Considerations for Cybersecurity during the Functional Safety Lifecycle

1 Contents

2 Revision History

Version	Date	Author	Comments
1.0	11/11/2020	PB	Initial release

3 Introduction

As computer technology has advanced, it has become smaller, more powerful and cheaper. These factors have helped to see the integration of computers into many products. One technology to have benefited greatly from this revolution is Industrial Automation and Control Systems (IACS). The Operational Technology (OT) used in control systems have gained better connectivity, easier configuration and access to process data that can be transmitted in real time, across a business.

As business requirements have changed, a growing demand to merge real time data from processes and manufacturing with business data has created the need to integrate corporate information technology (IT) network domains with localised OT production domains. This has resulted in dynamic business operations, Industry 4.0 / IIoT efficiencies and flexible batch / outputs to meet unique demands. The modernisation of plant, machines and equipment to meet these new requirements has also resulted in a requirement for greater connectivity between IT and OT systems which triggers another requirement for better collaboration between IT Engineering and Support teams and OT Engineering and Support teams. These advances have introduced potentially dangerous challenges, as connectivity and flexibility of IACS has increased so has the potential threats and the vectors from which those threats may emerge. From well-meaning but misguided insiders to malware that targets IACS and safety related systems.

Many forms of legislation have emerged or are emerging that require action on cybersecurity. In the UK the adoption of the Network and Information Systems (NIS) Directive, Control of Major Accident Hazards (COMAH) Regulations (with support from HSE OG-0086) and probably the soon to be updated Machinery Directive all have, or will have, requirements for cybersecurity. In functional safety there are widely accepted international standards that define our approach to a safe solution e.g. IEC 61508, IEC 61511, IEC 62061 and ISO 13849. Cybersecurity, as a much newer topic to industry, has an international standard, IEC 62443, but as it is newer the standard is not as widely accepted and / or implemented. One of the things that all these international standards have in common is they use, as a backbone, some form of management system and lifecycle. If IT and OT teams are going to collaborate better then these management systems will also be required to either work alongside each other or integrate together. It is important to also align and assure the training / competence of the IT and OT teams but this topic is not discussed in this document.

While functional safety and cybersecurity are large complex topics, this paper is only focusing on a limited scope. The aim of this paper is to compare and contrast Functional Safety Management (FSM) and Cybersecurity Management (CSM) to aid collaboration between IT and OT functional teams. There is no safety without cybersecurity and the more we analyse our cybersecurity risk the more safety challenges we will detect. This guidance document is aimed at the functional safety responsible person and is a discussion document for stakeholders. This paper does not cover the detail of the functional safety or cybersecurity lifecycles as these are covered in the relevant standards listed above.

For more information: The 61508 Association is a good source of information for Functional Safety (our details can be found at the bottom of this page). The UK National Cyber Security Centre (NCSC) is a significant source of information for cybersecurity. If you are new to the topic the NCSC *10 steps to cyber security* is a good starting point:
https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

4 Working Group Deliverables

1. Guidance on minimum information flow between the two lifecycles.
2. Guidance on a basic schedule for information flow.
3. Lifecycle maps to graphically represent the schedule and information flow. Figure 7.1 (section 7) and Annex A of this document contain the example lifecycle maps.

5 Scope

This paper will consider the industrial functional safety standards (IEC 61508, IEC 61511, IEC 62061, and ISO 13849) but the concepts can be adjusted and used in other sectors. As this paper is focused on the industrial sector cybersecurity standards, guidance from the industrial sector will also be considered (IEC 62443, HSE OG-0086).

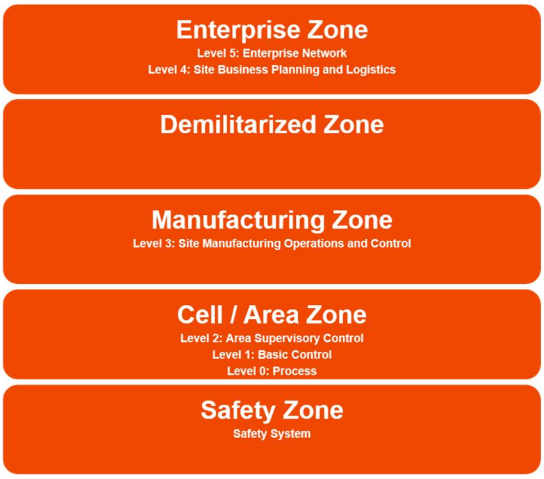
Functional safety and cybersecurity are complex topics however this paper will keep a narrow focus providing guidance and support for linking the two lifecycles. This paper focuses purely on safety-related systems. Control systems obviously also have requirements and an impact on both the functional safety lifecycle and the cybersecurity lifecycle but control system aspects are not covered in this paper.

As the cybersecurity lifecycle needs to be so much more dynamic than the functional safety lifecycle there is a slight difference in core philosophy. Typically for safety, management and planning is created and followed leading to reviews and updates. The cybersecurity lifecycle will probably go through a lot more changes through the life of the EUC. The cybersecurity lifecycle can be described as *Identify, Protect, Detect, Respond and Recover* (NIST Cybersecurity Framework) or the principles use by HSE OG-0086 as *Protect, Detect and Respond*. These two philosophies are pretty much the same it is just the descriptor that is different.

This discussion paper will consider the two management systems (for product, process and machine) in relation to functional teams, information requirements and overall responsibilities by lifecycle phase. This discussion paper will detail any problem areas and go on to discuss recommendations and possible solutions.

