for the purposes of risk assessment – some of this data will subsequently form part of the IACS Asset Register (see Appendix 2 A3 for the expected minimum content of an asset register).

With respect to the IACS Simple Network drawing:

- It should be sufficient to allow risk assessment, i.e. showing the general network architecture, how assets are connected to each other and connections to other networks
- It should show connections to (and any relevant aspect of) non-IACS zones (e.g. the corporate network)
- Note that typical system architecture drawings (as normally already available) are not generally suitable as simple network drawings as they are not for the

same purpose, although they could be used as a basis for such a drawing. A simple network drawing will typically not show as much technical detail, but will show the wider IACS scope and connections, zones, boundary etc. that is necessary for the purpose of risk assessment and deployment of cyber security countermeasures.

- Additional information that may be required which could be either shown on the simple network drawing or as separate tabulated data.
    - Basic network connectivity arrangements (e.g. connection type, protocols, data type etc.)
    - Expected data flows for conduits to allow data flow rules to be defined.
    - Any temporary connections such as portable assets (e.g. laptops) and assets where portable media connections are required / used.

Note 4 – Risk Assessment

Purpose

The purpose of this step is to assess the risk profile of each IACS zone based upon the IACS simple network drawing sufficient to allow appropriate and proportionate countermeasures to be defined (see Note 5). In this guidance the risk profile is considered to be a function of the consequence that could potentially be realised if the zone were compromised and the criticality of the assets within that zone.

Background

Since it is only necessary to determine which countermeasures are to be applied at the IACS zone level, the risk assessment should also be targeted at the zone level, i.e. there is no intention at this stage to carry out cyber security risk assessment for each MA / loss of essential service scenario.

Traditional, e.g. safety, risk assessment processes determine the potential consequences for a range of initiating events (e.g. due to equipment, control or human failure) and their likelihood. The scope and integrity of risk reduction measures necessary can then be specified to reduce the risk to the required level.

For cyber security threats, it is more difficult to determine the specific potential consequence of each threat or its likelihood without detailed analysis on an on-going basis as threats, and vulnerabilities to threats, change over time and past history is no indication of future likelihood.

It has been recognised that there are some IACS that are more critical in preventing MA and/or LES consequences. For example, SIS provides significant risk reduction against MA and both BPCS and SIS provide significant risk reduction against LES. (Note that for the purposes of this guidance, SIS shall include high integrity (PFD<0.1) layers of protection and other safety-critical protection / mitigation systems of undefined integrity and any other systems that are capable of defeating or otherwise causing them to fail dangerously.)

The approach adopted in this guidance therefore allows for identification of proportionate expectations for countermeasures in order to provide:

- a minimum benchmark against which to assess the suitability and sufficiency of a duty holder's risk assessment(s);

- an example approach to the assessment of risk (see appendix 4);
- an objective basis for expected countermeasures (see Note 5).

Approach

The duty holder should complete an assessment that determines the risk profile, without taking credit for any existing cyber security countermeasures, if there are potential MA and/or LES (as applicable) consequences associated with each zone and, if so, the criticality of the zone in preventing those consequences.

It should also be noted that in future it may be appropriate to consider not just if there are potential MA and/or LES consequences, but also to consider a range of consequence levels and apply more robust controls in a proportionate manner to higher consequence zones (see appendix 4 'Future Direction' for further information)

To carry out a suitable and sufficient risk assessment will typically require a range of competencies. This might include the IACS Responsible Person, IACS system vendor representatives and other specialists. It should be recognised that some members of the team, e.g. with IT specialist skills, may not have an understanding of the plant and associated processes and other documents and description will need to be provided, e.g. a simple process overview diagram showing how it connects to the IACS.

There are a range of approaches to risk assessment that could be adopted by the duty holder and the output of the assessment could be recorded in different ways (e.g. bow-tie diagrams, reports, annotated drawings, registers or a simple tabular format as shown in the example in appendix 5).

Inspectors should assess the adequacy of the duty holders risk assessment by considering if the duty holder's risk assessment has resulted in the expected countermeasure (see note 5).

Note that a duty holder may optionally have chosen to consider business continuity or data protection risk. But the assessment should show how MA and/or LES risk (as appropriate) has been considered in some way to demonstrate that appropriate and proportionate countermeasures have been selected.

Output of this Step

The output of this step should be a documented IACS risk assessment – the following should be noted.

- The risk assessment should show the risk profile for each zone, i.e.:
    - MA / LES consequences (as appropriate), and
    - The criticality of the zone in preventing these consequences
- The team members and their roles should be documented as part of demonstrating that the assessment was completed by competent personnel.

Note 5 – Define and Implement Countermeasures

Purpose

The purpose of this step is to define and implement appropriate and proportionate countermeasures to the IACS based upon the IACS Risk Assessment.

Background

There is a requirement to implement appropriate and proportionate countermeasures. With respect to technical countermeasures, this is interpreted as countermeasures that provide the zone with protection against foreseeable threat scenarios (i.e. appropriate) and where there is potential a MA and/or LES consequence relevant to that zone (i.e. proportionate).

With respect to organisational countermeasures (i.e. CSMS requirements within appendix 2) these should be applied where appropriate to ensure that the technical countermeasures are managed throughout their lifecycle and to achieve overall management of cyber security.

Approach

The duty holder should define countermeasures for each IACS zone (or for the IACS as a whole) where there is potential MA and/or LES consequence relevant to that zone, and the countermeasure would reduce the cyber risk of that zone.

Cyber security technical countermeasures are described in Appendix 5 which includes the countermeasures normally required along with optional alternative countermeasures to be considered when the required measures cannot be applied.

It may be necessary to modify the definition of the zones and conduits, for example to move assets associated with MA or LES consequences to a different zone to target the countermeasures appropriately. However, this must be balanced with operational performance requirements (e.g. time-critical data transfer between assets) and for management and standardisation etc. Any changes should be reflected in the IACS Simple Network Drawing and IACS Asset Register.

All required countermeasures should be managed by the IACS Responsible Person. For example, if remote maintenance is required, a controlled environment could be established from within the IACS boundary and its use managed under the CSMS.

To achieve defence in depth, a range of both protective and, detect and respond countermeasures are required. When duty holders are implementing the required countermeasures, protective countermeasures should be implemented first (e.g. identity access controls) followed by implementing the detect and respond countermeasures (e.g. security monitoring and incident response).

There are often also ‘quick-wins’ that are clearly reasonably practicable (typically they would be things like physical access controls, USB and network port blocking, disabling of unused network switch ports, changing of default passwords and enforcement of password policies) that can be readily implemented.

No single countermeasure provides absolute protection as new threats and vulnerabilities can be identified at any time. To reduce these risks, implementing multiple countermeasures in series, i.e. defence in depth, avoids single point failures.

It may not be practicable to implement some of the required countermeasures (as shown in appendix 5), especially for existing systems e.g. due to their proprietary nature or age. In such cases alternative countermeasures (e.g. the 'optional' countermeasures shown in appendix 5, or more robust 'required' countermeasures) to address the remaining risk should be considered and in particular to ensure that no serious deficiencies remain.

For any remaining gaps, the justification for not implementing any countermeasures, and other countermeasures considered etc. should be approved by management and recorded including records made to ensure that the countermeasures are considered in any future system upgrade projects or managed as part of obsolescence management.

The cyber security landscape including the range of countermeasures available changes frequently and therefore the IACS Risk Assessment including countermeasures should be reviewed periodically and as required (see appendix 2 A2).

Inspectors should assess the adequacy of the duty holder's definition of required countermeasures against the expected countermeasures shown in appendix 5, table 5.2 considering the range of threat scenarios (see appendix 5, table 5.1) that will be applicable to the zone. This will also indicate if the duty holder's risk assessment process was adequate.

Note that implementation of countermeasures to the SIS should be incorporated into the defined SIS lifecycle (see BS EN 61511 edition 2) for both new and installed SIS. Additional guidance is provided in "ISA-TR84.00.09-2013- Security Countermeasures Related to Safety Instrumented Systems".

<u>Output of this Step</u>
The output of this step should be:

- an updated IACS Risk Assessment (or associated documents) showing:
  - the countermeasures required for each zone linked to the threats that are addressed by the countermeasure;
  - the countermeasures in place for each zone;
  - the countermeasures not in place for each zone along with either:
    - plans for their implementation,

    or, if the required countermeasures will not be implemented (e.g. for existing systems):
    - what other countermeasures have been applied to achieve the equivalent level of protection
    - justification for not implementing any further measures, approved by management,
    - records made to ensure that the required countermeasures are implemented in any future system upgrade projects (e.g. as part of obsolescence management systems).

- a revised IACS simple network drawing and IACS asset register based on the countermeasures deployed as a consequence of the risk assessment;
- verification that no serious deficiencies remain in the countermeasures in respect of the MA and/or LES consequences.

Glossary of terms

ATG	Automatic Tank Gauging System
BPCS	Basic Process Control System
CA	Competent authority (as defined in the relevant regulations e.g. COMAH or NIS)
CCR	Central control room
COMAH	Control of major accident hazard
Corporate Network / Systems	Networks and systems that provide corporate IT functions such as email, web, file services and other corporate functions. Also, sometimes known as Enterprise Networks and Systems.
CSMS	Cyber Security Management System
DCS	Distributed Control System
DMZ	Demilitarised Zone – a DMZ is a physical or logical sub network that contains and exposes external-facing services (in this case limited IACS services) to a larger and less trusted network (in this case normally the corporate network which is connected to the internet). The purpose of a DMZ is to add an additional layer of security. If properly configured, an external attacker would only have direct access to equipment in the DMZ, rather than any other part of the network.
Duty holder	The person(s) or corporate body that has legal duties under relevant health and safety legislation or NIS Regulations. In the context of this guidance it will typically be the IACS owner or the IACS operator.
ECS	Electrical control system
EEMUA	The Engineering Equipment and Materials Users' Association
External Network / System	Networks or systems that are outside the defined IACS scope, for example corporate or third party
FAT	Forensic analysis tools
FTE	Fault Tolerant Ethernet
HAZOP	Hazard & Operability Studies
HMI	Human Machine Interface
HSE	Health & Safety Executive
IACS	Industrial Automation and Control System including Safety Instrumented Systems
ICS	Industrial control system
IDS	Intrusion detection system
IPS	Intrusion prevention system
IT	Information Technology
LAN	Local Area Network

LES	Loss of essential service (an incident resulting in reduction or disruption of service provision by an OES)
MA	Major accident (as defined in legislation (excluding NIS) shown in the 'relevant regulations' section of this operational guidance)
Major accident workplace	Any place regulated under the legislation (excluding NIS) defined in the 'relevant regulations' section of this operational guidance
NAS	Network attached storage
NIS	Network Information Systems
OES	Operator of essential supplies (as defined in the NIS Regulations)
OT	Operational technology
PFD	Probability of Failure on Demand
PHR	Process Hazard Risk Analysis
PIZ	Plant information zone
PLC	Programmable logic controller
Responsible Person	Person or group of persons responsible for IACS cyber security (typically not under the management controls of an IT department)
RDP	Remote desktop protocol
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrity Level
SIS	Safety Instrumented System
Threat	Any circumstance or event with potential to adversely impact the IACS
Virtual Machine Environment	An instance of an operating system (which could be a thin-client or full operating system, for example running a SCADA operator interface application), running in an isolated partition of a computer to allow multiple applications to run at one time without interfering with each other. The virtual machine may be part of the IACS and therefore measures should be taken to protect the cyber security of the IACS.
VLAN	Virtual Local Area Network
VPN	Virtual private network
Vulnerability	Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security
WLAN	Wireless local area network (also known as Wi-Fi)

Reference should also be made to IEC/TR 62443-1-2 for a full definition of terms and abbreviations used in this document.

Appendix 2: Cyber Security Management Systems

The section contains the organisational countermeasures, including those required:

1. To achieve overall management of cyber security, for example governance, risk management, asset management, supply chain management, staff awareness and training and minimising the impact of cyber security incidents etc., and
2. To ensure that associated technical countermeasures are appropriately managed, for example requirements to manage identity and access controls, data security, system security and resilience, security monitoring etc.

A. Managing security risk

A1 Governance

A formal governance framework should be established to ensure:

- senior management commitment, leadership, and risk ownership
- communication of the requirements, e.g. through appropriate policy
- oversight with respect to IACS cyber security including monitoring (e.g. by KPIs) and review (e.g. at senior management meetings) and assurance from senior management that IACS cyber risks are managed.
- security culture that ensures that IACS cyber security risks are managed on an on-going basis.

In addition, procedures should be in place for the following:

- definition of employee and third-party roles and responsibilities for IACS cyber security. This will include all personnel who have physical or logical access to the IACS. Groups of personnel may be defined rather than individuals where appropriate based upon role;
- briefing of employees and third parties of their roles and responsibilities;
- Note – it is important that the role of the 'IACS Responsible Person' (person or group of people responsible for IACS cyber security) should operate under the IACS CSMS rather than a general IT management system;
- definition of how cyber security risks will be assessed recognising the potential MA and/or LES consequences (as applicable) relevant to the site, decisions made regarding the required countermeasures and cyber security risks managed.

