Developing a Combined Lifecycle Management Approach for Both Functional Safety and Security for SIS

John Walkington, Global Manager, ABB FSM Technical Authority, ABB Limited, Durham, UK

Suresh Sugavanam, Senior Consultant, ABB FSM Technical Authority, ABB Limited, St Neots UK

The IEC safety standards[1] [2] identify the need for completing cyber security risk assessment to provide the necessary resilience against security risks. This paper will present one approach to developing a 'combined lifecycle management requirement' in bringing together the similar processes and competencies that are necessary to achieve a combined IEC 61511[2] and IEC 62443[3] compliant approach.

Functional Safety, Cyber Security, Lifecycle Management, Industrial Automation Control Systems.

Introduction

As we all recognise, there is no such thing as a 100% or absolute security application / implementation approach to securing industrial automation control systems (IACS). Industry presently recognises that cyber security is not a final destination, but an evolving target.

Cyber security at its heart is not solely about the capabilities of any specific product, but one that is predicated upon an overall management process which is really about finding the right balance regarding the impact on systems usability, competency & comprehension and the relationship to cost of ownership, since achieving higher security levels (which is supported with countermeasure implementation) may result in less convenience to the user. Invariably, Cyber security is all about security management system and the associated impact into today's IACS technology which we recognise currently possess the following high-level features:

- Leverages commercial off the shelf IT components
- Uses standardized, communication protocols
- Are distributed and highly interconnected
- Uses mobile devices and storage media
- Based on software (> 50% of manufacturers offerings are software-related)
- Can be highly specialized and complex IT systems

So, in terms of risk management, we can establish that several Cyber Security issues will need to be successfully managed across the lifecycle of the IACS assets where such modern integrated power & control technologies provide the following risk dimensions:

- Increased attack surface as compared to legacy, isolated systems
- Communication with external (non-OT) systems and exposure to attacks from/over the IT networks
- IACS patches and software updates which can negatively affect IACS performance

Leveraging many commercial off the shelf IT components and using standardized IP based communication protocols brings with it several good reasons regarding the benefits for such application solutions to the Asset Owners (e.g. interoperability). However, attacks are real and have an actual safety, health, environmental, and financial impact so we need to ensure the security of the dedicated IACS given their role and interconnectivity to potential threats.

Managing the Risk

We understand that IACS are in addition to their core functionality, highly distributed and interconnected. Because of this dimension, such automation systems can be viewed as highly specialized IT systems that they themselves are exposed to the same threats that "normal" IT systems currently endure (e.g. such as used in the Enterprise environment).

There are available statistics (and more expected to be published as a constant reminder), that identify the rate of malicious attacks are increasing. Industry is seeing a significant rise in reported security incidents (either intentional or unintentional) and this rate has a trend that increases from year to year. As IACS include the increasing use of commercially off the shelf (COTS) hardware and software components (e.g. operating systems and protocols) that are increasingly interconnected with business networks, this driven by the Asset Owner community to leverage the inter-operability benefits is making the IACS susceptible to software-based attacks.

Among the organisational challenges that are required to be successfully managed for IACS, the development of a security risk management approach is now 'the must do activity' for any Process Industry project. It is required to establish how the cyber security challenges contribute to an organizations risk profile and address IACS security throughout its entire lifecycle. A unique challenge here is that historic data is largely unavailable and due to the dynamic nature of the threat landscape, may be of limited use in forecasts of the future risk exposure. Companies must thus find novel ways of defining cyber security related risks.

Organisational Risk Culture

In your organisation today, how often do the information technology (IT) and operational technology (OT) teams meet, communicate and regularly align security management and technical means of risk reduction across the Asset lifecycle? Experience may suggest that we continue to be in danger of a 'Silo working culture' as in the past, it was rare that such cross-fertilisation was apparent as IT/OT requirements were seen to be separate and distinct. However, in today's world are they really that different? Figure 1 below highlights a number of key factors that would need to be discussed regarding the alignment and convergence of the IT/OT organisation risk management culture.

Dimension	IT	IACS
Technology Lifecycle	3-5 years	20+ years
Availability	Occasional outages tolerated	Outages not tolerable
Response Time Performance	Usually not considered	One of the key parameters
Patching	Timely	Less Frequent / As Required
Cybersecurity Awareness	Good	Improving
Process Safety Risk Awareness	Usually not considered	Good
Changes	Easier to implement	More challenging to implement
Safety & Security Integrity Awareness	Reduced	Good

Figure 1 – Safety and Security Operational Dimensions

The impact of risk for this IT/OT operational remit is that in the best scenario of a vulnerability being exploited, is that we lose some product or business sales, however at the other end of the spectrum, there is the potential for harm to people, process assets and environment. Regarding IACS, here we have the differing potential for automation random failures versus a planned Cyber-attack.