We have produced a few simple lifecycle maps to demonstrate where the functional safety and cybersecurity lifecycle could be synchronised. This is a point where information is required to flow between the two lifecycles before the project should proceed to the next phase. A project could move on without these synchronisations but this will result in at least part of a phase being re-worked. More synchronisation can be added if required. In practice the two lifecycles will not progress in synchronized harmony, each of the lifecycles will alternate in being slightly ahead of the other.
Please also read the paper "*Cyber Security – An introduction for Functional Safety Systems*" from *The 61508 Association* for general information.

Figure 5.1: Example Purdue Model


Enterprise Zone
Level 5: Enterprise Network
Level 4: Site Business Planning and Logistics
Demilitarized Zone
Manufacturing Zone
Level 3: Site Manufacturing Operations and Control
Cell / Area Zone
Level 2: Area Supervisory Control
Level 1: Basic Control
Level 0: Process
Safety Zone
Safety System

6 Acronyms and Abbreviations

CS team	- Cybersecurity team
CVE	- Common vulnerabilities and exposures
EUC	- Equipment Under Control
FS team	- Functional safety team
FSA	- Functional Safety Assessment
IT	- Information Technology
OG	- Operational guidance (UK HSE term)
OT	- Operational Technology
Pen testing	- Penetration testing

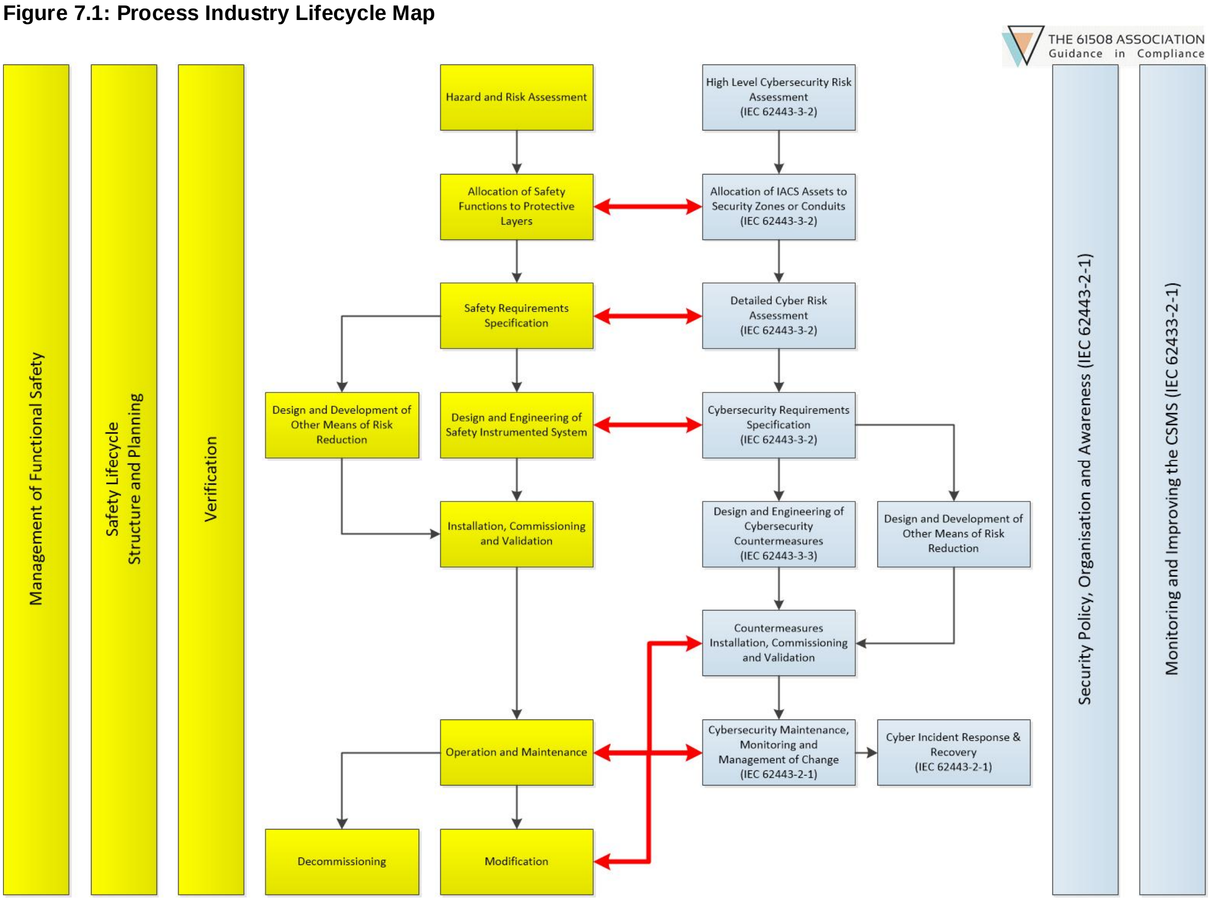
7 Management Systems

Management of functional safety combined with management of cybersecurity are key aspects to ensure a suitable and sufficient safety system. The two management systems, including support for planning, must be in operation prior to the start of the project. A pure IT cybersecurity management system is usually inappropriate for handling the cybersecurity of OT systems. A OT specific cybersecurity management should be defined before an attempt to link or harmonise the safety and cybersecurity lifecycles.