Evidence to demonstrate this aspect of the CSMS could include:

- cyber security policy (may be part of the Major Accident Prevention Policy for COMAH sites)
- records of monitoring (e.g. KPIs) and senior management review
- role and responsibility descriptions
- risk assessment processes

A2 Risk management

Procedures should be in place for the following:

- defining the scope of the IACS
- risk assessment by a competent team – assessing the risk profile of the IACS considering potential consequences (MA and/or LES as appropriate) and the criticality of the IACS in preventing the consequences.
- defining appropriate and proportionate cyber security countermeasures based upon the risk assessment and the vulnerability of the IACS to relevant threats.
- review of the IACS risk assessment to ensure it remains valid and identifying improvements that can be made to countermeasures and/or to the overall CSMS.
    - periodically (with the period reflecting the fast-changing nature of cyber security), and
    - as required (i.e. when changes proposed, following an incident, changes to the risk landscape such as knowledge of vulnerabilities, awareness of threat information etc.)
- documenting and retaining the outcome of the risk assessment / review along with responsibilities and time-bound plans for the implementation of any identified improvements.
- ongoing demonstration and assurance of the cyber security countermeasures in place such that their effectiveness is monitored, reviewed and any issued remedied.

See also note 4

Evidence to demonstrate this aspect of the CSMS could include:

- Risk assessment records
- IACS drawing(s)
- Risk assessment review records and improvement management plan

A3 Asset management

Procedures should be in place for the following:

- defining responsibilities for identifying, recording and managing IACS assets (e.g. as a simple network drawing and asset register(s)).
    - all IACS assets should be under the responsibility of the IACS responsible person and managed under the IACS CSMS, e.g. with respect to patch management, configuration management, change management etc.
    - This includes all assets required for the protection of the IACS such as perimeter devices for external IACS conduits. However, it is accepted that, especially for connections to corporate networks there can be an element of joint responsibility with corporate IT departments so long as these assets are managed under the IACS CSMS. For example – management process should ensure that a change to an IACS firewall / DMZ connected to the corporate network cannot proceed until the IACS change management process has been followed.

- to ensure that the asset register includes all relevant MA / LES IACS assets (see notes 3 and 4).
- recording relevant information about the IACS assets sufficient for the purposes of managing the assets (e.g. patching, management of change, incident response etc.). Relevant information to be included:
  - Unique identifier, location and zone reference
  - Asset / conduit type, manufacturer, serial number etc.
  - Relevant risk profile and/or criticality information (e.g. risk-level, restore criticality, known vulnerabilities such as untreated CVEs etc.)
  - Responsible Person (where responsibilities are divided, e.g. between different departments)
  - Network connectivity arrangements (e.g. addresses, ports, connection type, network protocols, encryption algorithms etc.) for each network connection.
  - For assets each network connection type should be included, e.g. for multi-homed assets, or other (e.g. fieldbus) connections.
  - For conduits (typically a firewall, router etc.) – each connection to other zones should be included.
  - for conduits – expected data flows to allow data flow rules to be defined.
  - Any temporary connections such as portable assets (e.g. laptops) and assets where portable media connections are required / used.
  - Firmware, operating system, and application software (including security software such as AV) types and versions (could be part of another system rather than the asset register but should be recorded)
- managing assets (including network devices) throughout their lifecycle, in particular obsolescence – recognising that industrial assets tend to have much longer operational lifespans than commercial IT systems. This should include producing decision making processes and plans / roadmaps.

See also note 3

Evidence to demonstrate this aspect of the CSMS could include:
- IACS simple network drawing(s)
- asset register(s)
- plan for ageing and obsolete hardware and software

A4 Supply chain

Procedures should be in place for the following:
- identifying third parties (including sub-contractors) that provide equipment, software, services (including by any remote connections) etc. that potentially result in cyber risk to the IACS and specifying the roles that they perform.
- specifying the cyber security requirements for these third parties including:
  - management (e.g. access controls, hardening, AV, personnel screening etc.) of any supplier devices and personnel connected to the IACS.
  - management (e.g. configuration management, AV etc.) of any devices following purchase or repair

An intelligent customer approach should be adopted. Trusted third parties (e.g. the original equipment manufacturer or vendor etc.) should be used where possible, especially for the supply of equipment or software

- periodic assessment and assurance of the suitability of third parties providing IACS services or components with respect to the cyber security requirements
- ensuring the protection of data shared with the third party
- Note – it may be useful to consider any connected non-IACS networks (e.g. corporate networks) as a third party (to the IACS) and treat as above.

Evidence to demonstrate this aspect of the CSMS could include:

- List of third parties used, their roles and responsibilities
- Definition of cyber security requirements for the third parties
- Reports of completed assessment and assurance of third parties

B. Protecting against cyber attack

B1 Protection policies and processes

Procedures should be in place for the following:

- Suitable procedures should be documented and implemented for all activities that are required to ensure the countermeasures are appropriately managed.
- security screening of new and existing personnel with IACS roles (see also IEC62443-3-1 clause 10.2):
  - Verification checks (character references, verification of qualifications, CV and identity) prior to (internal or external) appointment to an IACS role.
  - More detailed verification (e.g. criminal records, credit review, security clearance) should be considered for roles with more privileged access to the IACS where it is legally permitted.
  - Defining employment terms and conditions setting out confidentiality, legal, equipment and information handling requirements, disciplinary procedures etc.
  - Monitoring of performance, behaviour and conflict of interests with respect to cyber security responsibilities
  - Managing those leaving IACS roles including access to IACS equipment and systems
- configuration management of IACS assets such as:
  - network device configuration, e.g. firewall configuration, switches, routers (see also appendix 5 B4)
  - encryption devices like Wi-Fi access points, VPN etc. including encryption key distributions, rulesets and definitions
  - recording and maintaining of secure configuration checksums, device settings, versions etc.

  Configuration management should include details of the reason for configurations and version control to allow ongoing management and auditing.
- management of change processes for the IACS including authorisation, assessment and control of changes such as additions, changes to settings,

patching / updating of software, organisational change etc. IACS change control records should be retained;
- Implementation – validation testing of countermeasures installed as part of new projects, modifications, replacement or retrospective upgrade of installed systems. The testing should ensure that the measures provide the necessary cyber security and availability (through the use of redundancy and diversity where necessary) – see also appendix 5 C2)
- periodic audit and review of the CSMS policies and procedures. The outcome of the audits and reviews should be documented and retained and where necessary the CSMS should be modified in order to ensure that it remains effective as organisations and technologies change and develop;

Evidence to demonstrate this aspect of the CSMS could include:
- published and controlled policies, procedures and work instructions etc.
- personnel security records (recognising data protection requirements)
- configuration records (e.g. for firewalls, etc.)
- management of change records
- organisational and procedural change control records
- validation test records
- audit reports, review reports and management of resulting actions

B2 Identity and access control

Procedures should be in place for the following:
- recognising the external and insider threat and taking measures to minimise this risk by minimising physical and logical access to the IACS
- to define and periodically review users (or groups of users) and assets (for device to device communications) that are authorised for logical access the IACS, for example per zone, and removal of rights and return of equipment etc. following termination of employment or change of role etc.:
    - Authorisation to be based upon the principle of least access, i.e. permitting only necessary access with the appropriate level of privilege to fulfil the required roles / responsibilities.
    - Assets should include servers, workstations, real-time assets / controllers etc., network devices, and applications where applicable
    - The definition should include which assets (or groups of assets) for which a user, group, device or service (e.g. remote access) is authorised. This could be completed by zone or zone type (e.g. all BPCS zones) where appropriate.
    - As a minimum, authorisation requirements for plant operators, engineers and systems administrators should be defined.
    - Any third parties (e.g. vendor) authorisation should also be defined.
- to define the authentication methods to be used and how passwords, certificates and physical tokens etc. will be securely stored, distributed and managed
    - Where existing systems do not have adequate authentication methods (e.g. limited authentication methods or hard-coded passwords) then alternative countermeasures should be considered to minimise access.

- to define authorisation and additional authentication methods (e.g. multiple-factor) for remote access and the assets that permit such access.
- to define which assets are authorised for use for administrative tasks.
- for devices or services connecting from outside the IACS boundary, define and assure cyber security requirements for these networks (this could be achieved by considering these as part of the supply chain – see A4)
- for highly privileged access the following should be considered:
    - Separate administrator accounts that are only used when required. Also consider making these accounts temporary or time limited etc.
    - Multiple factor authentication and / or accounts useable from limited assets only.
    - Splitting access to highly privileged functions (e.g. install apps, transfer apps, change security settings) across multiple roles so that one person alone cannot breach security.
- to define and periodically review users or groups of users that are authorised for physical access the IACS based upon the principle of least access, i.e. only permitting those who need physical access to carry out their role and removal of rights and return of keys etc. following termination of employment or change of role etc.
    - Note – this may require changing any shared device credentials when personnel leave a role.
- to define physical access control measures required to prevent, limit or monitor access to IACS systems to those authorised and management of these measures (e.g. of physical key controls or electronic access control systems)

See also appendix 5 B2.

Evidence to demonstrate this aspect of the CSMS could include:

- authentication and authorisation approach definition (including for remote and highly privileged access)
- records of current authorised users / assets and the level of access / privilege etc. (noting data security requirements)
- records of change management for users, control of physical tokens / cards etc.
- records of physical access control authorisation and physical access control measures, e.g. key distribution or electronic access control records

B3 Data security

Procedures should be in place for the following:

- specification of how sensitive data about the IACS that might be useful to an attacker is minimised, stored, protected (for example encrypted in transit and at rest) and shared only as required.
    - e.g. network drawings, risk assessments, configuration records, asset registers, backups, firmware, application programs, and other software, staff information and other information etc.

    - Note – it is not sufficient to protect sensitive data purely using logical access controls, for example, a shared network resource on the corporate network where access is controlled by login credentials alone.
- specifying how IACS data that is not physically protected, i.e. potentially accessible outside of the IACS secure area (e.g. data on IACS mobile devices and media, wireless networks, wireless instruments, radio, satellite or public networks including remote connections) is protected, for example encrypted.
- Selection and generation of appropriate key algorithms and key length (note the keys themselves should be appropriately protected also) that are secure, noting that some algorithms / key lengths have been cracked.
- management of encryption countermeasures to be used where required for protection.
- Identification of essential data, data services, data connections etc. that are required to safely and securely operate and protection of these to ensure that they are available in the event of cyber-attack or fall-back methods are defined and tested. For example, back up access to operating procedures stored on the external networks and systems, fall-back method for e-permit systems, backups to VOIP phones, and access to known good backups and firmware.
- It should be noted that any wireless access is always vulnerable to denial of service attacks and there is little that can be done to prevent this. In these cases, consideration should be made of any necessary fall-back methods necessary to operate during a denial of service attack.
- Periodic validation of the above to ensure that data remains secured.

See also appendix 5 B3.

Evidence to demonstrate this aspect of the CSMS could include:

- Relevant procedures for identification of sensitive data and assets containing this data and how this is protected.
- Specification of encryption algorithms and keys used
- Records of essential data, services and connections identified and how these are protected where required.

B4 System security

Procedures should be in place for the following:

- specifying an IACS system architecture that provides a defensive architecture (for example based upon the Purdue model – see appendix 3 for examples) segregated into zones based upon risk with simple known data flows between different zones.
- specifying appropriate network segregation and access countermeasures to protect the IACS networks and zones.
- Defining how operation and maintenance tasks are completed, including for example:
    - file transfer and use across the IACS boundary via portable media or designated network connections including use of designated clean

devices, pre-scanning, limiting IACS assets used and authorisation (e.g. split roles) etc.
    - temporary access e.g. via laptops and how these assets are controlled
    - remote access facilities from outside the IACS boundary including how these are implemented, access limited, controlled and monitored and what countermeasures are required for securing.
    - repair and replacement of faulty equipment
    - relevant IACS operation and maintenance records should be retained.
- specifying IACS asset hardening requirements, recognising the need to secure a system by reducing its inherent vulnerability.
- awareness of current relevant IACS vulnerabilities and threats and recent relevant incidents in the industry to inform patch management
    - for example, by subscription to US ICS-CERT (ics-cert.us-cert.gov/)
    - it is recommended that sites participate in CiSP for sharing threat intelligence (www.ncsc.gov.uk/cisp)
    - other forums are also available, e.g. vendor vulnerability websites
    - understand vulnerabilities present (e.g. by testing when appropriate)
- Management of security updates (patch management). This should include:
    - recognition of the conflict between disruption to safe and reliable plant operation and protecting assets from ever-changing threats in determining patching processes, frequency and scheduling
    - recognition of patching requirements for operating systems, firmware and all other application software on all assets including network devices.
    - use of authentic, vendor-sourced, validated and approved patches and review and internal testing of patches before full roll-out
    - patching decisions (and records) based upon vulnerability and exposure reviews, threat information, appropriate vendor information, urgency and cyber security risk
    - patching externally exposed assets (e.g. those higher in the hierarchy such as historians, servers, portable devices, engineering stations etc.) more frequently than operational assets such as controllers.
    - patching some assets (e.g. redundant operator stations, training systems, test beds) more frequently to permit testing and to make at least some operator stations more resilient to attack.
    - identifying additional countermeasures to protect obsolete / un-patched software
    - authorisation of personnel carrying out updates including transfer of data (e.g. by portable media), and associated administrative tasks (split-roles may be considered)
    - methods for patching including fall-back and recovery methods if patching fails or causes issues.
    - management of any potential changes through appropriate change management processes.

See also appendix 5 B4.