For safety instrument systems (SIS) we recognise that the safety integrity level (SIL) is directly attributable to a defined level of risk reduction for the operational asset and the person most at risk on site; whereas the cyber security level (SL) could affect both plant and equipment onsite & offsite and have a greater impact on many more people. It can also have an adverse effect regarding the impact onto other emergency response systems such as fire water pumps, telecoms, etc. and therefore, many levels of attack are possible. For safety related systems, the risk is proportional to the probability of an unintentional human or device failure occurring and for the corresponding cyber SL, the severity of a successful attack being higher as it is an intentional and malevolent action.

Several recent publicised industry incidents identify several IACS vulnerabilities and attacks increasing in its sophistication. Imagine what would happen if a SIS was disabled and the BPCS set points were raised or set to manual on a high hazard manufacturing facility. Therefore, we can appreciate that Cyber-attacks on IACS can lead to:

- Off spec product / losing public or consumer confidence
- Equipment damage / production loss
- Environmental consequences / endangering public health
- Personnel injury / fatalities

It some situations, it could be argued that the cyber SL will generally be higher than the Safety Integrity Level for a specific plant because an attack can affect many systems/equipment simultaneously (common cause and common mode failures) e.g. as a reminder, SIL is usually related to individual risk and cyber SL may be related to the broader societal risk.

Why do we need a robust Lifecyle Management approach for IACS Cyber Security?

As mentioned earlier, IACS are increasing in accessibility and connectivity with the use of information technology (IT) solutions and off the shelf technology. This is further heightened by the fact that Businesses are continually developing their Information Management Systems (IMS) to gain a competitive advantage and so this means accessing information down at the IACS level and together with the use of standard operator interface platforms, provides the potential for increased vulnerability to a Cyber-attack.

In today's world, neither functional safety nor information technology are independent of one another. Safety Systems[4] and Cybersecurity are therefore dependent in allowing connectivity and exchange of data with other systems and within corporate networks. This increased level of integration provides significant business benefits including increased visibility of IACS and

common interfaces that reduce support costs and permit remote support. We have standards available for helping us in developing models, terms, and information exchanges that allow the IACS to share information in a consistent way.

However, this ability to exchange information increases IACS vulnerability to misuse and attack by individuals with malicious intent and introduces potential risks to the enterprise.

Managing Safety & Cyber Security - 4 key questions should be addressed?

Operating companies should have a plan and policy for security management. This requirement should have senior management comitment that is active and visible to achieve this goal. There are many things that should be undertaken to deliver such a plan and policy and they will require changes from many stakeholders from wthin the organisation. All of these stakeholders need to deliver on their responsibilities and play their part in the Cyber security change programme. To start the change regarding the safety and security of the IACS environment, an organization should ask itself 4 high-level key questions as identified in Figure 2 namely:

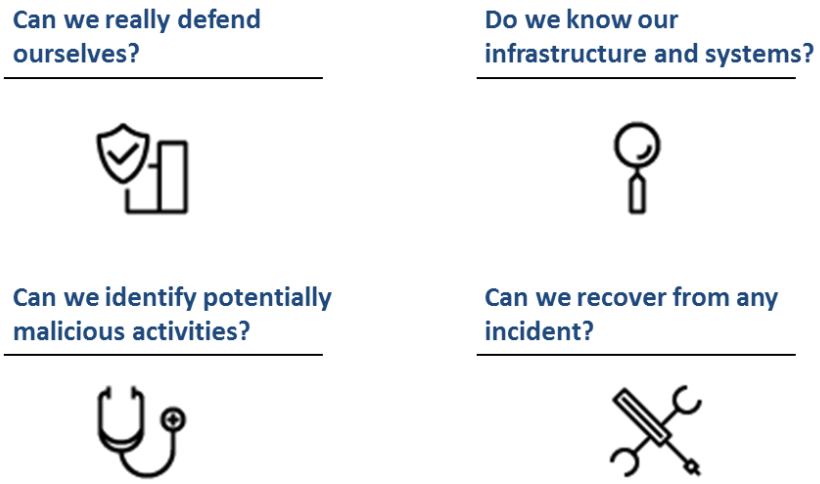

Figure 2 – 4 Key Security Questions to be Addressed

Essentially the development of a security management policy and management strategy should cover the following key principles:

- Our defense mechanism: Is it layered? Do we have defense in depth and robustness in place? Have we tested to verify this is the case?
- Know our system: What does it look like? Are the IACS boundary defined for the project? Is it ageing, distributed, maybe we carried out an upgrade of a subsystem lately? Do we have the latest topology, proper documentation, information about all assets/inventory database including IP address, OS used, applications installed? Where will I find all this information?
- Identify malicious activities: Have the security risk assessment been performed (which includes system vulnerability, threats, identification and counter measure requirements specification)? Have we implemented a proper level of monitoring? Do we have alerts active? Do we have the right logic in place to identify malicious activities? Have we tested our solutions? Have we tuned our solutions? Do we have competent people available to deliver and interpret such requirements?
- Recovery: Is the recovery plan and procedures available? If an incident did happen, do we know how fast we would be able to react and recover? Have we identified our strategy to achieve our goals? Do we have all the backups, right resources, competencies to achieve this in place? Are the staff trained in recovery procedure execution?

Proper Safety & Cyber Security Lifecycle Management

Given the risk management requirements associated with IACS and specifically for SIS as identified earlier, what do the organisational management requirements really need to cover? Experience would suggest that development of a strategy would need the following aspects to be established:

- Management Process
- Technology & Application Countermeasures
- Competency Assurance
- Human Factors

If we focus on the requirements of a lifecycle management process, then relevant Industry safety and security guidance identifies the following specific needs / requirements:

IEC 61511[2]: The policy & strategy for achieving functional safety shall be identified together with the methods for evaluating their achievement shall be communicated within the organisation.

IEC 62443[3]: Program designed by an organization to maintain the cyber security of the entire organization's assets to an established level of confidentiality, integrity and availability, whether they are on the business side or the IACS side of the organization.

ISA 84.00.09[5]: An organization's functional safety policy and strategy should be underpinned by an organizational cybersecurity strategy, both of which will be supported by robust performance measurement procedures.

Therefore, the goal for the organisation is to develop a comprehensive and combined safety and security lifecycle management approach that can be used to improve the safety, availability, integrity and confidentiality of components or systems used for IACS, and to provide the criteria for procuring and implementing secure IACS. Conformance with the requirements of the relevant industry standards is intended to improve programmable systems' security and help identify and address their vulnerabilities, reducing the risk of compromising confidential information or impairing the functionality or safety integrity of processes under control.

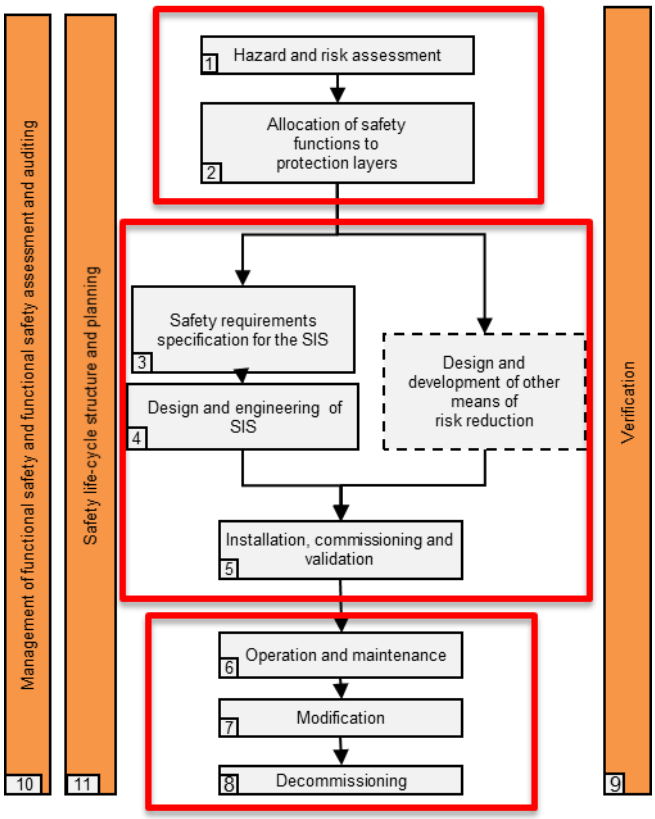

Figure 3 – IEC 61511[3] Safety Lifecycle

What will be important in the delivery of such a goal will be to avoid disruptive changes which would impact normal business operations while at the same time adopting cyber security practices in the organization and prioritizing on those changes which promise the biggest cyber security improvement.