The two management systems do have some overlap (e.g. policy, competence, roles & responsibilities, management of change, incident planning) but also have significant areas of difference. For example, both managements systems require ongoing monitoring of performance but the detail in this area is very different between functional safety and cybersecurity. We therefore recommend that the two management systems are initially kept separate until the organisations involved in the processes are more comfortable with the approach. Limited aspects of each management system can then be merged together. The reason for this approach is that the clear majority of organisations will have a mature functional safety management system but will have a recent and developing cybersecurity management system. One aspect of the management system that is generally easy to combine is maintenance planning and activities as these generally need to be tied together anyway. The functional safety management system must also cover all cyber-critical elements, i.e. those elements that have been identified as offering a significant risk through a cybersecurity incident.

It is important to understand that there may be a very different culture between the functional safety and cybersecurity people and teams. Misunderstandings and clarifications need to be dealt with carefully.
The machinery lifecycle map (Annex A.1) shows management of functional safety covering the complete lifecycle for machinery. Officially IEC 62061 and ISO 13849 end the lifecycle at the *Operation* phase however legislative frameworks, e.g. the EU Machinery Directive, have management requirements for the later lifecycle that can be supported by a complete functional safety management system.
The HSE guidance document OG-0086 is not in its own right a management system and lifecycle however we recommend that at least a simplified cybersecurity management system (procedures) is followed when using this guidance, for example something based on ISO/IEC 27001 or IEC 62443-2-1.

Figure 7.1: Process Industry Lifecycle Map


THE 61508 ASSOCIATION
Guidance in Compliance
Management of Functional Safety
Safety Lifecycle Structure and Planning
Verification
Hazard and Risk Assessment
Allocation of Safety Functions to Protective Layers
Safety Requirements Specification
Design and Development of Other Means of Risk Reduction
Design and Engineering of Safety Instrumented System
Installation, Commissioning and Validation
Operation and Maintenance
Decommissioning
Modification
High Level Cybersecurity Risk Assessment (IEC 62443-3-2)
Allocation of IACS Assets to Security Zones or Conduits (IEC 62443-3-2)
Detailed Cyber Risk Assessment (IEC 62443-3-2)
Cybersecurity Requirements Specification (IEC 62443-3-2)
Design and Engineering of Cybersecurity Countermeasures (IEC 62443-3-3)
Design and Development of Other Means of Risk Reduction
Countermeasures Installation, Commissioning and Validation
Cybersecurity Maintenance, Monitoring and Management of Change (IEC 62443-2-1)
Cyber Incident Response & Recovery (IEC 62443-2-1)
Security Policy, Organisation and Awareness (IEC 62443-2-1)
Monitoring and Improving the CSMS (IEC 62433-2-1)

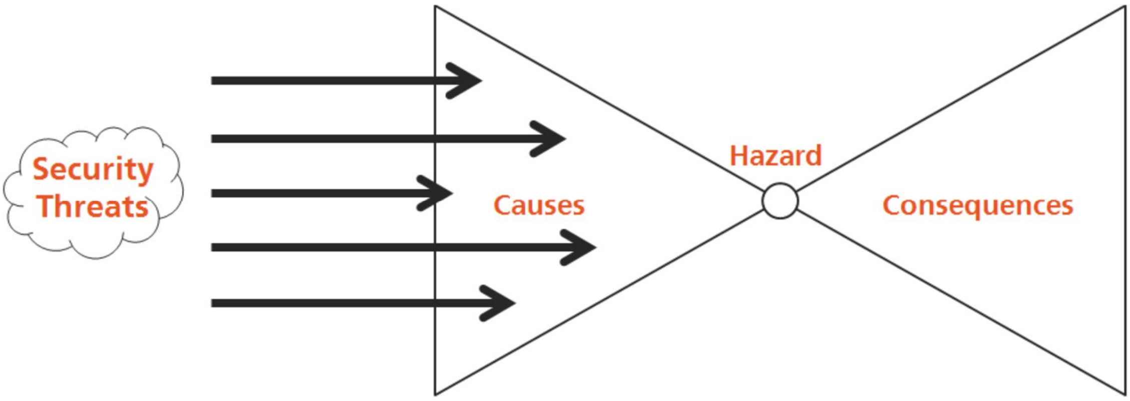
8 Lifecycle and Planning

When defining the roles and responsibilities as part of the planning the FS team needs to ensure they nominate a FS cybersecurity contact for the CS team to liaise with and that cybersecurity aspects are included in the roles and responsibilities. This person does not need to be an expert in both fields but should have sufficient awareness of both to communicate with both sides and understand when they don't understand something. It is very important that both the FS team and CS team have clear and communicated roles and responsibilities. Communication mechanisms and coordination procedures will be required to support the teamwork (this document can aid with this). The CS team should consider nominating a CS functional safety contact for the FS team to liaise with especially for high hazard industries.

Early in the project some consideration should be put into defining the approach to cybersecurity for the Functional Safety Assessment (FSA). If you are making first tentative steps into cybersecurity we recommend starting with simple questions such as:

> Are hazards mapped to any security threat that are understood to be the cause of a hazard? (see figure 8.1 below)
>
> Are you satisfied that the level of security protection in place is proportional to the level of safety risk?