Evidence to demonstrate this aspect of the CSMS could include:

- Procedures setting out requirements for network architecture, segregation and access.
- IACS simple network drawings

- Asset hardening procedures / instructions / templates
- Vulnerability / threat records
- Patch management procedures and records and associated change management records

B5 Resilient networks and systems

Procedures should be in place for the following:

- identification of key limitations, constraints or weaknesses (e.g. single points of failure) in the IACS critical systems that would result in loss of MA risk controls (and/or essential services as appropriate), for example network connections, IACS assets, etc. and plans (e.g. redundancy / backup) where necessary to address this risk. Note – for MA sites (where the critical systems are likely to be SIS, this may have already been covered as part of functional safety)
- disaster recover / continuity plans to include:
  - backup / restoration strategy for IACS assets
  - the strategy should consider criticality of assets – i.e. how quickly they need to be restored to firstly achieve safety and, for OES, to provide essential services (as applicable)
  - the strategy should allow recovery from a range of scenarios from hardware component failures through to total loss of IACS (e.g. following a ransomware attack) where applicable
  - the strategy should consider a range of restoration options and restoration order / timing depending upon the criticality – from installed standby equipment in other locations, hardware spares and software backups through to equipment that is not backed up (and would be rebuilt from accurate design specifications).
  - the strategy should consider the relevant competence and personnel requirements necessary to allow restoration.
  - secure online and offline backup storage including relevant configuration data, known good firmware, applications etc.
  - restoration testing where appropriate (based upon the strategy) considering a range of scenarios including hardware component failures, recovery on different hardware, recovery on current software versions, recovery from total loss of network etc. to ensure that backups or relevant assets are useable and can be restored within the necessary time.

Evidence to demonstrate this aspect of the CSMS could include:

- Records of review of limitations, constraints and weaknesses
- Disaster recovery strategy
- Software/firmware/application/configuration libraries and safes
- Restoration test records

B6 Staff awareness and training

Procedures should be in place for the following:

- social engineering – recognising that people are one of, if not the most, significant vulnerability but also the first line of defence;
- management of cyber security competence (definition of requirements, providing necessary training, knowledge and experience and ongoing verification including refresher where appropriate) of employees and third parties with IACS responsibilities relevant to their defined responsibilities;
- more widely implemented cyber security awareness training and promotion of a positive cyber security culture which includes making staff aware of the importance of the IACS systems and their cyber security countermeasures, communication and reporting of cyber issues.

Evidence to demonstrate this aspect of the CSMS could include:

- Definition of competence requirements for defined IACS roles and responsibilities
- Cyber security awareness training programme
- Competence management records

C. Detecting cyber security events

C1 Security monitoring

Procedures should be in place for the following:

- recognition of how security monitoring linked with threat intelligence is used to identify potential security problems and inform the security monitoring strategy.
- specify requirements for security monitoring of IACS assets such that the types of data to be analysed can be defined along with the reason why the data is important. Security monitoring should include the security alerts / events from the assets deployed that would indicate that a countermeasure has failed or been compromised – based upon a review of the countermeasures deployed. This could include, for example:
    - unauthorised assets connected to the IACS network
    - login failures and locked accounts etc.
    - access attempts from remote connections.
    - unauthorised activities by privileged (e.g. administrator) accounts such as security policy changes, new / modified user accounts, access to security logs
    - alerts from security software, e.g. AV, IDS, whitelisting etc.
    - For key assets (e.g. domain controllers, engineering workstations, assets accessed from non-IACS networks, assets used for file transfer by portable media, perimeter devices):
        - high network traffic (at key points)
        - high CPU usage (key assets)
        - low disk space

        - large numbers of events generated in security logs
        - unexpected shutdowns or reboots
        - For perimeter devices – repeated denied connections, configuration changes, management console access
- specify requirements for security monitoring data aggregation (if required), secure storage and access (typically for privileged users only)
    - Note – assets often provide standard configurations that result in significant numbers of events being logged.
    - It is important that security events can either be filtered for analysis, otherwise important events can be lost within 'event-floods'.
    - However, all security data should be captured even if it is not routinely analysed as this more detailed data will be useful in the event of a cyber incident.
- specify requirements for malicious code detection (anti-virus - AV) software and (optionally) intrusion detection systems (IDS)
- periodic and timely updating of security software updates and definition (e.g. AV, IDS, etc.)
- periodically analyse, review and document the outcome of security monitoring
- periodic inspection or monitoring to reveal tampering or penetration of physical security measures, including any remote areas (see appendix 5 B2.2) and to ensure that the cyber security measures are in place and in order.
- review and oversight of above findings by a competent person and management of any necessary actions including liaison with other parts of the organisation and relevant agencies.

See also appendix 5 C1.

Evidence to demonstrate monitoring of cyber security could include:

- procedures setting out security monitoring requirements including malicious code detection
- records of periodic monitoring (e.g. of security logs, virus detection logs, intrusion detection logs etc.);
- analysis and interpretation of the threat intelligence and periodic monitoring records and management of resulting actions.

C2 Proactive security event discovery

Proactive security event discovery should only be used once good quality security monitoring (C1) is well established. These further measures could also be employed in situations where other required security measures could not be employed, where risk is particularly high or where a cyber incident is suspected.

Where used, procedures should be in place for the following:

- baseline checks to establish normal operation and subsequent monitoring to detect deviations from normal that would indicate compromise or failure of

countermeasures, e.g. network usage and connections, user access, security policy, services running, network connections etc.
- vulnerability scanning to identify security issues such as policy weaknesses, misconfiguration, software flaws etc.
- Enhanced testing such as penetration testing, to address specific concerns, e.g. threats from external networks to the IACS. Procedures should define the period, requirements, scope etc. Note that even simple scanning of low level assets like controllers may cause them to fail so testing should be well planned, limited and conducted when offline to minimise issues.
- enhanced monitoring / analysis – e.g. looking for specific events such as out-of-hours use, unusual network traffic, unexpected use of software or scripts. Also, targeted monitoring during suspected incidents.

See also appendix 5 C2

Evidence to demonstrate this aspect of the CSMS could include:
- relevant proactive security event discovery procedures
- analysis and interpretation of associated test and / or monitoring records and management of resulting actions.

D. Minimising the impact of cyber security incidents

D1 Response and recovery planning

Procedures should be in place for the following:
- development of a cyber incident response plan to include:
  - clear and concise articulation of the incident response plan that considers human factors, e.g. the stress of dealing with an incident.
  - recognition of the risks to the IACS based upon MA (and essential services where applicable) consequences
  - recognition of likely impacts on the IACS from likely attacks
  - definition of required roles and responsibilities, including any external (e.g. call-off) support and relevant government agencies. An incident controller / manager / single point of contact should be included.
  - how cyber incidents that may impact on the IACS are identified, reported and assessed and when the incident should be declared, e.g. following corporate network incidents, unexpected IACS behaviour / failures etc.
  - for NIS sites only – reporting requirement under Regulation 11 to inform NIS competent authority (NIS.Cyber.Incident@hse.gov.uk) of significant NIS incidents and noting that NIS incident could be as a result of a network information system failure (e.g. a safe failure of a SIS).
  - definition of tools, data and information necessary for incident response noting that systems may be offline or compromised, e.g. access to credentials required, backup systems, restoration files and media, procedures, communications.
  - pre-defined initial mitigation / containment measures based upon likely threats to be carried out to ensure continuing safety and availability. For example – disable remote access, limit (e.g. by predefined firewall rules)

or disable (e.g. by physical disconnection) access from the non-IACS networks, increase proactive monitoring etc. Note – the impact of such actions on essential services and operations (for example loss of external services to the IACS such as VOIP phones etc.) should be considered and work-arounds should also be provided but safety should be the primary consideration.
    - availability, collection and analysis of data / information and secure storage for during and post-incident analysis. A decision log should be kept.
    - escalation and recovery strategies to identify the source, minimise impact, contain and eradicate the attack.
    - requirements for declaration of end of incident and actions to prevent reoccurrence
    - Note – it is important to consider not just server and workstation assets but also other assets, especially network devices.
- periodic exercise of the incident response plan based upon credible and relevant cyber security threats and previous incidents (and exercises).
- Where formal emergency plans are required by legislation, the cyber incident response plan shall be part of the emergency plans and consideration shall be given to ensure that emergency response is not hampered by cyber security countermeasures (e.g. physical access controls). In addition, where site emergencies may compromise any countermeasures in place for cyber security, these should also be considered in the plan.

Evidence to demonstrate this aspect of the CSMS could include:

- Incident response plan
- Incident response exercise plans and records

D2 Lessons learned

Procedures should be in place for the following:

- following an incident or exercise conduct a root cause analysis to identify measures to prevent reoccurrence based upon incident (or exercise) data.
    - This may include technical or management system improvements.
    - Particular consideration should be made to security monitoring requirements.
- following an incident or exercise conduct a review of the incident response plan.

Evidence to demonstrate this aspect of the CSMS could include:

- Post incident / exercise root cause analysis
- Improvement management plan
- Evidence of review of incident response plans

Appendix 3: Example Simple Network Drawings

This appendix provides some examples of zone configurations for illustrative purposes only. **They do not provide 'accepted' architectures or good practice**, since the overall network architecture will depend upon the site risk, the network data flows and other factors, but are used to illustrate particular points as discussed in the accompying 'points to note'.

One of the main purposes of the simple network drawing is to facilitate the risk assessment and allow cyber security countermeasures to be applied to achieve defence in depth.

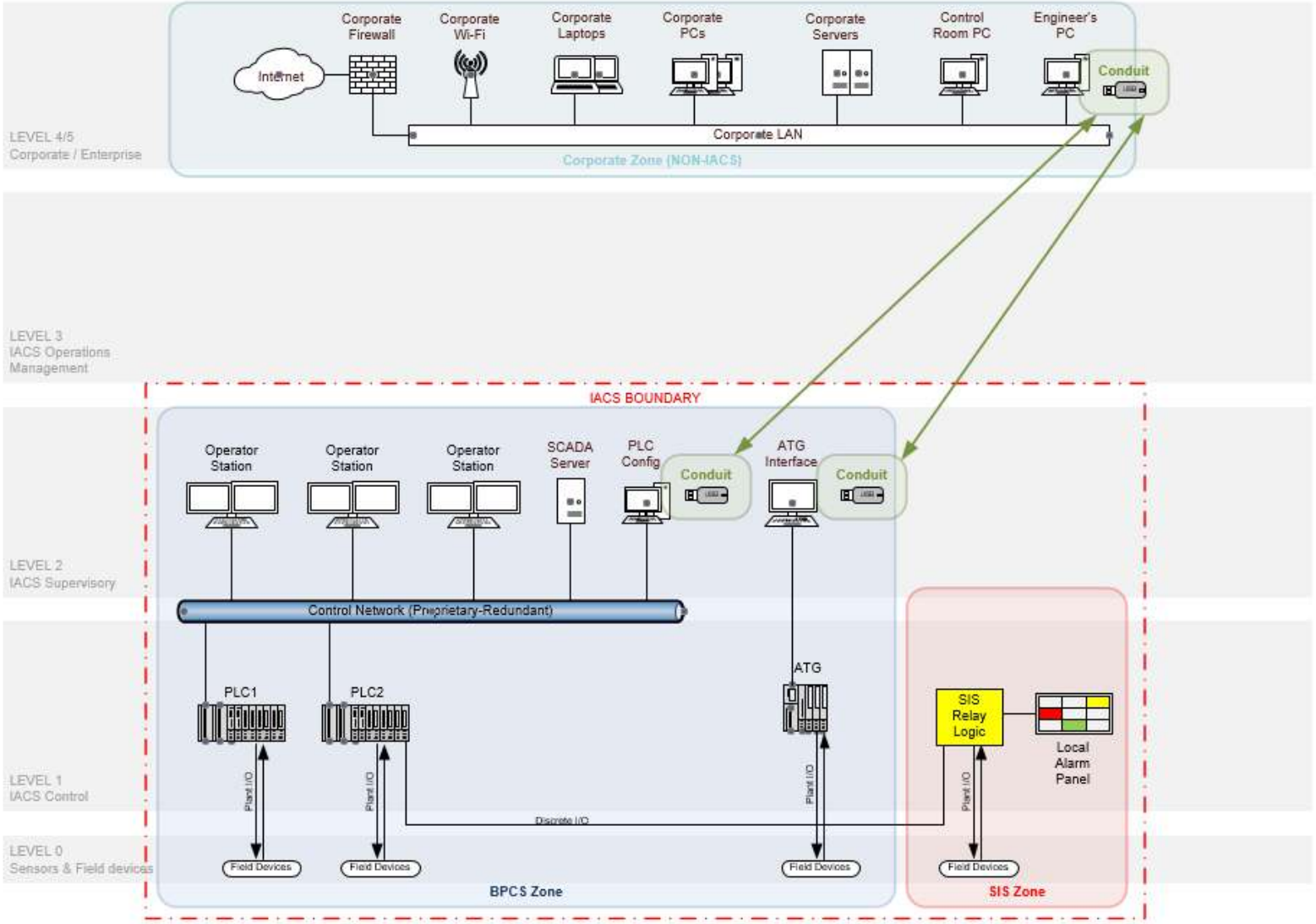
Therefore, the simple network drawing should be complete in that it shows the overall IACS architecture, the full range of IACS assets and associated connections, and helps understand data flows between the various IACS assets.

The drawing should also clearly show the IACS boundary, zone boundaries and any relevant conduits.

The simple network drawing does not need to show detail that is not necessary for its purpose. For example, it is not necessary to show every single asset of the same type, nor every single physical network connection, just logical connections. Such detail will generally be covered by a System Network / Architecture Drawing.

A Simple Network Drawing is to a System Network / Architecture Drawing in a similar way that a Process Flow Diagram is to a Piping and Instrumentation Diagram.