At the heart of the implementation requirements will be the lifecycle management process itself. For the process safety community, following the IEC 61511 Safety Lifecycle is one approach to achieving the goals to meet functional safety requirements. By taking an overview of the lifecycle management diagram as found in IEC 61511 we can establish three Key management process stages (refer to Figure 3):

- Assessment Phase
- Develop & Implement Phase
- Operate & Maintain Phase

During the assessment and SIS development lifecycle phases there will be requirements to consider the impact of security, both physical and cyber onto the needs of the SIS. In doing so what does IEC 61511 specifically require for security for SIS?

If we further refer to IEC 61511 Ed 2 2016 Part 1 at Clause 8.2.4, the standard establishes the need for:

"A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices …;
- a description of identified threats …;
- a description of the potential consequences …;
- consideration of various phases such as design, implementation, commissioning, operation, and maintenance;
- the determination of requirements for additional risk reduction; a description of, or references to information on, the measures taken to reduce or remove the threats"

Further, at Clause 11.2.12, it identifies that:

"The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).

- NOTE Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010."

Here we can establish that the needs of the security risk assessment from IEC 61511, links across to the security requirements found in IEC 62443 to deliver the necessary conditions and potential countermeasures to be established for the SIS.

At the practical level, we need a coordinated IT/OT teams effort to achieve this requirement. At the design level for a SIS we require the functional design specification (FDS) to cover both the physical and cyber security requirements, so in other words we need the IT/OT departments working together.

So, what of the security requirements for the SIS? We know that IEC 62443 is a performance-based standard and so relies on a management process with competency assurance to underpin its goals in a similar way as to that of the safety standards.

Competency Management – Security / Cybersecurity

Ensuring awareness for cyber security risks and necessary countermeasures to be applied requires a learning and training programme to be established across the organization to adequately address them, but with an appropriate level of information for the individual's role (i.e. every employee should have the level of awareness that is appropriate for their specific role). Competence management including defining the cyber security aspects of organizational roles, defining cyber security specific roles in the organization, defining necessary skills for the individual roles and finding the appropriate people to fill the roles and ensuring continuous training to build and maintain the necessary competences for these people will be an important feature of the necessary security culture change.

So, before we focus more on the Lifecyle management process itself, none of this will matter unless we have a supporting competency assurance process in place as well. If we recall, the functional safety standard IEC 61511 warrants for:

- "Persons, departments, organizations or other units which are responsible for carrying out and reviewing each of the safety life-cycle phases shall be identified and be informed of the responsibilities assigned to them
- Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable
- A procedure shall be in place to manage competence of all those involved in the safety life cycle
- Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role"

Then by review of IEC 62443, there are very similar requirements identified as:

- "All personnel should receive adequate technical training associated with the known threats and vulnerabilities of hardware, software and social engineering
- In the area of IACS, the same emphasis should be placed on cyber security as on safety and operational integrity, because the consequences can be just as severe.
- Security awareness for all personnel is an essential tool for reducing cyber security risks. Knowledgeable and vigilant staff are one of the most important lines of defence in securing a system.

- It is therefore important for all personnel to understand the importance of security in maintaining the safe operation of the system"

Hence for any one organisation, it would be prudent to develop a competency assurance programme that as a minimum would raise the general awareness and appreciation of both aspects of safety and security so that responsible persons at least have a good idea of the joint challenges both the IT and the OT departments will need to consider successfully deliver a safe and secure automation solution.

Why is it worth to have a combined safety & cyber security lifecycle management approach?

The key benefit from this approach will essentially be for optimising the cost and effectiveness of safety & cyber security within the organisation. The primary issue is that both (security and safety) requirements need to be addressed during the

proper lifecycle phase e.g. the process of allocation of security and safety requirements for the IACS needs to be undertaken before systems design. If these both are not addressed at the proper time, the system design may well not include the development of appropriate safety/security protection measures.

A delay in this process may result with the system being designed and implemented without the necessary features being available to deal with the potential vulnerabilities & threats. Typically, this can be difficult to address and implement during later lifecycle phases. In other words, we can only properly address the specific safety and security requirements at the specific system lifecycle phases. This is why we need to consider an approach that can execute both lifecycle activities simultaneously.

So now we could start to argue that we should not treat the combined life-cycle approach as a benefit, but rather as a 'necessary condition' for proper implementation of both the standards requirements. We may have many sets of such requirements found in existing and independent QMS, FSM, CSM processes, however we have a single objective. Here we have similar requirements across safety and security for a management 'process' to be in place and one that is proven to be efficient and robust i.e. an integrated QMS/FSM/CSM/IMS[5] system (to provide focus, clarity and guidance).