Figure 8.1: Security threat bow tie



The FS team will also need to adjust their usual FS lifecycle phase inputs and outputs to include synchronisation points between the FS team and the CS team. If they wish to the FS team could liaise with the CS team at the start / end of every lifecycle phase then this is excellent but may prove impractical or ambitious. A minimum number of synchronisation points, between the FS team and CS team, shall be setup and the Figure 7.1 / Annex A of this document recommend lifecycle phase synchronisation points by a red arrow detailed on each lifecycle map.

It is not possible to detail exactly what information is required to pass between the FS team and CS team as these synchronisation points will vary dependent upon many factors including application sector, safety risk, security threat, equipment complexity and system size. If, as with many people, cybersecurity is a relatively recent consideration the first step should be to encourage communication between the FS & CS teams which will in turn develop the details of which information is required to be exchanged.

Examples of information exchange between teams:

1. Once the *Allocation of Safety Functions to Protective Layers* is complete the FS team needs to make this information available to the CS team including an explanation of the independence requirements to enable the *Allocation of IACS to Security Zones or Conduits*. This should explain to the CS team why any extra interfaces or conduits are required.
2. During these same two *Allocation* phases the two teams will need to discuss and agree how the safety-related system fits into the zones and into which zone will all the other safety-related assets sit.
3. Once the CS team has completed the *Allocation of IACS to Security Zones or Conduits* the information will need to be provided to the FS team to enable the development of the *Safety Requirement Specification* detail.

4. Once the FS team has completed (or nearly completed) the *Safety Requirement Specification* then the specification, preferably with a networked device / software summary, needs to be sent to the CS team so they can start the *Detailed Cyber Risk Assessment*.

9 Risk Assessment and Safety Requirements

Both functional safety and cybersecurity use a risk based approach which means that both areas require some form of hazard (functional safety) or threat (cybersecurity) analysis followed by risk estimation, risk analysis and risk evaluation which will then lead, with sufficient measures, to adequate risk reduction. The approach for each will be different but risk assessment is a key start point for each lifecycle. The cybersecurity risk assessment will need a more frequent time or event driven review when compared to the safety risk assessment.

The objective of the hazard and risk assessment combined with the allocation of safety functions is to develop a sufficient understanding of the system (identification of assets and scope) to ensure a proper safety, and now cyber, performance. We recommend that the safety hazard analysis is performed prior to any detailed cybersecurity threat and risk analysis. The safety hazards and risks are generally static unlike the cybersecurity threats and risks which will be very dynamic requiring a much more frequent review.

There does need be some cybersecurity input into the safety hazard and risk analysis which is reinforced by IEC 61508-1:2010 sub-clause 7.4.2.3 which has a requirement for a security threats analysis as part of the hazard and risk analysis phase. We therefore also recommend that a high-level cybersecurity risk assessment is performed prior to the safety hazard and risk analysis. The high-level cybersecurity risk assessment is used to determine the business and health & safety impacts in the case of breach, compromise or incident. This high-level assessment does not have to go into detail about how an attack could be performed but an awareness should be held of what a credible attack would look like to inform this process.

The high-level health & safety impacts are required for the safety hazard and risk analysis. Once the safety hazard and risk analysis is complete the safety lifecycle can move to the safety specification phases (e.g. allocation of safety functions to protective layers, safety requirements specification). For the safety design, think about defence in depth / layers of protection. Where you can remember to add in non-cyber affectable safety layers such as vent valves. Once a reasonable amount of specification information is available for the functional safety aspects it is possible for the detailed cybersecurity risk assessment to begin. As the functional safety specification proceeds and changes this will impact the detailed cybersecurity risk assessment and as the cybersecurity detailed risk assessment proceeds and changes this can impact the functional safety specification. This portion is therefore a two-way iterative process until both tasks are considered relatively complete. IEC 61508-1:2010 sub-clause 7.5.2.2 calls for a vulnerability analysis at the overall safety specification phase which can be delivered via a detailed cybersecurity risk assessment. Ideally there would be very close synchronisation between the safety and security risk assessments. This is complex, hence why we have suggested the above approach. For less complex systems it may be practicable and better to perform a joint safety and security risk analysis if appropriate competence is available.

A conflict resolution process may be required as the FS team and CS team proceed through their risk and threat analysis processes to ease the two teams to a compatible technical solution. Some organisations can find allowing cybersecurity risks to influence the safety requirement specification a significant cultural challenge. Many people have been involved in functional safety for years and struggle to adapt to the fact that cybersecurity is an issue so they are not prepared to make changes to mitigate the risk. Consideration for cultural issues should be a key part of any safety or cybersecurity management system.

Again, if someone is new to cybersecurity we would recommend starting by adding in simple cybersecurity related questions into the safety hazard and risk analysis process. Which of the risk reduction measures are configurable, programmable, contain software, complex electronics or connectivity such as network ports and therefore could be impacted by cybersecurity? How can the zones and conduits impact the hazard and risk analysis? Is there a common cause cybersecurity aspect that could remove most or all of the layers of protection? During the safety hazard and risk analysis process it is important to consider possible new *hazardous situations* and possible *combinations of hazards* (safety) *and threats* (cybersecurity).

It is important to remember that for cybersecurity the risk assessment should cover both major accident hazards and loss of essential services consequences if these are applicable e.g. the EUC is covered by COMAH and NIS.

9.1 Security Zones and Conduits

The output of the high-level cybersecurity risk assessment is an input into allocating (or grouping) of IACS assets into security zones or conduits. The start of the definition for the security zones and conduits can only begin once the majority of the safety functions have been allocated to protective layers. The security zones and conduits will have an impact on the safety requirements specification and so at least the safety-related system portion of the zones and conduits should be defined before the SRS is finalised. The zones and conduits can possibly affect the allocation of safety functions to protective layers therefore there could be a link between these steps.