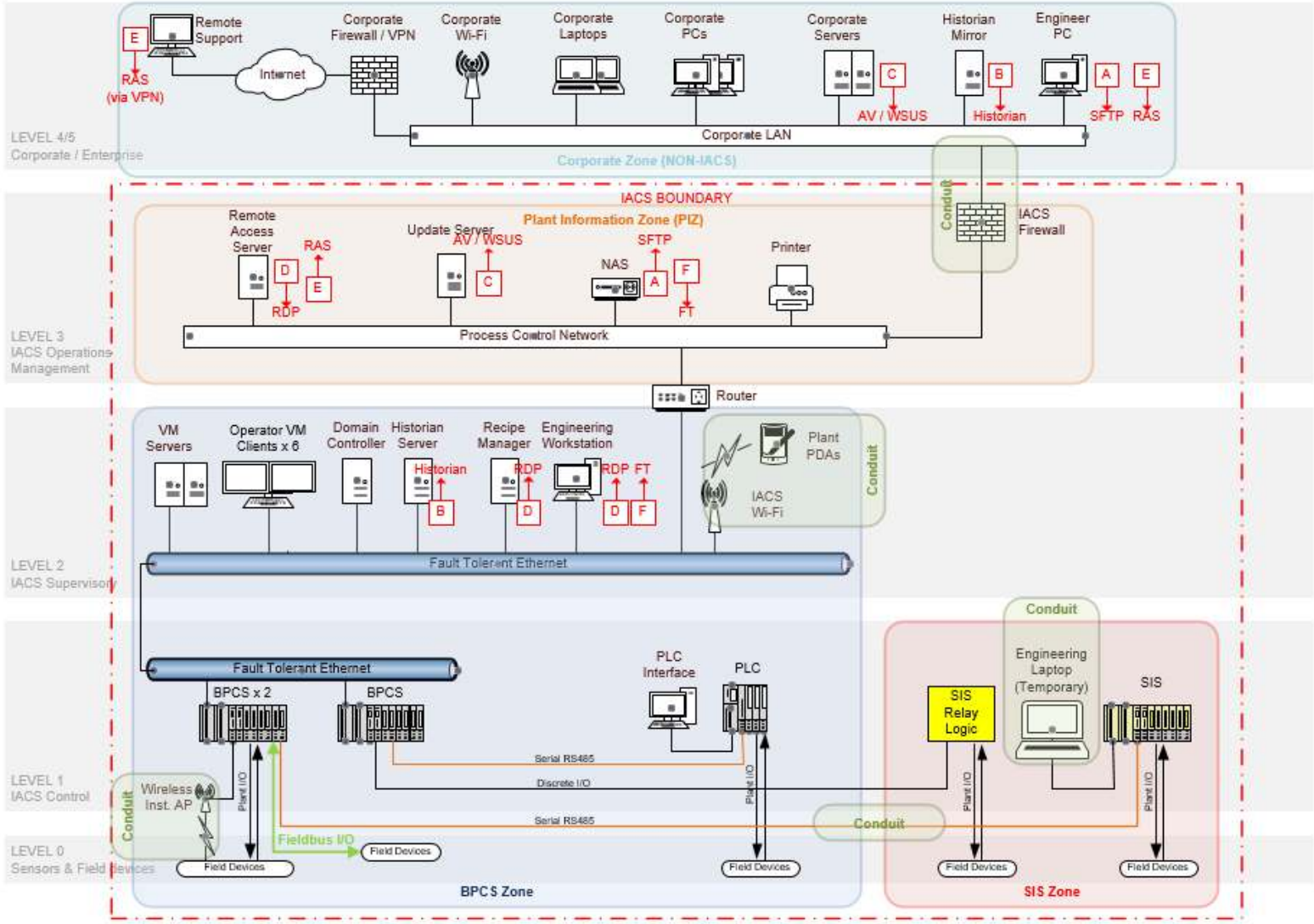
Figure 3-1 Small Site



Points to Note:

1. In this example for a small site there is a SIS zone and a BPCS zone. It is assumed that the BPCS and SIS zones are both associated with MA and/or LES processes.
2. Note that the field devices (e.g. sensors, actuators etc.) are included within the scope of the IACS.
3. There are no network conduits because there are no network connections between the IACS zones or to the corporate zone. Note that the discrete I/O shown is not a network connection but hardwired electrical connections (e.g. 4-20mA) and therefore not considered a conduit.
4. The corporate zone shows a control room PC that is used to provide office applications (email, business systems etc.) to the control room operators. Although this might be physically located next to the control room operator stations it is not part of the BPCS zone because it is not under the responsibility of the IACS responsible person and not connected to the IACS – zones should not be defined upon the physical location of the assets.
5. Even though the IACS is segregated ('air-gapped') from the corporate zone and internet, this does not mean that there is no risk from cyber threats.
6. On this drawing symbols have been added to depict that data transfer occurs via USB portable media between the Engineer's corporate PC and the IACS PLC Config workstation and ATG Interface workstation – this is an external conduit and a potential route for cyber threats to cross the IACS boundary.
7. Also, other unused USB ports and network interfaces (e.g. Wi-Fi, Bluetooth) on the operator stations or servers within the BPCS zone provide potential vulnerable points.
8. Therefore, although the network segregation aspects have been addressed by the air-gap, other technical countermeasures should be considered, e.g.:
    a. Physical and Logical Identity and Access control,
    b. System security including Network Architecture and Access, Asset Hardening and control the use of USB portable media etc.
    c. Security Monitoring

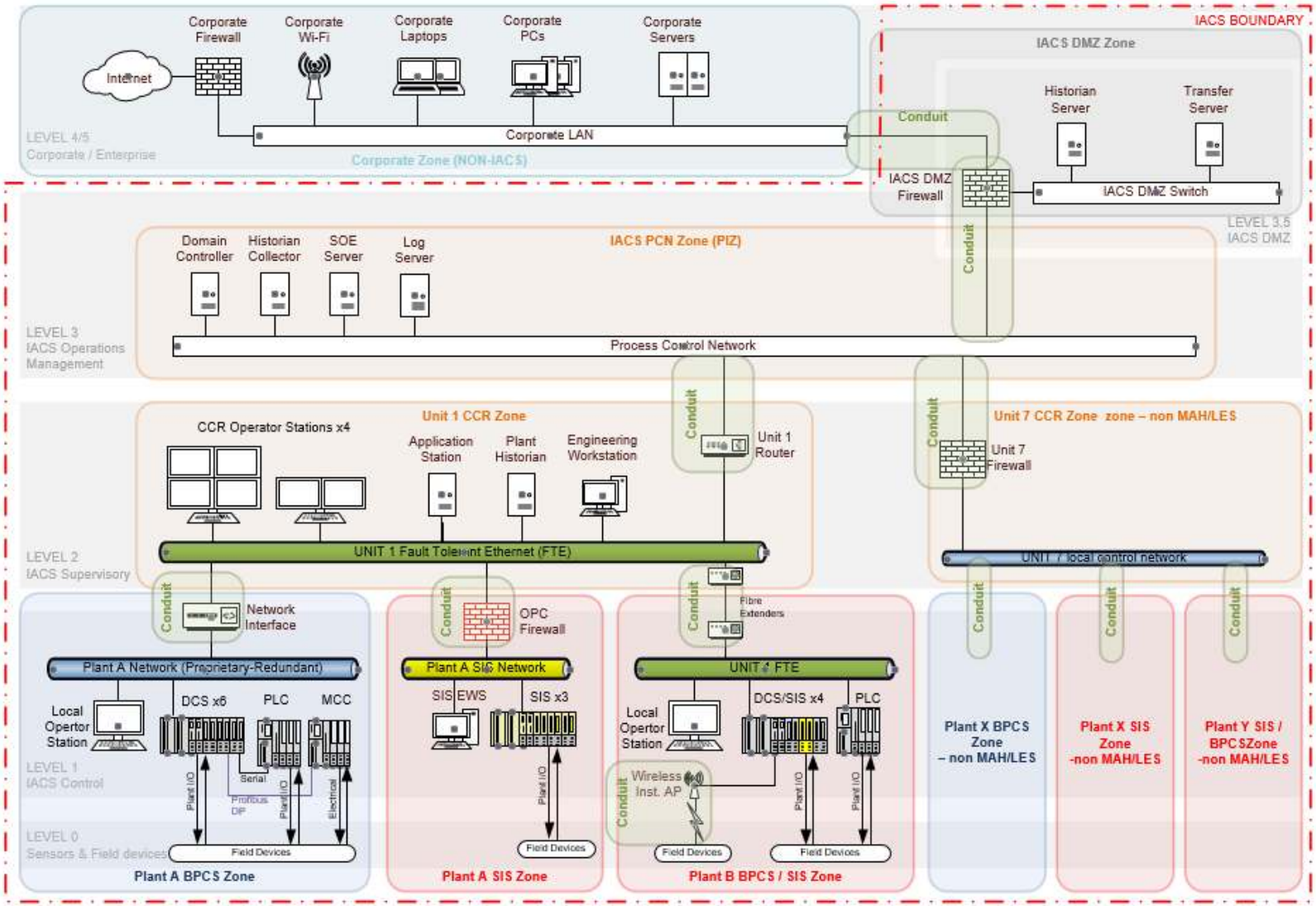
Figure 3-2 Medium sized Site



Points to Note:

1. In this example for a medium sized site (where the BPCS is all on a single network) there is a SIS zone, a BPCS zone and a plant information zone (PIZ).
2. As above, the field devices are within the IACS scope. In this case there are some fieldbus devices – this is essentially a network and therefore may require countermeasures to be applied, e.g. hardening
3. It is assumed that the BPCS and SIS zones are both directly associated with MA and/or LES processes. The PIZ is also therefore associated with MA and/or LES since it is connected to the BPCS zone and there is significant data transfer to allow normal operation and control.
4. There is a conduit between the BPCS zone and the SIS zone, presumably to provide read only data from the SIS to the BPCS. In this case segregation has been achieved by using a dedicated point-to-point serial connection. Note that the discrete I/O also shown between these zones is not a network connection but hardwired electrical connections (e.g. 4-20mA) and therefore not considered a conduit.
5. The engineering laptop is also a potential external conduit if it could be used to transfer data between the SIS zone and other systems.
6. There is a router between the PIZ and BPCS zone. This would permit only the necessary connections between the BPCS and the PIZ. A firewall could also be considered for this duty depending upon the necessary data access etc.
7. Segregation between the IACS zones and the corporate zones has been achieved with a firewall. It is within the IACS boundary and therefore subject to management controls of the IACS. (Some corporate rules may not allow this and therefore would <u>also</u> require a firewall on the corporate side).
8. Although only a firewall is shown in this case for simplicity, segregation between the IACS and the corporate zone would be better achieved with an IACS-DMZ. This would especially be appropriate where multiple connections are made across the boundary and / or where there are more privileged connections made to the IACS.
9. Note that the drawing has been marked up in red to show the necessary connections between the zones. This can be a useful approach and help subsequent specification of the firewall rules but is likely to be impractical on larger networks.
10. There is a historian mirror in the corporate zone which provides historian data to the corporate PCs. This allows the PIZ firewall to be configured to limit access only between the two historians and therefore minimise threats from other connections.
11. Remote access to the IACS Engineering workstation and Recipe manager from either the Engineer's corporate PC or from remote support is provided as follows:
    a. For remote support a dedicated corporate device is provided which must first connect to the corporate network via VPN. Other options could be considered to provide a secure corporate environment, such as remote desktop solutions (e.g. Citrix).
    b. The corporate device then connects the IACS Remote access server to establish a secure environment within the IACS.
    c. Remote desktop protocol (RDP) is then used to access the BPCS zone devices
    d. Other controls would need to be in place to ensure adequate cyber security (authentication, monitoring etc.)
12. Network Access Controls are also in place to permit file transfer via the NAS between the corporate zone and the BPCS (e.g. for backup storage) and to gather anti-virus / operating system updates via the Update server.
13. Both wireless instrument and wireless PDAs are in use on the IACS and therefore it would be necessary to secure these networks with encryption.
14. A temporary connection is provided for an engineering laptop within the SIS zone. Both the laptop and connection would need to be managed to prevent unauthorised access and introduction of malware etc.
15. Therefore, the full range of technical countermeasures should be considered.