Coordination and management of different types of 'Risks' for the identification of hazards, threats and vulnerabilities is therefore a common element in which such an integrated process environment will support centralisation, ease of review/maintenance and overall visibility.

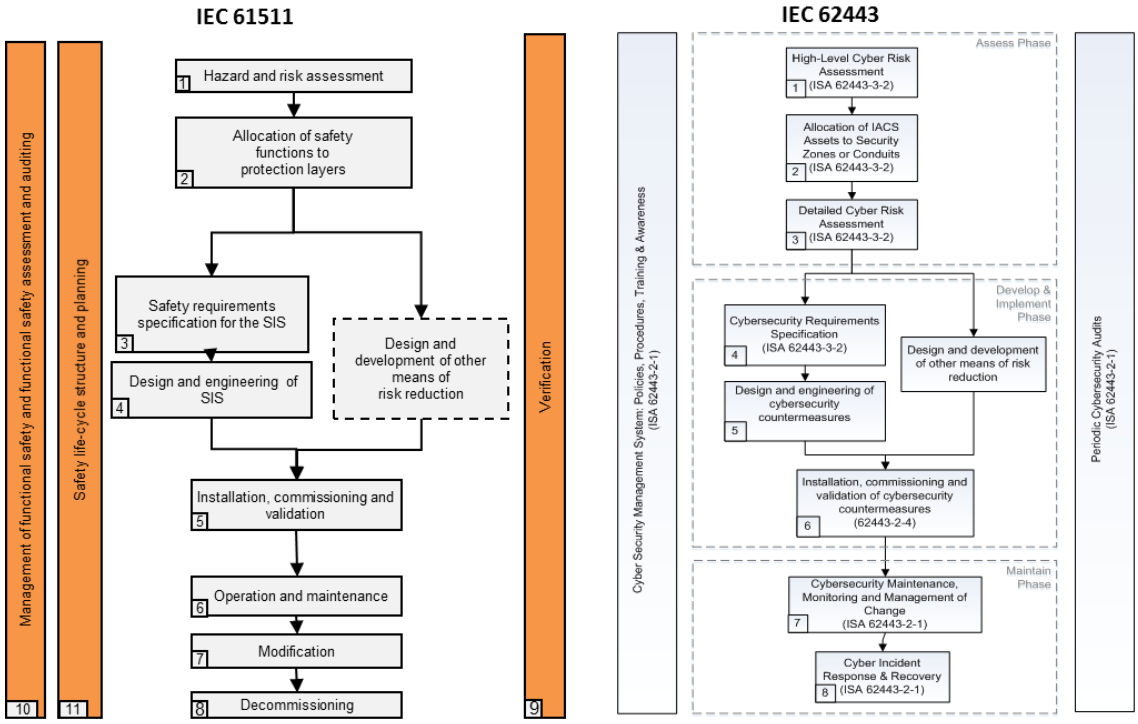

Figure 4 – Comparison of EC 61511 and IEC 62443[3] Safety and Security Lifecycles

To deliver, we will need similar phases to be applied for system lifecycle such as risk assessment, design, engineering, operation & maintenance, and in doing so, avoidance of any 'Silo Mentality' regarding roles, responsibilities, raising awareness and competency assurance, etc.

Such a combined lifecycle management approach would result in execution of similar performance-based requirements such as Audits and Assessments to support risk management/assumptions. This would therefore provide a common approach, schedule visibility, traceability to standards' requirements and support for effective culture change.

How can such benefits be achieved? Well, compare the security lifecycle with the safety lifecycle, by its very construction it essentially requires the same lifecycle management approach to be applied[6]. Refer to Figure 4.

Cyber Security versus Functional Safety: Similar, but different

When you break down the various lifecycle phases between both these Industry standards, you can establish the following similarities:

- Cyber Security and Functional Safety standards are both performance based
- Both call for well-defined management system supported by proper company policy, planning and implementation procedures
- Both are about processes (control and avoidance of human faults)
- Both require competency management
- Both require regular audit / assessment
- Both can cause potentially dangerous events
- In contrast, there are also the following key differences:
- Functional Safety process hazards are more predictable (hazards are generally known) than cyber threats and system vulnerabilities which evolves on a day basis
- Cyber Security risk is constantly changing (threats change due to technology obsolescence and the attacker is constantly evolving)
- Functional safety risk may be quantified, and Cyber Security risk is based on qualitative measures