As part of the security concept there will be a natural inclination to reduce the number of interfaces and conduits on a system but it is important to understand that functional safety may require extra layers, i.e. extra interfaces / conduits, that are independent. In general, a balance of requirements between those of the functional safety world and the cybersecurity world needs to be achieved. Some people focus on complete isolation (an air gap) as a cyber defence, it is important to remember that defence in depth is the best approach and no single layer of defence, including the air gap, is sufficient in itself for cybersecurity.

9.2 One or Many Cybersecurity Risk Assessments

The above description of the cybersecurity risk assessments could be one big assessment that is split over various times and resources or it could be considered as multiple separate assessments. It does not really matter as long as the general process is followed, the outputs are delivered and link with the functional safety lifecycle is intact. As examples the UK HSE OG-0086 discusses a single cybersecurity risk analysis but IEC 62443-3-2 (published while this working group output was being finalised) discusses a high-level risk assessment and then later a detailed risk assessment. Both mechanisms are valid approaches to cybersecurity for IACS. A suitable output from the activity is the most important aspect.

10 Design and Engineering of Safety-Related Systems

Once the safety requirements specification and the detailed cybersecurity risk assessment are complete the design and engineering of the safety-related system can begin. Alongside this the final details can start to be added to the cybersecurity requirements specification and the two separate phases from the two different lifecycles can have an impact on each other so these two tasks need linking to ensure relevant information exchange.

The cybersecurity requirements specification can actually be started a lot earlier than this as some of the detail (e.g. regulatory requirements, asset owner requirements, basics of the threat landscape) will be available prior to the start of the project. Other requirements (e.g. short description of physical and logical environment for equipment, details on how components connect to network technology, implementation of cybersecurity controls) can only be defined once the design and engineering for the safety-related system is mainly completed.

If the safety-related system utilises programmable electronics then these components shall have cybersecurity related features or other components shall be added to the system design that do provide suitable and relevant cybersecurity features. These cybersecurity features shall be enabled considering the application and balancing usability with security. A cybersecurity *defence-in-depth* approach shall be utilised. The cybersecurity requirements specification shall define the zones and conduits for all systems.

Once the design and engineering of the safety-related system is complete the safety lifecycle can move onto the installation, commissioning and validation phase. Once the cybersecurity requirements specification is complete the cybersecurity lifecycle can move onto design and engineer the various cybersecurity countermeasures. These two phases can be undertaken independently as there is very little common ground between the two phases.

10.1 Safety Commissioning and Validation

Safety-related system installation can be started before all the cybersecurity countermeasures are engineered. Care needs to be taken during the installation, commissioning and validation phase for safety-related systems. Technology could be powered up with minimal or no cybersecurity countermeasures in place but still exposed to cybersecurity threats. We strongly recommend therefore that at least some minimal level of cybersecurity countermeasures are in place before commissioning takes place. A significant portion of the cybersecurity technology should be in place from FAT onwards, this is possible if the cybersecurity requirements specification is started early allowing the selection of basic countermeasures. This will security testing to take place at FAT and onwards ensuring devices are correctly configured prior to commissioning.

A defined safety-related system installation and commissioning cybersecurity approach / procedure is required. We recommend as a minimum physical security, backup / recovery, patch management, anti-virus, device hardening, accounts / credentials setup and logging / monitoring are all available prior to the start of safety-related system commissioning (if they are applicable to the application). We strongly recommend that safety-related system validation only takes place once all the relevant cybersecurity countermeasures are in place.

10.2 Other Means of Cybersecurity Risk Reduction

Not all cybersecurity countermeasures can directly be linked to a system. Just like in safety-related systems layers of protection are used to achieve the desired outcome. Other forms of risk reduction for cybersecurity are aspects of physical security (preventing access to systems and infrastructure) and policies and procedures (change control, competence and account management).

11 Operation, Maintenance and Modification

Safety operation should never be started without all the relevant cybersecurity countermeasures in place. In other words, the cybersecurity countermeasures must be installed, commissioned and validated before safety operation is allowed to commence. The cybersecurity monitoring also must be operational prior to the start of safety operation. It is essential that during operation both safety and cybersecurity have linked management of change and planned preventative maintenance activities to maintain the require safety integrity and cyber resilience.

The machinery functional safety standards, IEC 62061 and ISO 13849, have a lifecycle that ends when the machinery is placed into *Operation*. Pre-operation checks will be required to ensure that suitable cybersecurity countermeasures are in place.

It is recommended that safety-related controls that have been identified as having a significant risk for cybersecurity have a mechanism for sequence of event recording. All unusual safety-related system issues and unknown trips shall be investigated before a start / re-start. The cybersecurity monitoring solution / mechanism must also be in place and in operation before start / re-start.

All methods of access and remote access shall have been designed into the system and considered in the safety and cybersecurity risk assessments. If not, the project shall return to an earlier phase of the lifecycle to assess, specify, design and validate the access / remote access mechanism.
If during the operational life of the system a specific substantial threat is identified this shall trigger a review of the cybersecurity risk assessment.

Proof testing of safety functions must include testing aspects for relevant security measures to ensure these also still perform as intended. This may need to include penetration testing associated with the safety function. In general, Pen testing for IACS can be problematic. If Pen testing for IACS is required this should be planned carefully and further guidance sought. The required proof test interval may differ from the performed penetration test interval.