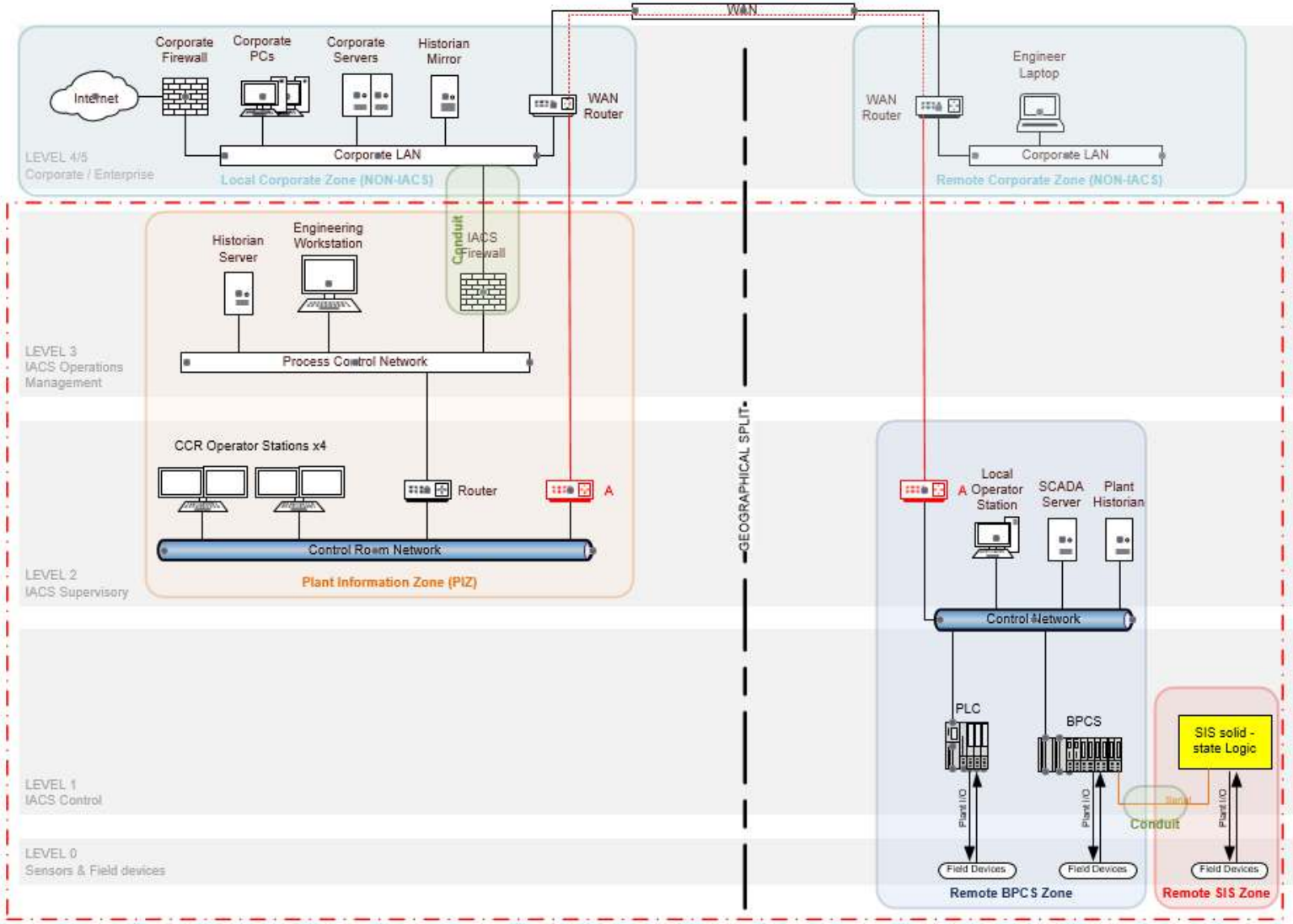
Figure 3-3 Large Site



Points to Note:

1. This example shows a larger, more complex site with a range of configurations.
2. It is a large multi-unit site with each unit having one or more plants, although only two units are shown (unit 1 is fully shown and unit 7 only partially shown – the detail from levels 0-2 is omitted). In practice there would likely be a drawing for each unit showing just levels 0-2 and a top-level drawing showing levels 3-5.
3. It is assumed that Units 1-6 are associated with MA and/or LES processes. However, unit 7 has been designated as non-MA/LES and it is assumed that the data flows to/from unit 7 are minimal and therefore, rather than apply the full range of countermeasures to Unit 7, it has been segregated with a firewall. This ensures that any cyber security threats from Unit 7 are minimised. Equally, it would be acceptable to apply the countermeasures to Unit 7 and treat it part of the IACS.
4. In addition to the relevant comments from the medium and small site:
5. Unit 1 shows a combination of a newer (more inherently secure) control/ safety system and associated operator interfaces etc. (Unit 1 CCR zone and Plant B BPCS/SIS zone) alongside older (less secure) control/ safety systems (Plant A BPCS zone and Plant B SIS zone). Given the less secure nature of the latter, an OPC firewall has been used to segregate the Plant A SIS zone and would be designed to allow simple and secure firewall rules to be applied.
6. A ‘CCR zone’ has been defined for each unit in between the BPCS and PIZ zones. This zone could have been considered part of the BPCS zone(s) but in this case, given the network size, better segregation can be achieved by defining a separate zone. Such an approach may also be useful reflect local geographical splits or responsibilities.
7. The PIZ zone also shows a Log Server – this would allow aggregation of security logs from across the network.
8. A DMZ zone is used to provide historian and file transfer services to the corporate zone to / from the IACS zones. This would be appropriate because significant number of connections would otherwise be needed to communicate to all the units. The DMZ effectively aggregates the data which is then passed to the Corporate Zone and minimises the data connections required (and therefore minimises exposure to threats).

Figure 3-4 Remote Site



Points to Note:

1. In this example, there is a centralised control room with a remote operating site which could be one of many, or the remote site could be an offshore installation.
2. The zones shown have been significantly over-simplified to allow focus upon the remote site issues, for example no IACS-DMZ zone.
3. The connection between the local and remote zone has been shown as a WAN in this case but it could equally be a satellite or other radio solution or via a public network. Selection of appropriate technology to give the desired throughput and availability would be necessary.
4. Essentially the objective is to provide a secure connection between the local and remote sites, i.e. points A-A shown in red, such that the remote and local zones are logically connected as if they were physically connected.
5. There are, in effect, no conduits between A-A because although the data physically traverses the zone and IACS network boundary, it is logically separate.
6. The technical (and organisational) countermeasures required to achieve a secure connection between A-A will depend upon the connection type, the number of remote connections required and other factors etc.:
    a. In this respect a secure connection is one that cannot be accessed (eavesdropped, modified etc.) from non-IACS zones (including a corporate zone).
    b. it will be necessary to protect the data over the unsecure (non-IACS) connection between the two end-points, e.g. using VPN or other similar technologies.
    c. It should be noted that even dedicated satellite / radio connections are unlikely to be secure because of the potential for access to the communication link remote from the intended transceivers.
    d. Some WAN or other providers may also be able to provide a more secure connection without requiring end-to-end protection, e.g. using VPN. In these cases, it will be necessary to understand the potential vulnerabilities of the WAN and make sure they are addressed. For example, cyber security may be reliant upon correct configuration of the WAN routers so tight configuration management and targeted periodic penetration testing may be appropriate.
7. It will also be necessary to consider other threats. For example, with any external connection, denial of service attacks cannot be prevented.
8. The remote location may also have corporate function requirements (in this case an engineer laptop is shown). In these cases, the remote connection will have to provide a separate remote corporate zone that is logically separate to the IACS. Other options using remote desktop environments may also be possible. However, provision of non-IACS functions are outside the scope of this guidance so long as the IACS is sufficiently protected.

Appendix 4: Risk Assessment

As recognised in note 4, there are a range of different risk assessment approaches that could be adopted by a duty holder. For the purpose of this guidance, the following simplified risk assessment process uses zone-based consequence and criticality analysis in order to establish a risk profile as a basis for selecting appropriate and proportionate expectations for countermeasures.

The general concept (based upon IEC62443-2-1 (Ed. 2 draft), is to identify zones that are associated with MA and/or LES consequences and to determine the criticality of those zones in preventing those consequences.

Although not its primary purpose, it may be useful to duty holders as an illustrative example of one method of assessing risk as a basis for defining countermeasures.

The objectives of this assessment are to:

- identify zones that directly or indirectly perform functions protecting against major accident or loss of essential service consequences;
- take a precautionary approach without unnecessarily precluding beneficial technologies;
- allow countermeasures to be modified as technologies develop alongside intelligence on threats and vulnerabilities.

Approach

At this point, IACS assets should already have been identified as described by Note 3 and have been allocated to zones. Each zone should be assessed to determine if it is associated with MA and/or LES consequences and the criticality of the zone.

Consequence

Given that the technical and organisational countermeasures considered within this guidance represent a minimum level of protection, there is no value for the purpose of inspection in considering consequences beyond the generic consequences of:

- major accident (MA);
- loss of essential service (LES);
- Non MA/LES.

Levels of consequence within these generic descriptors may be considered in the future as risk management frameworks develop to target more robust countermeasures at higher consequence scenarios and for more sophisticated attacks – see ‘Future Direction’ section below.

The duty holder should define consequences for each zone.

Defining Zone Consequences

A zone will be considered to be associated with MA and/or LES consequences if:

1. The assets within that zone provide functions protecting against MA and/or LES consequences (typically control system zones and safety system zones), or
2. The assets within that zone are not segregated from another zone that has been defined as being associated with MA and/or LES consequences (typically plant information zones, IACS-DMZ)

In practice, relevant consequences are inherited up from the MAH and/or LES plant up through the network architecture until a point of network segregation (i.e. perimeter device or air-gapped with only limited controlled data transfer).

This requires an understanding of the network architecture and segregation and may be an iterative approach since the network architecture and segregation may be changed as a result of defining appropriate countermeasures which could subsequently change the associated consequence for each zone.

Non MA/LES Consequences

It is recognised that in some cases there will be systems (including BPCS, SIS etc.) that fall under the ownership or responsibility of the same personnel responsible for MA/LES IACS but which are not associated with MA/LES consequences. For example – assets associated with supporting process plant that do not handle MA substances or provide essential services.

In these cases, the duty holder should either:

- Show these assets as within the IACS but within a zone marked as 'non-MA/LES IACS' or
- Show these assets as outside the IACS boundary (non-IACS)

In either case it will not be necessary to apply countermeasures to these non MA/LES assets, although any connections to these systems would be considered as external conduits and the IACS would need to be segregated from these non-MA/LES assets (see appendix 5 B4). It is recommended that it is clear within the risk assessment that these non-MA/LES assets have been considered.

Assets with LES Consequences in External or Corporate Zones

In most cases the IACS assets should not be located within external or corporate zones and should be moved in such cases to be within IACS zones. However, it is recognised that in some limited cases for Operators of Essential Services, IACS assets that are required for the provision of the essential service (e.g. business sales / provisioning systems) cannot be moved from the external or corporate zone.

In these cases, the duty holder should either:

- Recognise these as essential data services and provide appropriate protection (see Appendix 2, B3) noting that the protection (e.g. paper backup system) would need to fully deliver the essential service, or
- Define an additional IACS zone within the external or corporate zone to contain these assets and provide appropriate countermeasures to protect this zone.

Criticality

The criticality of the zones can now be determined. For the purposes of this guidance, the following definitions apply:

- relevant IACS zones: zones containing IACS assets that indirectly perform functions supporting the areas for which relevant consequences have been defined;
- critical IACS zones: zones containing IACS assets that directly perform functions supporting the areas for which relevant consequences have been defined.
- Note – if a zone is able to compromise a critical function of a critical zone, for example by the transfer of malicious data, then that zone will also be a critical zone. For example:
    - if a BPCS zone had the capability to defeat safety functions within a critical SIS zone (without other measures being taken to prevent unauthorised defeat such as hardwired SIS enables) then both the BPCS and SIS zones would be critical zones;
    - if an electrical system zone could cause a critical BPCS zone to disrupt an essential service then both would be critical;
    - if a compromised plant information zone could write malicious commands to a BPCS that was critical to the delivery of an essential service then the plant information zone would also be a critical zone.

Table 4.1 provides examples of IACS zone criticality based upon typical IACS architectures:

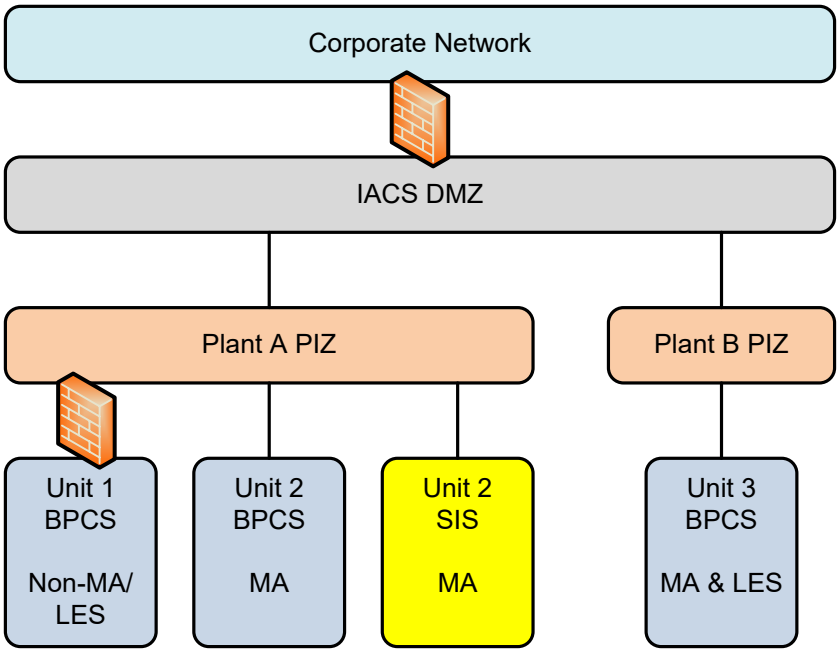
Major accident		**Loss of Essential Service**	
Relevant Zone	**Critical Zone**	**Relevant Zone**	**Critical Zone**
Control system zone	Safety system zone	Plant Information zone	Control system zone
Plant Information zone		IACS DMZ	Safety system zone
IACS DMZ			
Table 4.1: examples of IACS zone criticality			

Having identified the IACS assets and zones and their criticality to the prevention of MA and/or LES consequences, relevant countermeasures can be allocated as described in Appendix 5.

Example Risk Assessment based upon Zone Consequence and Criticality

This section provides inspectors with an example of how zone consequence and criticality could be used to conduct a simple risk assessment.

