Managing Your Risk:

How security establishes a suitable environment for safety

siemens.com/simatic-pcs7/process-safety

Content

1 Introduction

The frequent news stories relating to cyber breaches have led to a global increase in sensitivity toward the topic of security in all industries. Process safety practitioners are increasingly concerned with the potential impact of security threats on implemented safety instrumented functions (SIF).

The process automation industries have traditionally employed independent protection layers (such as BPCS and SIS) for safety so it is perhaps not surprising that there is a trend toward justifying the adoption of physical separation in order to potentially improve the security of an installation.

However, the potential advantages of physical separation (or air gapping) are offset by restrictions which bring inefficiencies and encourage workarounds. As a result such system implementations are not necessarily able to properly address other important business needs, such as system availability. E.g. an air gapped system setup might lead to careless use of potentially infected portable media which, in turn, could compromise system availability.

Holistic approaches dealing with the requirements for all security objectives (i.e. availability, integrity and confidentiality) will lead to more robust system architectures. Such solutions are generally found by establishing the relevant essential functions, including safety functions, and adopting a 'system wide' security approach.

Therefore this paper will provide guidance on how to ensure an acceptable security level for the complete installation and help to identify areas of particularly high risk which might need special attention due to the potential catastrophic consequences if security is compromised.

In process safety the BPCS and the SIS are often considered Independent Protection Layers (IPLs) and are credited with some level of risk reduction. In case of the SIS this claimed risk reduction can be considerable (i.e. as much as 3 orders of magnitude). Cyber threats are increasing in number and sophistication so it is important that the potential impact of such threats are assessed and, where necessary, the appropriate countermeasures put in place to ensure that the high level of risk reduction often associated with these vital protection layers is not compromised.

Essentially the disciplines of process safety and cyber security are managed by two different groups of people: the safety experts and the security experts. Each group has different know-how and uses different techniques for approaching the respective topic.

Naturally, safety experts are primarily focused on safety systems. However, based on security threat and risk assessments, there is a concern that their focus might shift away from safety toward the potential security impact on availability or IP protection, especially if the safety risks are less than catastrophic. This distraction risk can be avoided by adopting the approach of "essential functions" i.e. those functions required to maintain health, safety and environment of the equipment under control - as described in the IEC 62443-series of standards. An essential function can be a SIF, but it also can be another functionality realized by BPCS or SIS, or a combination of both.

A cyber attack or incident on a high hazard process plant or on critical infrastructure could adversely affect the functioning of such an essential function in a worst case scenario thus increasing the risk of disruption to critical services or the risk of consequences for people and the environment.

Protecting critical industrial infrastructure from cyber attacks now increasingly requires the adoption of new and rapidly evolving cyber security standards aimed specifically at Industrial automation and control systems. It should be noted that these standards are still in development. Some parts of the IEC 62443 standard have been released but others are not yet finalized.

Integrated BPCS and SIS architectures are increasingly being deployed which can also bring a different view in terms of applying cyber security.

This paper outlines an approach to implementing cyber security in an integrated BPCS and SIS scenario and gives an overview of how security and functional safety can be addressed more effectively.

1.1 Increasing number of cyber attacks

The arrival of malware which specifically targets industrial automation and control systems has triggered a significant change in attitude toward cyber-security. It has suddenly become very apparent that malware could directly affect control and protection systems. Developing such malware was technically challenging in the first instance, but, now this line has been crossed, other subsequent malware has been able to use similar approaches to compromise systems. In effect early cyber threats have provided proof of concept to hackers. Enabling toolkits are now widely available on the internet. Hacking and cyber attacks are no longer solely the preserve of misguided amateurs and disgruntled employees. Criminal groups are increasingly involved and the threats are ever more sophisticated.

1.2 Plant incidents with the potential to affect safety

There are very few, if any, recent examples where safety Instrumented functions (SIFs) have actually been compromised as a result of a security breach. In general the non safety related aspects of industrial automation control systems present an easier, more tempting target and it is primarily plant availability that has been targeted and impacted.

For example:

In 2003, the Slammer worm penetrated the industrial control system network of First Energy's Davis-Besse nuclear power plant in Ohio. It disabled a safety monitoring system for nearly five hours[1].