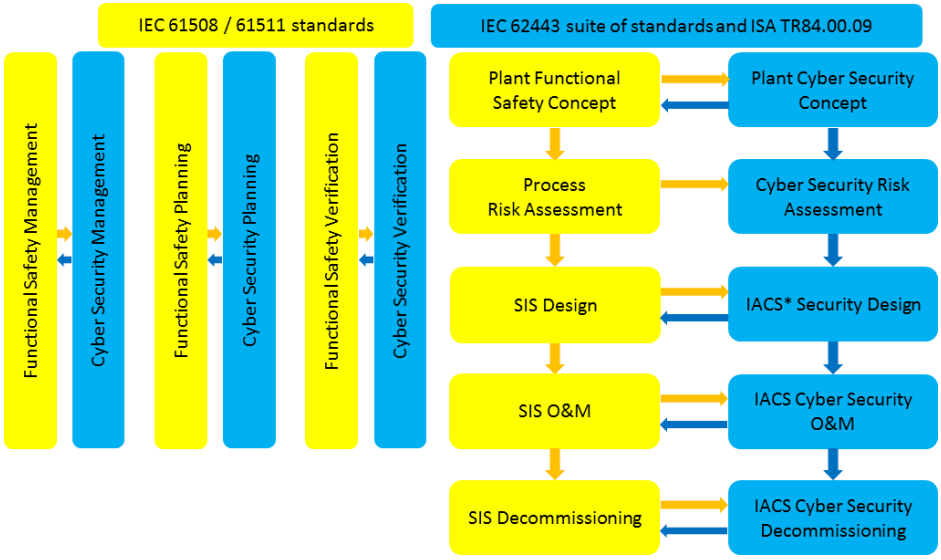

Figure 5 – Breakdown of Safety and Security Lifecyle Phase Management and Technical Clusters

We therefore need to be aware of similarities and differences for when integrating our combined safety and security lifecycle management processes e.g. for safety the risk can be quantified as a risk reduction factor say of 200; but for Cyber risk we are concentrating on the system vulnerabilities and likelihood of attack that are potentially evaluated more on a basis of personal experience and assumptions

Classification of the cyber risk may be identified as high or low, or some other qualitative levels, but essentially still not numerical (that said, we may have this type of risk quantified in the future, but experience suggests it is currently based on a qualitative measure). Hence breaking down the safety and security lifecycle further, the relevant management, verification and validation requirements can be seen as one significant cluster of a combined process, and the technical aspects a second cluster as identified in Figure 5.

One practical approach to develop a combined lifecycle management approach

So, to deliver a combined-integrated lifecycle management process, what needs to be considered for implementing a combined safety & security lifecycle requirement? One approach[7] to consider this achievement would be to facilitate the following implementation approach and for an integrated lifecycle management process to be established.

Process

Identify a systems champion within the organisation who is familiar with management processes and has the necessary seniority and skill set to get this implemented.

To achieve the systems / process review, develop some form of procedural mapping matrix to bring together the findings of the organisation against your targets of compliance e.g. refer to Figure 6.

Item	Targets of Compliance (DTC)	Lead Question & Additional Prompts for Clause Alignment	IEC 61511	IEC 62443	IEC 27001
1.1	**Functional Safety Management System** **and/or** **Cyber Security Management System** **and/or** **Information Management System**				

Figure 6 – Procedural Mapping Matrix

Next identify and develop a dedicated team with requirements from both the IT/OT environment to participate and apply their efforts to develop an integrated management set of policies, procedures and templates.

Develop a series of lead questions for information gathering and to establish the terms of reference for the integration assignment. Provide focus and structure for the management review process e.g. opening questions and expected responses / good practices. Refer to Figure 7.

Identify what is available within the organisation across the range of available procedures and documents as on date and essentially try not to duplicate any systems/effort where possible.

Item	Targets of Compliance (DTC)	Lead Question & Additional Prompts for Clause Alignment	IEC 61511	IEC 62443	IEC 27001
1.1	**Functional Safety Management System** **and/or** **Cyber Security Management System** **and/or** **Information Security Management System**	Is there a defined Functional Safety / Security / Information Management system or an equivalent safety and/or security/information management system available and applied for the safety & security lifecycle management activities at site? 1. An approved management process in place and in use by the organisation. 2. Within the management procedures, processes and people are defined for operational activities and that such requirements are regularly communicated by the management team. 3. Lifecycle specific requirements & activities are identified and the necessary guidance provided for all relevant personnel 4. The management overview document provides details the structure and the relationships between different levels of documents and requirements for safe and secure operation. 5. Standard Operating Procedures (SOPs) exist which support the FSM/CSM/ISM regarding operational functional safety and/or security requirements.			