The following example architecture is considered:



This could result in the following example risk assessment output:

Zone	Consequence	Criticality	Comment
Unit 1 Demin plant BPCS zone	Non-MA/LES	N/A	
Unit 2 Product storage BPCS zone	MA	Relevant	BPCS is relevant for MA
Unit 2 Product storage SIS zone	MA	Critical	SIS is critical for MA
Plant A PIZ	MA	Relevant	MA consequence inherited from lower unit 2 BPCS / SIS zones
Unit 3 Fuel export BPCS zone	MA LES	Critical	BPCS is critical for LES
Plant B PIZ	MA LES	Relevant	MA / LES consequence inherited from lower unit 3 BPCS zone
IACS DMZ	MA LES	Relevant	MA / LES consequence inherited from lower plant A / B PIZ zones

Future Direction

The risk assessment approach above along with the approach described in appendix 5 for selection of countermeasures allows inspectors to assess if duty holders have defined the basic level of appropriate (i.e. where relevant to cyber security threats) and proportionate (i.e. are applied only where there are potential MA and/or LES consequences) countermeasures on MA / LES sites.

The basic level of countermeasures shown in appendix 5 of this guidance have been developed in accordance with NCSC guidance and represent, in many cases, partially achieving some aspects of the cyber assessment framework (CAF – see https://www.ncsc.gov.uk/guidance/indicators-good-practice).

This is the first stage of a managed approach to overall management of cyber security risks that will protect these sites from less sophisticated cyber security threats that is practical and achievable in a reasonable time frame.

At a later stage, once basic levels of countermeasures have been more widely adopted and as risk management frameworks develop, it is expected that these basic level countermeasures may need to be improved to target higher consequence scenarios. It is expected that these improved countermeasures would be defined in terms of higher levels of compliance with the NCSC CAF, proportionate to the risk. This guidance will be updated in future to describe the higher levels of countermeasures as the CAF framework develops.

Although there will be a staged approach to defining appropriate and proportionate countermeasures within this guidance for the purpose of inspection, duty holders remain responsible for applying relevant good practice and selection of countermeasures to address the MA and/or LES (as appropriate) risks on their site.

Appendix 5: Cyber Security Countermeasures

This appendix provides an interpretation of the basic level of countermeasures and an example approach on how to decide which of these countermeasures should be allocated to each zone.

The general approach to defining which countermeasures should be allocated to each MA/LES zone should be based upon the threats relevant to these zones.

However, the existence of the defined basic level of cyber security suggests that there are two realistic approaches to the allocation of countermeasures to zones:

1. starting with a list of all reasonably foreseeable threat scenarios, analyse each zone against these threat scenarios and select all countermeasures that would protect against these threat scenarios; OR
2. starting with a list of the basic level of countermeasures, analyse each zone applying these countermeasures unless a countermeasure clearly is not appropriate on the basis of some form of analysis – e.g. based upon threat scenarios of other method such as attack trees.

It is recognised that there are some countermeasures that will always be appropriate, e.g. B4.1a Network Architecture. Equally, some countermeasures will only be appropriate where there are specific threat scenarios, e.g. B.3.1 Encryption might only be appropriate because there is the threat of a compromised remote access connection.

Example Approach based upon Threat Scenarios

This section provides inspectors with an example of how allocation of countermeasures could be completed based upon threat scenarios.

At this point, IACS assets should already have been identified as described by Note 3 and have been allocated to zones and each zone should have been assigned an associated MA/LES consequence (MA/LES/none) and criticality (relevant or critical) as described by Note 4 and Appendix 4.

To define technical countermeasures, each zone should be assessed to:

1. determine which threat scenarios are relevant to that zone,
    - The threat scenario descriptions should be generic in nature to recognise that it is not possible to describe future (or indeed present) threats and vulnerabilities accurately.
2. define the appropriate technical countermeasures to protect against the relevant threat scenarios determined:
    - defence in depth is required and therefore every technical countermeasure that could protect against a particular threat scenario should be allocated, i.e. all countermeasures should be allocated where relevant, even if other countermeasures are already allocated.
    - the duty holder should record a level of detail sufficient to be specific to the actual zone and site. For example, it is not adequate to simply state that encryption is required for a zone, there should also be reference to what is

to be encrypted and how, such as *'Wi-Fi (name) to be encrypted – see doc. (doc. Ref. no.)'*.
    - It may be obvious that some technical countermeasures are required for every zone,
3. where the required technical countermeasures cannot be applied consider other countermeasures (including those marked as optional) to provide equivalent protection.
    - For example, it may not be technically feasible to apply all aspects of asset hardening to some existing control systems if they use default privileged logical access accounts – in these cases additional monitoring or segregation could be applied.
4. where the required technical countermeasures are not currently in place, define time-bound plans for their implementation.

Example Threat Scenarios

The following example threat scenarios should be used by inspectors to assess the adequacy of a duty holder's assessment. This table is not intended to be exhaustive in the list of threat scenarios (and only simplified scenarios are provided), nor in the associated technical countermeasures and may be updated in future.

Duty holders should develop a list of reasonably foreseeable threat scenarios relevant to their site based upon relevant intelligence.

Table 5.1 – Expected Technical Countermeasures Based upon Threat Scenarios

Threat Scenario	Technical Countermeasure
Unauthorised physical / logical access to IACS assets by un-authorised employee	B2 Identity and Access Control ○ Physical and logical access controls to limit access to minimum B3 Data Security ○ Encryption for recorded user / device credentials / certificates to prevent unauthorised use B4 System Security ○ IACS Network Architecture, Segregation and Access to prevent access from other networks, e.g. corporate C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions

Threat Scenario	Technical Countermeasure
Unauthorised physical / logical access to IACS assets by authorised employee	B2 Identity and Access Control ○ Physical and logical access controls to limit access to minimum B3 Data Security ○ Encryption for recorded user / device credentials / certificates to prevent unauthorised use B4 System Security ○ IACS Network Architecture, Segregation and Access to limit access to least required C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions
Unauthorised physical / logical access to IACS assets by authorised third party, e.g. vendor, integrator etc.	B2 Identity and Access Control ○ Physical and logical access controls to limit access to minimum B3 Data Security ○ Encryption for recorded user / device credentials / certificates to prevent unauthorised use B4 System Security ○ IACS Network Architecture, Segregation and Access to limit access to minimum, e.g. from one vendor's system to another's. C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions
Unauthorised physical / logical access to IACS assets by external party	B2 Identity and Access Control ○ Logical access controls to limit access to minimum Wider site security to prevent physical access to the site B3 Data Security ○ Encryption for remote access and remote connections B4 System Security ○ IACS Network Architecture, Segregation and Access to prevent access from external networks ○ Asset hardening to minimise exposure to vulnerabilities C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions

Threat Scenario	Technical Countermeasure
Unauthorised access to IACS data connection (internal conduits and connections within a zone)	B2 Identity and Access Control ○ Physical access controls to prevent addition of unauthorised devices ○ Logical access controls to prevent access to assets Wider site security to prevent physical access to IACS networks B3 Data Security ○ Encryption for wireless networks and wireless instruments to prevent access to these networks C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions
Unauthorised access to externally accessible data connection (remote connections, remote access)	B2 Identity and Access Control ○ Logical access controls to prevent access to assets ○ Logical access controls to prevent credential theft e.g. more robust authentication (e.g. multi-factor) B3 Data Security ○ Encryption for external data connections that bring data into IACS ○ Encryption for remote access B4 System Security ○ IACS Network Architecture, Segregation and Access to prevent unauthorised access to more critical assets if connections compromised C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions
Malware (including viruses, worms, ransomware etc.) introduced from external networks, portable assets and media, or within purchased assets	B4 System Security ○ IACS Network Architecture, Segregation and Access to minimise spread of malware ○ Asset Hardening to reduce exposure to vulnerabilities C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions ○ Malicious code detection systems to identify and contain known malware / threats
Software flaws	B4 System Security ○ Asset Hardening to reduce exposure to software flaws
Denial of service	B4 System Security ○ IACS Network Architecture, Segregation and Access to minimise spread and impact C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions

Threat Scenario	Technical Countermeasure
Equipment Loss, theft etc.	Wider site security B2 Identity and Access Control ○ Physical access controls B3 Data Security ○ Encryption for devices / media
Social Engineering (e.g. phishing, spear-phishing, watering holes, scanning, corruption etc.) to gain unauthorised access	B2 Identity and Access Control ○ Logical access controls to limit access to minimum ○ Logical access controls with more robust authentication for higher privileged authorisation C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions

Interpretation of IACS Technical Countermeasures Requirements

This section of appendix 5 describes typical basic expectations for cyber security countermeasures for the purpose of inspection, it remains the responsibility of the duty holder to manage cyber security risks.

The following countermeasures are based on:

- the risk assessment of Note 4 and Appendix 4: Risk Assessment;
- the NCSC NIS principles and guidance;
- the current draft version of IEC 62443-3-1 Security for industrial automation and control systems, Security Technologies for Industrial Automation and Control Systems. (Draft 1, Edit 1, December 2012).
- other relevant countermeasures;
- consideration of countermeasures that address IACS-wide vulnerabilities, irrespective of localised risk on the basis that:
    - traditional risk assessments may not have identified safety functions or impact on essential service for cyber threats because they did not consider multiple contingencies (i.e. several things occurring at once) or threats that have malicious intent; or that
    - these systems could be used to attack the other zones. Examples could include malicious code detection systems and the use of perimeter devices whose application will depend on the architecture and layout of the IACS;

However, it should be noted that the cyber security landscape is a frequently changing and so the following list should not be seen as exhaustive.

Table 5.2 – Interpretation of Countermeasures

B2 Identity and access control

The purpose of the identify and access control technical countermeasures is to limit logical and physical access to the minimum required and that users (or automated functions) that can access the IACS are appropriately verified, authenticated and authorised.

B.2.1 Logical Access

Note – defining and managing authorisation based upon the principle of least access and authentication should be covered in the CSMS – see appendix 2 B2.

B2.1a Authorisation

Countermeasures for Relevant and Critical MA/LES IACS

1. Technical tools for implementing authorisation requirements are typically included in the operating system or control system software settings, e.g. through account management tools.
2. For larger IACS, domain control may optionally be used for implementing authorisation requirements across the whole network to reduce the complexity and time required for management of authorisation.
3. Some control / safety system (and other) applications also have authorisation tools in addition to the operating system authorisation – it is important that these tools are both configured correctly.
4. Authorisation to the IACS should be separate to other non-IACS networks / zones, i.e.
   a. no use of domain trust with these other networks / zones
   b. users should use different access credentials for the IACS than other non-IACS networks / zones to ensure that any compromised credentials in these systems (which may not be protected to the same level) cannot be used to attack the IACS.
5. Highly privileged (e.g. Administrator) access should be enabled only on assets where required.
6. Advanced role based authorisation tools may optionally be used but are not widely implemented at this time in IACS (e.g. as described in IEC 62443-3-1).

Countermeasures for Critical MA/LES IACS

1. Where role definitions allow and it is technically possible, separate authorisation tools should be used for the critical zones.
2. Where available key switches or similar shall be used to prevent unauthorised use of highly privileged operating modes (e.g. force or program mode). Access to these keys shall be managed under the CSMS – see appendix 2.

B2.1b Authentication of Users

Countermeasures for Relevant and Critical MA/LES IACS

1. Any method or combination of methods to confirm the identity of individuals. See also IEC62443-3-1:
   - Password Authentication
   - Challenge/Response Authentication
   - Physical/Token Authentication
   - Smart Card Authentication
   - Biometric Authentication
   - Location-Based Authentication
2. Some control / safety system (and other) applications also have authentication facilities separate to the underlying operating system authentication. It is important that these are both configured correctly to prevent unauthorised access. For example, if authentication is achieved within the control / safety system application but using generic operating system authentication then these generic credentials should be protected with strong and unique passwords.
3. Note – different methods may be appropriate for different roles. For example:
   - Control room operator stations may use a common operator username and password as access is controlled by physical location. In such cases, measures must be taken to ensure that the common username / password can only be used on the intended assets for interactive login and that a strong password is used.
   - Remote access (from the corporate or external networks) e.g. by engineers or technical support, should require multi-factor authentication, e.g. physical token authentication or challenge/response authentication to protect against attacks (e.g. key loggers) on the remote device if that device is not managed by the IACS team.
   - Different authentication credentials should be used for highly privileged e.g. administrator access and only used for these tasks. Alternatively, multi-factor authentication or time limited accounts could be used for highly privileged accounts, especially from remote locations or network devices.
4. Password Distribution and Management Technologies may optionally be used (e.g. as described in IEC62443-3-1) to facilitate more robust password management.

Countermeasures for Critical MA/LES IACS

1. Where role definitions allow, and it is technically possible, separate authentication methods should be used for the critical zones.

B2.1c Authentication of Devices

Device to device authentication between the core control and safety system components may or may not have been built in to these systems and would not normally be a matter for the end-user.

Device-to-device communication may be in use to communicate to other devices within the IACS such as historian, database or third-party servers, or across the IACS boundary, for example remote sites or the corporate network. This would include situations with central control rooms operating remote sites and situations where data is transferred between the IACS network and the corporate network for data historian or business system purposes.

Countermeasures for Relevant and Critical MA/LES IACS

1. Only IACS authorised assets shall be connected to the IACS.
2. The IACS assets should be configured to deny connections by default and only permit authenticated connections.
3. Device-to-device authentication should be used using certificate based authorisation or very strong and random password(s) that are unique to each connection type.
4. Password Distribution and Management Technologies may be optionally used (e.g. as described in IEC62443-3-1) to facilitate more robust password management.

Countermeasures for Critical MA/LES IACS

1. Device-to-device authentication should be used using certificate based authorisation or very strong and random password unique to each connection.