In 2011-12 the US Department of Homeland Security tracked 23 cyber attacks on companies related to the national gas pipeline system. They assessed that the targeted information, if successfully accessed, would have allowed an intruder to disable many compressor stations, blacking out the US energy grid, "at the click of a mouse".[2]

Oil installations in Iran and Saudi Arabia have also been hit by malware with one high profile hack affecting some 30,000 PCs.[3]

In April 2013, oil plants and an oil exporting terminal on Kharg Island, Iran, were affected by a virus in the ICS. The Kharg Island facilities process 80 percent of Iran's crude oil. Components were taken off-line.[4]

On an undisclosed date in 2014, a cyber-attack took place on the ICS of a German iron producing plant. The industrial control system breakdown caused substantial physical damage to the production plant.[5]

[1] Kevin Poulson (2003), "Slammer worm crashed Ohio nuke plant network", SecurityFocus. Online: http://www.securityfocus.com/news/6767

[2] Jason Ryan (2012) "DHS: Hackers Mounting Organized Cyber Attack on U.S. Gas Pipelines", ABC News. Online: http://abcnews.go.com/Blotter/dhs-hackers-mounting-organized-cyber-attack-us-gas/story?id=16304818

[3] Nicole Perlroth(2012)," In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back", New York Times, Online: http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?

[4] Gregg Keizer (2012), "Virus attack on oil processing facilities in Iran", Computerworld. Online: http://www.computerworld.com/s/article/9226469/Iran_confirms_cyberattacks_against_oil_facilities

[5] Gregg Keizer (2012), "Virus attack on oil processing facilities in Iran", Computerworld. Online: http://www.computerworld.com/s/article/9226469/Iran_confirms_cyberattacks_against_oil_facilities

2 Concept of "Defense in Depth" for Industrial Security

The concept of defense in depth is a security strategy in which several layers of defense wrap themselves around the system to be protected, in this case the automation system, like the layers in an onion. The implementation of defense-in-depth requires a combination of various different security measures.

Physical and organizational security measures are summarized under the heading "Plant security".

Measures concerning the security cells, such as forming security cells, securing access points and the secure communication between different security cells, are summarized under the heading "Network security".

Measures such as "system hardening", "user and patch management" as well as "malware detection & prevention" are summarized under the heading "System integrity".

By consequently implementing a "Defense in Depth" strategy, plant operators and their security advisors take additional defensive measures to protect against cybersecurity risks and follow the general recommendation of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT recommends:

- Minimizing network exposure for all control system devices. Critical devices should not have direct access to the Internet.
- Placing control system networks and remote devices behind firewalls and isolating them from the company network.
- Using secure methods such as Virtual Private Networks (VPNs) when remote access is required. Keep in mind that VPN is only as secure as the connected devices.