11.1 Maintenance

The threat environment that a system faces will change over time. A key maintenance requirement therefore is a periodic review of the cybersecurity risk analysis the results of which shall be recorded and under change control.

Maintenance does not now just cover maintenance of the equipment under control but also cybersecurity aspects and cybersecurity countermeasures. The overall safety-related system maintenance planning should include reference to these even if they are completed by another resource to ensure these tasks are completed. As examples maintenance is required for accounts (for when people leave), updating / patching of software for security reasons (tested and assessed before deployment) and configuration control (is the system the same as before). The maintenance plan should include activities to test out the cybersecurity countermeasures to ensure they are still protecting the system(s). All maintenance devices shall have been designed into the system and considered in the safety and cybersecurity risk assessments. If not, the project shall return to an earlier phase of the lifecycle to assess, specify, design and validate the device. The maintenance plan and procedures shall detail requirements for if there is a requirement to send project information / files off site for fault finding purposes or modification including aspects for loss of critical data.

Maintenance aspects also need to cover the disaster recovery approach ensuring that the IACS has options for respond, recover, wipe and start again.

11.2 Modification

Both functional safety and cybersecurity require change control procedures which are interlinked, this includes aspects of configuration control. Modification requests for the safety-related systems shall trigger an impact analysis which will consider not only the safety but also cybersecurity and associated countermeasures. Modification to cybersecurity countermeasures shall also trigger an impact analysis which will consider not only cybersecurity but also the safety-related system. This may result in a change, engineering and re-validation of part or all of the safety-related system. Authorisation for changes shall be made by the relevant team, this probably means a dual authorisation process. Modifications to safety-related systems can lead to new security vulnerabilities so the impact analysis may call for a new or updated security risk assessment. Either before or as security measures are changed (including patching) analysis and tests shall be conducted to verify safety function performance.

Modification to the safety-related system or the cybersecurity countermeasures shall be controlled using credentials. Significant cybersecurity modifications, such as changes to zones, conduits, networks and systems shall not be allowed without re-visiting earlier phases in the lifecycle. All safety-related modifications shall follow the approach defined by the relevant functional safety standard(s).

Security driven changes or updates could affect the integrity of the safety related system in which case a special risk assessment and careful coordination and communication between the FS team and CS team may be required to reach a resolution. This process may identify special compensation measures which would need approval from both the functional safety and cybersecurity responsible person. Any vulnerabilities should be carefully tracked, monitoring and managed during this coordination process. Modification also needs to cover disaster recovery aspects including backups for any changes made.

11.3 Monitoring

Monitoring of the IACS for cybersecurity threats and status is a very important tool from the defence in depth approach. Functional safety also uses aspects of monitoring to look for potential or actual failures during operation. These two types of monitoring are different and don’t need to be combined however the resulting data can be useful in combination. For example, if a safety device is shown to have abnormal operational characteristics the cybersecurity monitoring data should be reviewed to see if it could have been as a result of a threat / incident. In general, all forms of monitoring are good tools to improve the efficiency of any system but too many monitoring tools should be avoided else someone may end up spending a lot of time assessing false positives. Monitoring tools can either be onsite or offsite but either way the tools themselves are a possible attack surface. If the cybersecurity monitoring is tracking safety related or functional safety aspects then consideration can be given to automated shutdown on monitoring issues but a balance for availability / denial of service needs to be included.

12 Functional Safety Assessment

Some of the functional safety standards that may have been used for a project have a formal requirement for functional safety assessments or FSAs. As the functional safety standard may require that the safety related system design provides the necessary resilience against any identified security risks the FSA should consider those aspects of cybersecurity that can impact safety performance or safety integrity.

13 Other Issues

ISO/TR 22100-4 states the following:

Legal frameworks for putting a machine into service or placing it on the market for the first time (responsibility of the machine manufacturers) and ISO 12100 restrict the scope of safety of machinery to the "intended use" and the "reasonably foreseeable misuse" of a machine. Every kind of intentional violation (sabotage/spying) of a machine is de facto a criminal act which is outside the scope of current safety legislation. Consequently, it is also out of the scope of standardization for safety of machinery, which supports such legislation.

ISO/TR 22100-4 does however go on to state:

However, manufacturers providing machinery which can have vulnerabilities to IT-security attacks and/or threats should take this aspect into account in particular when IT-security attacks and/or threats can have an impact to safety of machinery.

However, ISO 12100 defines *reasonably foreseeable misuse* as:

Use of a machine in a way not intended by the designer, but which can result from readily predictable human behaviour.

A key question for any risk assessment (especially for machinery) is therefore; *is a cybersecurity incident reasonably foreseeable?* The risk assessment team should consider the level of sophistication of an attack (therefore the level of defence that should be considered) and should be based on suitable threat actor information. For the UK we recommend that the NCSC information on threat actors is used as a baseline supplemented with any extra specific intelligence for a particular industry/operating environment. Publicly available information on threat actors from the NCSC is available via the NCSC and NCA (2017) "The Cyber Threat to UK Business 2017-18 Report". Threat actor information is also available for countries other than the UK.

13.1 Assessing Products

The assessment of a system, by a system integrator, and the assessment of a product, by the product manufacturer, typically have different requirements, for example the IEC 62443 series covers these in different parts. When the assessment is on a product which can be used in many different applications then the cybersecurity approach is required to be quite generic.