B.2.2 Physical Access

Physical security control should be implemented to prevent both external and insider threats. Risks from external threats (including visitors) are generally addressed by protection measures provided for wider security issues, e.g. at the establishment boundary or for access to specific plant areas or control rooms. These are not covered within this guidance, and may provide additional layers of protection but do not generally address insider threats.

The physical security controls should aim to prevent:

- Unauthorised physical access to IACS assets
- Unauthorised physical modification or operation of IACS assets
- Unauthorised observation of IACS assets, e.g. for the purpose of planning cyber attack
- Unauthorised introduction of new systems, communications interfaces or other hardware
- Unauthorised introduction of rogue devices intentionally to cause hardware manipulation, communications eavesdropping or other harm

Note – A significant portion of documented attacks against IACSs had elements of physical access that were violated in order to execute the penetration.

Note – defining and managing authorisation for physical access based upon the concept of providing least access should be covered in the CSMS – see appendix 2.

Countermeasures for Relevant and Critical MA/LES IACS

Either limit or monitor access as follows:

1. Access Limiting Systems:
   a. Active (e.g. key-card access) or passive (e.g. locking of equipment rooms, cabinets etc.) systems to prevent access to IACS assets.
   b. Protection of IACS media – e.g. software, documentation, backups by securing in a physically secure place.
   c. Hardening communication lines that are vulnerable to unauthorised access, e.g. network cables that pass through or near publicly accessible areas, e.g. using enclosures.
2. Access Monitoring Systems:
   a. Systems such as CCTV, alarms or similar to record and/or alert of unauthorised presence, e.g. within an IACS equipment room to deter unauthorised action – particularly useful for remote / unmanned locations.
3. Physical protection measures should be more robust in more remote areas if these are not under the wider site security arrangements, for example a remote unmanned location. In these cases, in addition to access limiting techniques, access monitoring should be employed or more frequent inspection depending upon the risk.
4. It is important to select an appropriate technique to allow the minimum level of access to be achieved. For example, if physical access is limited at the room level this may not be sufficient if the room is also accessed by non-IACS personnel, thus increasing the insider threat. All personnel that have physical access to the IACS will have IACS responsibilities (see appendix 2 section A.1) with associated competence and screening requirements and therefore techniques that limit access to the minimum are advantageous.

Countermeasures for Critical MA/LES IACS

1. Where role definitions allow and it is technically possible, separate access limiting systems shall be used. For example, the equipment cabinet key for high risk zones should be different to the key for other zones.

B3 Data Security

The purpose of the data security technical countermeasures is to protect relevant data that is stored or transmitted from unauthorised access, modification or deletion or otherwise made unavailable.

B3.1 Encryption

Note that encryption technologies are not currently widely available for use within control and safety system communications, although may be implemented in future.

Encryption techniques should be used to protect data that is either in transit or at rest.

See IEC62443-3-1, which includes information on different types of encryption techniques.

The data that requires protection should be identified as part of the CSMS – see appendix 2.

Countermeasures for Relevant and Critical MA/LES IACS

1. As a general rule, if encryption is readily available for any connection then it should be enabled.
2. Wireless networks (Wi-Fi) should be encrypted. Note that WPA2 enterprise is more secure. WPA1 and WEP should not be used.
3. Wireless instrumentation networks should be encypted. Encryption is usually available but for some protocols it must be enabled.
4. Remote connections / networks, i.e. connections over non-IACS networks should be encrypted, e.g. using VPN or similar. The associated configuration (including user and access rights) must be documented, tested, kept up-to-date and changes managed as part of the CSMS.
5. Network connections that bring data into the IACS network from other networks, e.g. to download patches (WSUS), anti-virus definition files or file transfers should use encrypted connections, e.g. TLS, secure FTP, or similar to prevent injection of malicious versions from the other network.
6. Tools for the secure storage of data such as passwords ('password vaults') may optionally be used, e.g. to allow and monitor authorised access to, for example, device passwords. Where such tools are used, the data should be encrypted when stored or in transit.

Countermeasures for Critical MA/LES IACS

No additional countermeasures

B4 System security

The purpose of the system security technical countermeasures is to protect relevant IACS assets from cyber-attack through the use of robust and reliable countermeasures.

<u>B4.1 IACS Network Architecture, Segregation and Access</u>

A system-wide view needs to be considered when considering the IACS network architecture, segregation and access countermeasures based upon the system design requirements, the network connectivity required, the potential risk profile of each zone and the other countermeasures in place.

The overall intent of this section is to provide an overall defensive architecture with strong boundary defences between the IACS and other networks and simple data flows at these boundaries to permit effective monitoring.

In general, there are three main areas to consider when employing these countermeasures:

1. Architecture – i.e. the overall IACS network structure to allow a defensive architecture model to be adopted.
2. Segregation – i.e. how the IACS networks are segregated from other networks and internally.
3. Access – i.e. how the IACS network is connected to other networks.

B4.1a IACS Network Architecture

Countermeasures for Relevant and Critical MA/LES IACS

1. The IACS network should be physically configured into different levels to form a hierarchical architecture (see appendix 3 for examples) such that a defensive architecture can be applied, for example based upon the Purdue Model:
   - Level 4 & 5 – Corporate / Enterprise
   - Level 3.5 – Optional DMZ between IACS and non-IACS
   - Level 3 – IACS Operations management
   - Level 2 – IACS supervisory control, e.g. operator, application, batch processing, engineering workstations etc.
   - Level 1 – IACS controllers (including PLCs etc.) and real-time operations
   - Level 0 – IACS sensors and field devices
2. More vulnerable activities such as file transfer, external network connections and data transfer etc. should be carried out only at the top levels of the IACS hierarchy, i.e. level 3 and above. Real-time operation etc. at lower levels, i.e. levels 0-2.
3. Network communication should only be permitted between adjacent levels. The network architecture should be designed to ensure simple known data flows only between different levels and different zones and securely transfer data into higher risk zones from lower risk zones.
4. Where data is required to traverse multiple levels of the network it should either:
   - Be passed to an asset in the adjacent level which should then pass to the next level and so on, using different protocols or services at each step such that a single vulnerability cannot be exploited to gain access across multiple levels of the hierarchy, OR
   - Connected via a perimeter device (see network segregation below B4.1b)
5. In some cases, it may be simpler and more cost effective to remove or not introduce assets or network connections that could pose a cyber security risk or substitute them with ones less vulnerable to threats, for example:
   a. Removal of remote operator terminals where operation could be achieved in other more secure ways such as hardwired local indicators/limited functionality devices or migration to a central control room.
   b. Use of non-programmable systems in remote areas.
   c. Note - Non-programmable systems may not provide the required functionality / flexibility required leading to other risks.
   d. Air-gapping zones where there are no or minimal data transfer requirements. However, this consideration must be balanced with the need for operability and maintainability, for example: air-gapping a zone where data transfer is required for operation and maintenance reasons could increase cyber security risks due to increased use of USB drives etc.
   e. Provide an additional historian server on the corporate network that gathers data from the IACS historian rather than have all corporate PCs access the IACS network.

Countermeasures for Critical MA/LES IACS

No additional countermeasures

B4.1b IACS Network Segregation

Network segregation considers:

1. Physical segregation, i.e. different physical network devices
2. Logical segregation, i.e. use of filtering, blocking devices to segregate network communications

Countermeasures for Relevant and Critical MA/LES IACS

1. The IACS zones should be physically segregated from (i.e. not share the same network hardware with) non-IACS networks / zones; e.g. using virtual networks (VLAN) or other network multiplexing devices.
   a. Virtual networks (VLAN) and other network multiplexing devices do not typically provide sufficient segregation on their own because they typically don't permit physical and logical access controls, patching, change management, configuration management etc. to be effectively managed under the IACS CSMS. For example, the configuration management console would normally be accessible from both sides of the network.
   b. Note that the above does not apply to situations where physically separate network infrastructure runs within the same cable – for example different fibres within a shared cable so long as the cable and associated connections are managed by the IACS CSMS, e.g. including physical access controls to IACS personnel only.
   c. Note that virtual networks (VLAN) and other network multiplexing devices may optionally be used to provide additional segregation within IACS zones, e.g. between vendors or as part of fieldbus networks.
2. Where there is currently sharing of network hardware on existing installed IACS, the following approach should be adopted to address the situation (in order of preference):
   a. Provide additional network hardware to achieve physical segregation or the non-IACS network / zone connections removed, or
   b. Consider the shared hardware as non-IACS (this may result changes to the simple network drawing) and alternative measures taken to provide the necessary access (see 4.1c item 6 below) over this non-IACS network.

3. The IACS networks / zones should be logically segregated from non-IACS network / zones, i.e. for external conduits. This is to ensure that the organisational and technical cyber countermeasures can be applied to the IACS risk zones only – it would not be proportionate to apply countermeasures to the non-IACS networks / zones. This should be achieved either by:
   - physical separation of the IACS networks / zones from the non-IACS networks / zones (also known as air-gapping), OR
   - the use of network devices for filtering, blocking or access control ('perimeter devices') to restrict the traffic to minimum required between the IACS and non-IACS networks / zones.
4. The IACS zones should be logically segregated from each other where appropriate:
   a. The principle of least access should be applied, i.e. only allowing assets that need to communicate, to communicate, e.g. using routers.

b. Whilst perimeter devices provide more protection, they should not be placed between assets that pass real-time control data due to the increased latency.
c. Logical segregation between IACS zones should preferentially be achieved using hardware network assets (switches / routers / perimeter devices as appropriate) rather than multi-homed assets (i.e. single device having multiple network cards connected to different networks / network levels) as they allow better access control and management.
d. Logical segregation between IACS zones can also be achieved using dedicated network connections, such as between a SIS zone and a BPCS zone.

5. Where required, perimeter devices such as firewalls (or similar such as unidirectional gateways / data diodes) shall be implemented as follows:
   a. Perimeter devices should be configured on the basis of least access, i.e. deny by default, and should only permit minimum data connections.
   b. Perimeter devices should permit inspection and monitoring of traffic passing through the device.
   c. Hardware perimeter devices (rather than e.g. host-based firewalls) should be used being more secure and easier to configure / maintain.
   d. The configuration of all perimeter devices should be subject to configuration management and validation testing – see appendix 2 B1)
   e. Perimeter devices may optionally also be used as additional risk reduction countermeasures on a case-by-case basis, e.g. un-patched systems to prevent access to vulnerable assets.
   f. Note – host-based firewalls are not widely implemented in IACS environments for control of network communications but may be optionally used as additional risk reduction on a case-by-case basis, e.g. un-patched systems to prevent access to vulnerable assets. Where they are used it is recommended that the configuration is kept simple.
   g. Perimeter devices may optionally be used to separate server layers and control layers in larger networks.
   h. Specialised (e.g. in-line) perimeter devices may optionally be used in some applications and are particularly useful for specific IACS protocols (e.g. OPC, Modbus) or where specific data types are required to traverse multiple layers of the hierarchy.
6. An optional IACS DMZ level should be considered for external conduits that cross the IACS boundary where there is significant data transfer (often to the corporate network), which includes intermediate assets to allow data / file transfer etc.
   a. It may be advantageous to provide a DMZ to allow more secure data / file transfer rather than try to manage data / file transfer by removable media or portable device.
   b. Where used different authentication and protocols / ports should be used for communications to higher / lower levels of the IACS network architecture
   c. Note that the IACS DMZ is a protection for the IACS and therefore should be the under the responsibility and management of the IACS CSMS
7. Within a zone, communication links containing real-time communications (i.e. typically communications between controllers, PLCs or fieldbus devices etc.) should be physically separated from other IACS networks (that contain the servers and workstations).

a. In older existing systems, this may have been done by use of proprietary networks and network interfaces or point-to-point (e.g. serial) connections.
b. Where TCP/IP networks are used (e.g. Modbus over TCP/IP) provide a dedicated network that is separate to other IACS networks.

Countermeasures for Critical MA/LES IACS

1. Where practical, physically segregate (i.e. air gap) the critical zones from other zones and provide communications via discrete I/O connections. It should be noted that in many cases, the amount of data that is required to be passed for operational reasons may make this option impractical.
2. Where critical zones are connected to other zones either:
   - Use dedicated network / serial connections to transfer data to/from the critical zone, for example a point-to-point network rather than using the wider IACS networks, OR
   - Use a perimeter device

B4.1c IACS Network Access

Network access countermeasures are used to ensure secure access to the IACS zones from non-IACS zones.

Countermeasures for Relevant and Critical MA/LES IACS

1. Non-IACS managed devices should not be able to directly connect onto IACS networks / zones, e.g. using VPN or other network connection protocols.
2. Where remote access is required for applications (e.g. remote engineering, configuration etc.) from non-IACS networks / zones:
   a. Remote / virtual desktop environments are often used for this type of access (e.g. RDP, Citrix etc.).
   b. Encrypted connections should be used – see B3 above. Note that this could include the use of VPN but (as stated above) the VPN should not connect the remote host device directly to the IACS network.
   c. Dedicated server hardware and software assets within the IACS should be used to provide the remote access. Separate assets should be considered for external connections or, for example, different vendors etc. if different network access is required to limit remote access.
   d. Where possible use dedicated client hardware and software for accessing the IACS that is subject to cyber security controls – for example corporate network laptops.
   e. Remote connections should be provided at higher levels in the IACS network architecture only (preferably from within the IACS DMZ) with users ‘browsing down’ to lower levels if necessary.
   f. The environment must be configured in a secure way and hardened (see B4.2), including ensuring that a compromised remote (non-IACS) host cannot be used to gain access to the IACS environment.
   g. Additional measures will be necessary to ensure that threats (e.g. key loggers) cannot be used to compromise IACS access, e.g. limited authorisation (i.e. only those that required remote access) and multi-factor authentication, (see B2)
   h. Access should be subject to monitoring and, where possible, disabled between each use.