Figure 7 – Questions and Prompts to Facilitate Procedural Mapping

Next it is recommended to start with the requirements of IEC 27001 first, as some baseline aspects from the company existing ISMS will be used to support the IACS management processes.

Establish what systems, processes, documents exist and currently address the necessary clauses as found within IEC 27001 and identify the required clauses and researched company procedures into your mapping matrix. Refer to Figure 8. At the same

time, you will also establish if you have any gaps in your systems, or where such documents may require a modification in certain sections of the existing contents to make them compliant.

Item	Targets of Compliance (DTC)	Lead Question & Additional Prompts for Clause Alignment	IEC 61511	IEC 62443	IEC 27001
1.1	**Functional Safety Management System** **and/or** **Cyber Security Management System** **and/or** **Information Security Management System**	Is there a defined Functional Safety / Security / Information Management system or an equivalent safety and/or security/information management system available and applied for the safety & security lifecycle management activities at site? 1. An approved management process in place and in use by the organisation. 2. Within the management procedures, processes and people are defined for operational activities and that such requirements are regularly communicated by the management team. 3. Lifecycle specific requirements & activities are identified and the necessary guidance provided for all relevant personnel 4. The management overview document provides details the structure and the relationships between different levels of documents and requirements for safe and secure operation. 5. Standard Operating Procedures (SOPs) exist which support the FSM/CSM/ISM regarding operational functional safety and/or security requirements.			**4.2.1a) Scope and boundaries of ISMS** **4.2.1i) Obtain management authorization to implement and operate the ISMS** **4.2.2d) Define how to measure the effectiveness of the selected controls** **4.3.1 General document requirements** **4.3.2 Control of documents** **7.1 Management review of the ISMS**

Figure 8 – Assessment Findings of Compliance to IEC 27001

Then run the process again for IACS safety and security regarding the similar clauses in both IEC 61511 and IEC 62443. During this process, compare the relevant clauses and existing procedures to establish commonality and a fit.

Throughout the discussions, identify and record the common and specific procedures for establishing an optimised safety and security lifecycle management approach specific to your organisational needs. Refer to figure 9.

Item	Targets of Compliance (DTC)	Lead Question & Additional Prompts for Clause Alignment	IEC 61511	IEC 62443	IEC 27001
1.1	**Functional Safety Management System** **and/or** **Cyber Security Management System** **and/or** **Information Security Management System**	Is there a defined Functional Safety / Security / Information Management system or an equivalent safety and/or security/information management system available and applied for the safety & security lifecycle management activities at site? 1. An approved management process in place and in use by the organisation. 2. Within the management procedures, processes and people are defined for operational activities and that such requirements are regularly communicated by the management team. 3. Lifecycle specific requirements & activities are identified and the necessary guidance provided for all relevant personnel 4. The management overview document provides details the structure and the relationships between different levels of documents and requirements for safe and secure operation. 5. Standard Operating Procedures (SOPs) exist which support the FSM/CSM/ISM regarding operational functional safety and/or security requirements.	**IEC 61511**-1/5.1,1/5.2.1.2. Identify the management activities that are necessary to ensure the functional safety objectives are met. Managing functional safety requires the identification of the activities that should take place to achieve safe operation and identification of the personnel that will be responsible for conducting each activity. Identifying the right people with the right skills to work on an SIS project is simply good project management. **IEC 62061**- 4.1: Specify the management and technical activities that are necessary for the achievement of the required functional safety of the SRECS. **IEC 61800-5-2**- 5.1: Specify the responsibilities for the management of functional safety and the activities to be carried out by those with assigned responsibilities.	**4.3.2.2 CSMS** Identify, assess and document the systems, processes and organizations to which the CSMS applies. **4.3.2.3 Organizing for security** Establish the entities responsible for managing, conducting and assessing the overall cyber security of the organization's IACS assets. **4.3.2.3.1 Obtain senior management support** **4.3.2.3.2 Establish the security organization(s)** **4.3.2.3.3 Define the organizational Responsibilities** **4.3.2.3.4 Define the stakeholder team makeup**	**4.2.1a) Scope and boundaries of ISMS** **4.2.1i) Obtain management authorization to implement and operate the ISMS** **4.2.2d) Define how to measure the effectiveness of the selected controls** **4.3.1 General document requirements** **4.3.2 Control of documents** **7.1 Management review of the ISMS**

Figure 9 – Compliance Levels to IEC 61511 and IEC 62443

And finally, complete the mapping matrix, identify the combined lifecycle management approach and develop a series of activities/actions to close any gaps in compliance. Refer to figure 10. Once available, update the approach into your QMS portal and develop a roll-out strategy for the organisation to communicate and eventual audit the benefits of the new lifecycle management process.