A generic assessment of a product looking at the vulnerability of the hardware (USB ports etc) and the firmware (looking for CVEs) can be undertaken which can also include aspects for production excellence. Generic assumptions can be made for threats and risks but most of this detail will come from any final application. If the lifecycles are being used to assess a product, for example a Programmable Logic Controller (PLC) or Variable Speed Drive (VSD), focus should also be given to ensuring that the device can only function as intended; you can only properly mitigate cybersecurity risk for a system when you consider the risk for final system / application. A piece of equipment or machine may need to be treated in a similar way to a product.

A product should have some level of cybersecurity assessment by the manufacturer and then a full cybersecurity assessment by the integrator. The integrator will need to take in to account the application specific configuration/software development as part of the cybersecurity assessment.

14 Existing and Emerging Standards

14.1 Functional Safety / Safety Standards and Guidance

IEC 61508-1:2010 *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*
IEC 61511-1:2017 *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definition, systems, hardware and application programming requirements*
IEC 62061:2015 *Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems*
ISO 13849:2015 *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*
ISO/TR 22100-4:2018 *Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*

14.2 Cybersecurity Standards and Guidance

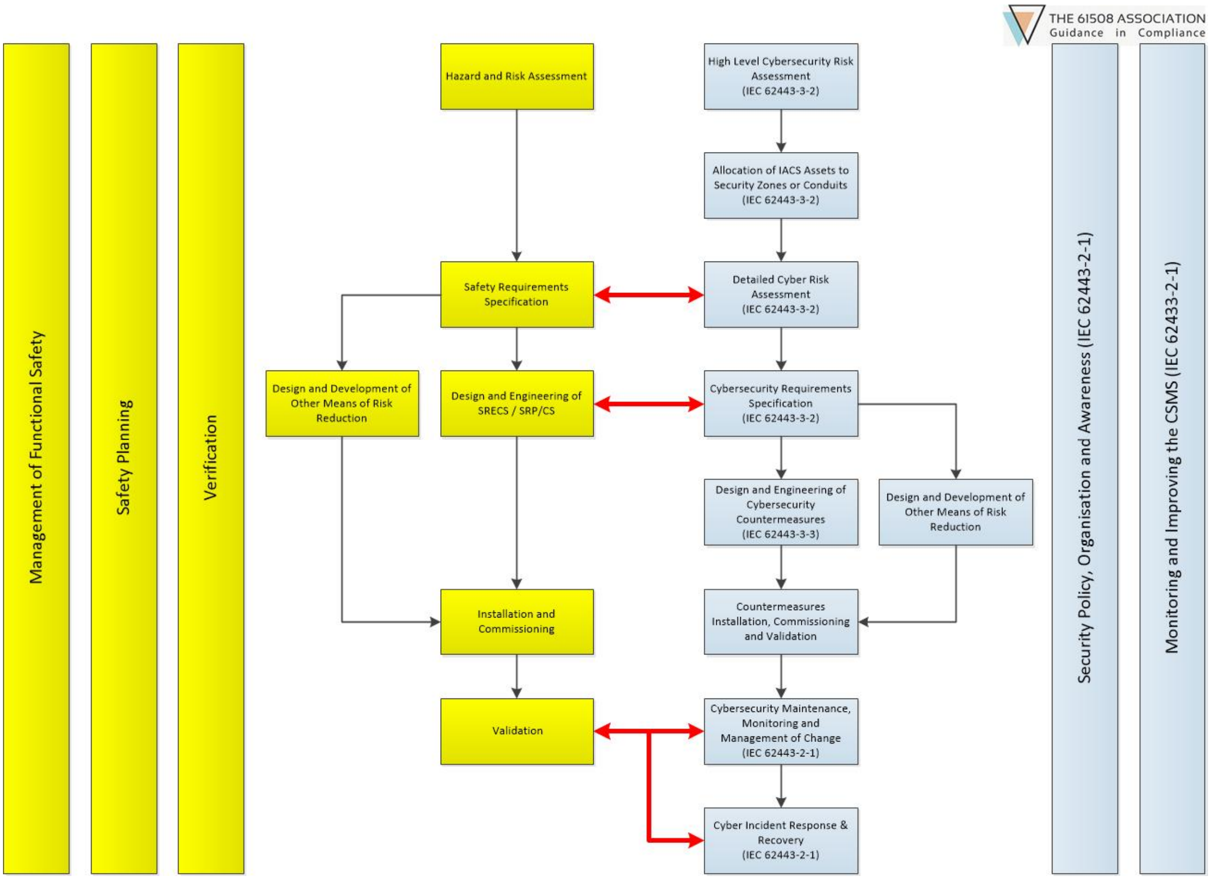
IEC 62443-2-1:2010 *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*
IEC 62443-2-4:2017 *Security for industrial automation systems – Part 2-4: Security program requirements for IACS service providers*
IEC 62443-3-2:2020 *Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design*
HSE OG-0086:Edition 2 *Cyber Security for Industrial Automation and Control Systems (IACS)*
IEC TR 63074:2019 *Safety of machinery – Security aspects related to functional safety of safety-related control systems*