3. Where access is required to/from non-IACS networks / zones for automatic data transfer (e.g. historian data, automatic virus signature updates, automatic patch retrieval)
    a. Encrypted connections should be used for any data brought into the IACS – see B3 above.
    b. Connections should be provided at higher levels in the IACS network architecture only (preferably to the DMZ).
    c. Different protocols or services (ports) used to transfer data to/from the IACS networks than used to communicate with low-level assets in the IACS network architecture.
    d. Different authentication credentials used to transfer data outside the IACS networks than used to communicate with low-level assets in the IACS network architecture.
4. Where access is required for manually initiated data transfer (e.g. file transfer)
    a. Encrypted connections should be used – see B3 above.
    b. Connections should be provided at higher levels in the IACS network architecture only (preferably to the DMZ).
    c. Different protocols or services (ports) used to transfer data to/from the IACS networks than used to communicate with low-level assets in the IACS network architecture.
    d. Different authentication credentials used to transfer data outside the IACS networks than used to communicate with low-level assets in the IACS network architecture.
5. Where access is required for portable assets (e.g. USB media, laptops)
    a. They should be under the responsibility and management the IACS CSMS, e.g. with respect to ensuring appropriate countermeasures are in place (e.g. access controls, patching, hardening, monitoring etc.)
    b. They should be configured to disallow, or otherwise prevented from, being connected to other networks where possible.
6. Where access is required between two or more IACS zones using non-IACS networks:
    a. This would include situations such as remote IACS sites using corporate or third-party networks to communicate.
    b. This would include situations where shared hardware has been identified and the shared hardware has been considered as non-IACS (see 4.1b item 2 above)
    c. Countermeasures should be employed to ensure the data integrity and privacy over the non-IACS networks. This could be achieved with either:
        - A VPN connection to provide a secure tunnel between the IACS end-points, OR
        - Other equivalent means of segregation and access. For example, it may be possible to configure some wide area networks to achieve equivalent segregation and access. In such cases it may be necessary to complete additional testing and monitoring to ensure that data is not subject to unauthorised access or tampering.
7. If IACS assets use domain name servers (DNS) to resolve IACS network addresses the DNS server should be provided within the IACS network and not use non-IACS DNS servers.

Countermeasures for Critical MA/LES IACS

1. Where critical zones are accessed from other zones for the purpose of writing data to the critical zone that could defeat or compromise it (e.g. SIS defeats from the BPCS), additional measures should be taken to prevent this:
   a. Key switch or other hardwired enable switch that only permits data to be written to the critical zone when authorised.
   b. Associated management systems to ensure that data is validated (e.g. defeat log)
   c. Note – without these additional measures, the zone writing the data would, by definition, also become a high risk zone.

B4.2 IACS Asset Hardening

Asset hardening is a countermeasure to ensure that securely configured assets are deployed.

B4.2a Server and Workstation Operating Systems

Use of commercial off-the-shelf operating systems (such as Microsoft Windows or Linux) is widespread on IACS servers and workstations, although high-security implementations may become available in future.

Countermeasures for Relevant and Critical MA/LES IACS

1. Use of defined secure builds for assets (including any virtual machines or similar).
2. Where available implement vendor security hardening guidance.
3. Disabling or controlling access (e.g. by password, BIOS changes etc.) to boot, recovery or configuration modes / partitions.
4. Disabling all unnecessary services, especially those that allow remote access (e.g. FTP, remote terminal access, web servers, unused network services etc.)
5. Removal of all unnecessary applications / software. Note - provision of corporate applications (email, web access, corporate documents, office applications etc.) should normally be provided by workstations outside of the IACS boundary (even if they are physically located in the control room etc.).
6. Disabling or modification of any default passwords (both vendor and operating system). Where default access accounts are required then they should be configured to be strong and unique and issued only to authorised personnel in a secure manner.
7. Disabling unused ports, e.g. USB, networks ports etc. either by configuration or physically.
8. Where virtual machines are used and either the host or virtual machine is outside of the IACS, ensure that these are:
   - Securely configured;
   - Used in combination with other techniques (e.g. multi-factor authentication) to prevent malware or unauthorised access to the virtual machine from the host machine or vice-versa (e.g. due to capture of data such as passwords by key-loggers).

9. Additionally, for highly vulnerable assets, application white-listing / sandboxing / software integrity checking should be considered if technically possible to prevent these assets becoming pivot points into the IACS.
    - Highly vulnerable assets are defined here as those that communicate with non-IACS networks / zones typically via a perimeter device, e.g. historians, file transfer servers, remote access servers OR that are used for file / data transfer using portable media.
10. Host Configuration Management Tools – (as described in IEC62443-3-1). Use of these tools is often not applicable to IACS at this time as control and safety systems are usually configured by the control / safety system application; however, they may become applicable in future. These tools may optionally be used to centrally manage configuration of other IACS assets, e.g. with respect to security policies etc.
11. Automated Software Management Tools – (as described in IEC62443-3-1). Use of these tools is often not applicable to IACS at this time as control and safety systems applications are usually installed as part of the control / safety system standard build; however, they may become applicable in future. These tools may optionally be used for inventorying and managing software deployment for other IACS assets, especially on larger systems and where standard commercial technologies are used.

Countermeasures for Critical MA/LES IACS

No additional countermeasures

B4.2b Network Devices

Use of commercial off-the-shelf network devices (switches, firewalls, printers, network storage etc.) is widespread for IACS network devices, although high-security implementations or control / safety system vendor specific devices are becoming available in some cases.

Countermeasures for Relevant and Critical MA/LES IACS

1. Where available implement vendor security hardening guidance.
2. Disabling or controlling access (e.g. by password, configuration changes etc.) to boot, recovery or configuration modes / partitions.
3. Disabling all unnecessary services, especially those that allow remote access (e.g. FTP, remote terminal access, unused network services or functions etc.)
4. Disabling or modification of any default passwords (both vendor and operating system). Where default access accounts are required then they should be configured to be strong and unique and issued only to authorised personnel in a secure manner.
5. Disabling unused ports, e.g. USB, networks ports etc. either by configuration or physically.
6. Where possible, configuring the network device to only accept connections from IACS assets. This is typically done by binding network ports to specific MAC addresses or using ‘sticky ports’ where once a port is physically disconnected, it will only accept connections again when re-configured.

7. Where possible, network devices that are used to connect to a higher level in the network architecture should be configured to prioritise traffic of the lower level to prevent denial of service attacks from above.

B4.2c Real-time and Embedded Operating Systems

Use of real-time and embedded operating systems is widespread in control and safety system real-time assets such as controllers, logic solvers, network access gateways (e.g. fieldbus etc.). Their configuration and cyber security is therefore generally a matter for the vendors.
Traditionally these operating systems were not designed with cyber security in mind and very little can be done by the end-user to harden these – protection is mainly by prevention of unauthorised access.

Countermeasures for Relevant and Critical MA/LES IACS

1. Where available implement the vendors security hardening guidance
2. Disabling all unnecessary services, especially those that allow remote access (e.g. FTP, remote terminal access, web servers, unused network services or functions etc.)

Countermeasures for Critical MA/LES IACS

No additional countermeasures

B4.2d Web (and similar) Technologies

Many assets have web (or similar well known open) technology capability to provide data or access available. These could be used both within and outside the IACS boundary. Web technologies are particularly vulnerable because the technology and its vulnerabilities are well known to attackers.

Countermeasures for Relevant and Critical MA/LES IACS

1. Where web technologies are used within the IACS to provide data or access to non-IACS network clients the following shall be implemented:
    a. The web technologies should only be deployed using the latest security applications, e.g. from a DMZ
    b. The perimeter device at the IACS / non-IACS boundary shall limit access to a minimum
    c. The associated assets should be subject to security monitoring
    d. The web technologies and associated perimeter device should be configured by competent personnel to ensure cyber security.
    e. Note – it is more secure and recommended for data to be passed to non-IACS devices outside the IACS in a secure fashion and then to provide web services from the non-IACS device than provide web services from within the IACS boundary to clients outside.
2. Where web technologies are used within the IACS to provide data or access to IACS network clients the following shall be implemented:
    a. Client access should be limited to the devices that require it. Perimeter devices or similar should be used to enforce this.

b. The web technologies and associated assets should be configured by competent personnel to ensure cyber security.

Countermeasures for Critical MA/LES IACS

1. Web technologies should not be used to provide data or access outside of the critical zone. Appropriate network segregation (air-gapping or perimeter devices – see B4.1 above) should be used to enforce this requirement.

B4.3 Patch Management Tools

Patch management countermeasures typically provide capability to acquire, test and install multiple patches across a range of assets across networks, therefore reducing the burden of manually managing and completing these tasks.

Countermeasures for Relevant and Critical MA/LES IACS

- Where patch management tools are used to acquire patches from outside the IACS network, reference should be made to B4.1c Network Access requirements – see above.
- Patches should be sourced from trusted locations and where applicable approved by the control / safety system vendors.
- Where patches are automatically distributed they should not be installed on mass, or on real-time operational systems.
- Where patch management tools are used they should be used as part of a well-defined management system process – see appendix 2 B4.

Countermeasures for Critical MA/LES IACS

No additional countermeasures

C1 Security Monitoring

The purpose of the security monitoring technical countermeasures is to enable security monitoring of relevant IACS to detect potential cyber security problems and track the ongoing effectiveness of the countermeasures.

Note the requirement to define what security logging and monitoring data is required is covered in appendix 2.

C1.1 Security Monitoring Data Capture and Distribution

Countermeasures for Relevant and Critical MA/LES IACS

1. Where required, security monitoring should be enabled on the assets (servers, workstations and network devices etc.) and conduits (e.g. perimeter devices)
2. Security monitoring should be configured to ensure security monitoring data (logs) are securely stored for an appropriate time and define appropriate access to authorised personnel only.
3. On larger IACS systems operators may optionally forward a copy of security monitoring data to centralised servers to reduce the amount of time required to

review and analyse security monitoring data located on multiple assets. Some logging server software available provides automatic log aggregation, analysis and alert functions which may reduce the manual workload and may optionally be used.
4. Where security logs are sent outside the IACS network for review and analysis (e.g. to a corporate security monitoring function) these should be securely transferred and stored outside the IACS (see also B3 Data Security requirements in appendix 2 and B4.1c Network Access requirements above)
5. Where possible time should be synchronised between logging assets to allow security monitoring data to be correlated.

Countermeasures for Critical MA/LES IACS

No additional countermeasures

C1.2 Malicious Code Detection Systems

Countermeasures for Relevant and Critical MA/LES IACS

1. Installation of anti-malware software where possible on workstations and servers. Note that for real-time operating components such as operator stations duty holders should consult system vendors to ensure that the anti-malware software is appropriate.
2. Configuring the anti-malware software to ensure alert generated are seen, logged and acted upon.
3. Configuring the anti-malware software to enforce scanning of any portable media used, unless this is handled outside of the IACS.
4. Tools may optionally be put in place to distribute malware definition files across IACS zones to reduce the amount of time required to manually update, noting the network access requirements in B4.1c above.

Countermeasures for Critical MA/LES IACS

No additional countermeasures

C1.3 Intrusion Detection and Prevention Systems (IDS / IPS)

Set up and monitoring of IDS / IPS can take significant resource and are considered optional at this time. However, they can provide risk reduction where other required countermeasures are not possible (i.e. to provide equivalent protection) or to address specific risks.

1. Optional installation of intrusion IDS / IPS on key network connections – for example external conduits (e.g. to corporate network or remote access).
    - IPS should not be used between real-time operating communications due to the potential for false-detections to result in loss of operationally critical communications.

C2 Proactive Security Event Discovery

The purpose of the proactive security event discovery technical countermeasures is to enable detection of malicious activity within relevant IACS that is not identified with more standard security monitoring.

Proactive security event discovery should only be used once good quality security monitoring (C1) is well established. These further measures could also be implemented in situations where other required security countermeasures could not be implemented to provide equivalent protection, where risk is particularly high or where a cyber incident is suspected.
However, care must be exercised as many of these techniques can cause failure of real-time operational assets.

Countermeasures for Relevant and Critical MA/LES IACS

1. Optional use of Vulnerability Scanners – (as described in IEC62443-3-1). Vulnerability scanning remains a challenge in IACS environments as many real-time control and safety systems may be taken offline by scanning. It may be optionally used at the higher levels of the IACS network hierarchy or other less operationally critical assets and networks or opportunistically during plant downtime so as not to affect online systems. It may also be useful for testing purposes on offline systems or new systems prior to introduction.
2. Optional use of Forensics and Analysis Tools (FAT) – (as described in IEC62443-3-1). These tools may optionally be deployed to determine a normal network baseline and detect / respond to unusual network activity or to test the operation of specific countermeasures. Again, care must be taken to ensure that online systems are not compromised when used. Where used the purpose and scope should be well defined.
3. Optional use of Penetration testing. Penetration testing remains a challenge in IACS environments as many real-time control and safety systems may be taken offline by testing. It may be optionally used at the higher levels of the IACS network hierarchy or other less operationally critical assets and networks (especially for situations where other required countermeasures could not be implemented) or opportunistically during plant downtime so as not to affect online systems. It may also be useful for testing purposes on offline systems or new systems prior to introduction.

Countermeasures for Critical MA/LES IACS

No additional countermeasures