Item	Targets of Compliance (DTC)	Lead Question & Additional Prompts for Clause Alignment	IEC 61511	IEC 62443	IEC 27001	Findings
1.1	**Functional Safety Management System** **and/or** **Cyber Security Management System** **and/or** **Information Security Management System**	Is there a defined Functional Safety / Security / Information Management system or an equivalent safety and/or security/information management system available and applied for the safety & security lifecycle management activities at site? 1. An approved management process in place and in use by the organisation. 2. Within the management procedures, processes and people are defined for operational activities and that such requirements are regularly communicated by the management team. 3. Lifecycle specific requirements & activities are identified and the necessary guidance provided for all relevant personnel 4. The management overview document provides details the structure and the relationships between different levels of documents and requirements for safe and secure operation. 5. Standard Operating Procedures (SOPs) exist which support the FSM/CSM/ISM regarding operational functional safety and/or security requirements.	**IEC 61511**-1/5.1,1/5.2.1.2. Identify the management activities that are necessary to ensure the functional safety objectives are met. Managing functional safety requires the identification of the activities that should take place to achieve safe operation and identification of the personnel that will be responsible for conducting each activity. Identifying the right people with the right skills to work on an SIS project is simply good project management. **IEC 62061**- 4.1: Specify the management and technical activities that are necessary for the achievement of the required functional safety of the SRECS. **IEC 61800-5-2**- 5.1: Specify the responsibilities for the management of functional safety and the activities to be carried out by those with assigned responsibilities.	**4.3.2.2 CSMS** Identify, assess and document the systems, processes and organizations to which the CSMS applies. **4.3.2.3 Organizing for security** Establish the entities responsible for managing, conducting and assessing the overall cyber security of the organization's IACS assets. **4.3.2.3.1 Obtain senior management support** **4.3.2.3.2 Establish the security organization(s)** **4.3.2.3.3 Define the organizational Responsibilities** **4.3.2.3.4 Define the stakeholder team makeup**	**4.2.1a) Scope and boundaries of ISMS** **4.2.1i) Obtain management authorization to implement and operate the ISMS** **4.2.2d) Define how to measure the effectiveness of the selected controls** **4.3.1 General document requirements** **4.3.2 Control of documents** **7.1 Management review of the ISMS**	**1. Identify common procedures** **2. Identify specific application procedures and include ISMS / CSMS / FSMS cross references and terminology exchange** **3. Identify and close the compliance gaps** **4. Modify the QMS document control database with appropriate structure / navigation** **5. Communicate the integrated safety and security lifecycle management system and provide relevant training and subsequent system audit schedule**

Figure 10 – Identification of any Gap Closure Actions and Mapping Matrix Conclusions

Conclusions

All stakeholders recognise that we need to manage different types of risks. When it comes to execution of safety and security lifecycle policies and systems, then we can seek ways to streamline and address in an effective way common goals and activities across the IT/OT environment.

A critical part of the organisations capabilities to successfully deliver safety and security requirements will be the need to develop and implement an integrated lifecycle management approach. In doing so the following benefits may be realised:

- Potential to integrate requirements from the functional safety and cyber security standards into one management 'process' underpinned by company QMS
- Baselining the relevant safety and security standards clauses against the existing company procedures supports corporate memory and ease of explanation to both internal and external stakeholders
- Supporting holistic 'safety' claims for functional safety & cyber security
- Enforcing focus and cross working team requirements to improve 'safety culture', awareness and communications within the organisation
- Supporting the business drivers to constantly monitor and manage 'the current operational risk'

References

1. IEC 61508: "Functional safety of E/E/PE safety-related systems, Edition 2.0", (2010-04)
2. IEC 61511: "Functional safety – safety instrumented systems for the process industry sector. Edition 2", (2016-02)
3. IEC 62443-2-1 "Industrial communication networks – Network and system security –
4. Part 2-1: Establishing an industrial automation and control system security program" (2010)
5. ISA-TR 84.00.09-2017 "Cybersecurity Related to the Functional Safety Lifecycle"
6. IEC 27001 "Information technology, Security techniques, Information security management systems, Requirements" (2013)
7. ABB Safety and Security Lifecycle Management Processes