15 61508 Association Recommended Practices

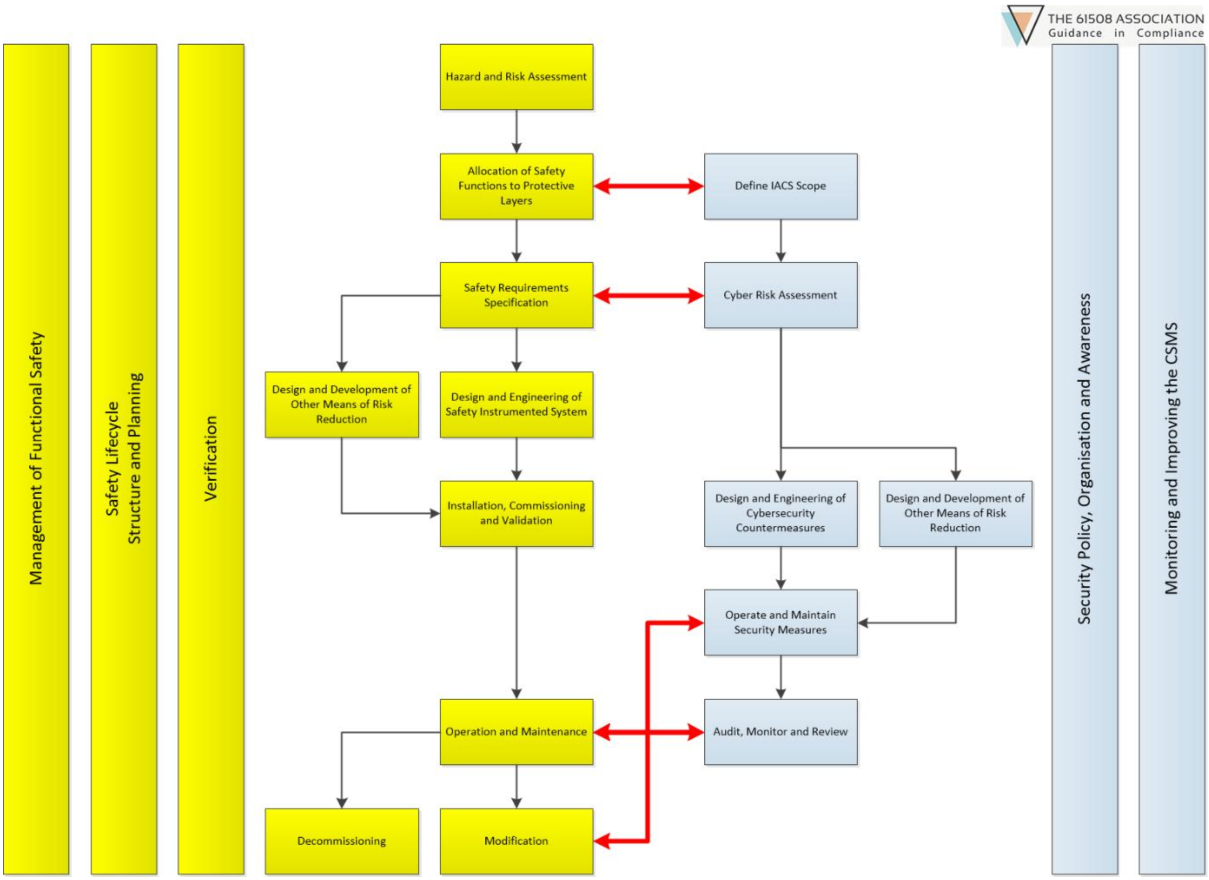
This document sets out to describe current best practices in management system and lifecycle handling for functional safety systems, but does not seek to prescribe specific measures, since these will depend on the application, and any existing constraints of the installation.

Annex A – Lifecycle Maps

Annex A.1 – Machinery Lifecycle Map


THE 61508 ASSOCIATION
Guidance in Compliance
Management of Functional Safety
Safety Planning
Verification
Hazard and Risk Assessment
Safety Requirements Specification
Design and Development of Other Means of Risk Reduction
Design and Engineering of SRECS / SRP/CS
Installation and Commissioning
Validation
High Level Cybersecurity Risk Assessment (IEC 62443-3-2)
Allocation of IACS Assets to Security Zones or Conduits (IEC 62443-3-2)
Detailed Cyber Risk Assessment (IEC 62443-3-2)
Cybersecurity Requirements Specification (IEC 62443-3-2)
Design and Engineering of Cybersecurity Countermeasures (IEC 62443-3-3)
Design and Development of Other Means of Risk Reduction
Countermeasures Installation, Commissioning and Validation
Cybersecurity Maintenance, Monitoring and Management of Change (IEC 62443-2-1)
Cyber Incident Response & Recovery (IEC 62443-2-1)
Security Policy, Organisation and Awareness (IEC 62443-2-1)
Monitoring and Improving the CSMS (IEC 62433-2-1)

Annex A.2 – Process OG-0086 Lifecycle Map



THE 61508 ASSOCIATION
Guidance in Compliance
Management of Functional Safety
Safety Lifecycle Structure and Planning
Verification
Hazard and Risk Assessment
Allocation of Safety Functions to Protective Layers
Define IACS Scope
Safety Requirements Specification
Cyber Risk Assessment
Design and Development of Other Means of Risk Reduction
Design and Engineering of Safety Instrumented System
Installation, Commissioning and Validation
Design and Engineering of Cybersecurity Countermeasures
Design and Development of Other Means of Risk Reduction
Operate and Maintain Security Measures
Operation and Maintenance
Audit, Monitor and Review
Decommissioning
Modification
Security Policy, Organisation and Awareness
Monitoring and Improving the CSMS

** End of Document **