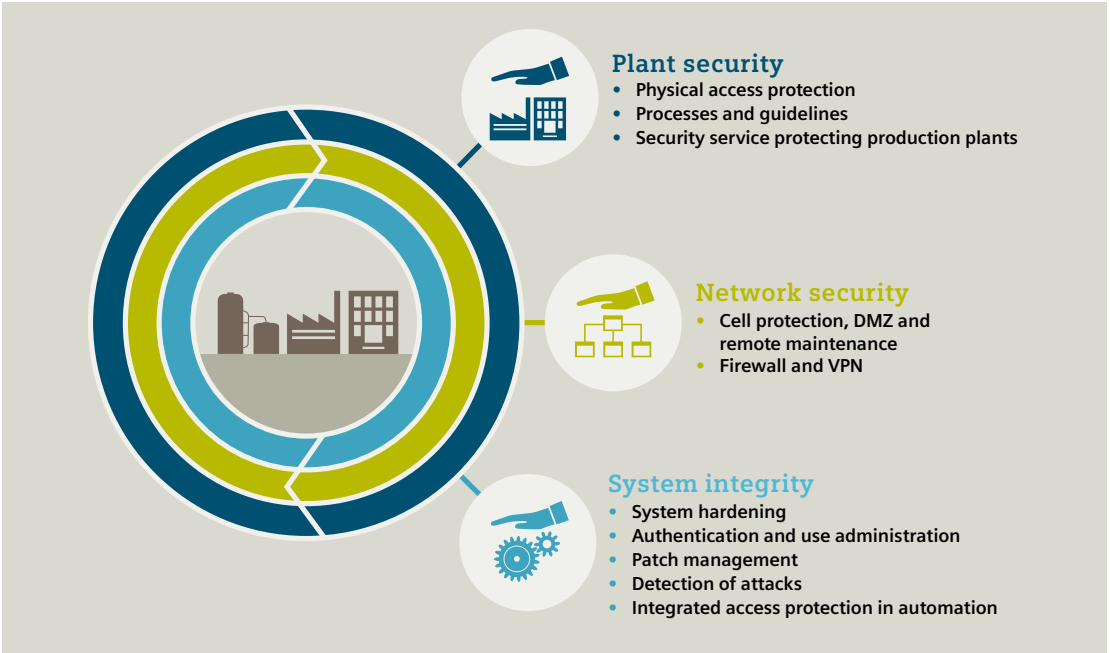


Figure 1: Defense in Depth

3 Security compared to Safety

At first glance there are similarities in the safety and security disciplines, such as risk management and a lifecycle approach, but taking a closer look at the underlying concepts / philosophies reveals that both topics have to be treated differently.

The objectives of the functional safety and security disciplines, such as achieving plant safety and high availability, may well be the same but the rationale for each is quite different.

Functional safety seeks to avoid accidents and damage in the event of a trip condition or system failure, by taking the process to a safe state, thus ensuring safety for people and the environment. It is primarily concerned with factors internal to the safety system, such as hardware integrity and systematic safety integrity and seeks to avoid random hardware failures and systematic failures rendering the safety system ineffective when a demand occurs.

Security, on the other hand, protects a machine or process plant against external factors, such as manipulation by people or malware, thus ensuring the continuing availability and protection of sensitive data (e.g. IP knowledge).

3.1 Culture and Competence

When it comes to the requirements for establishing a supportive organizational culture and the necessary competences for safety and security there are similarities. Both safety and security need to be led from the top of the organization and need to be installed as part of day to day activities. Both also requires competence to be addressed for all involved – although, particularly for smaller companies, the necessary expertise can be in short supply. This is particularly the case with security because it is such a new discipline.

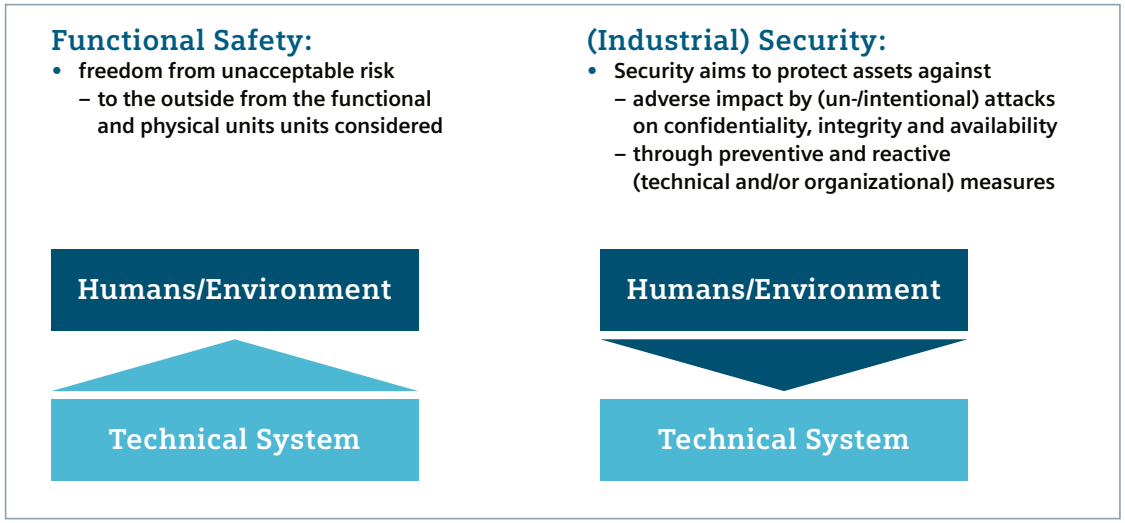


Figure 2
Definition of Functional Safety and Industrial Security

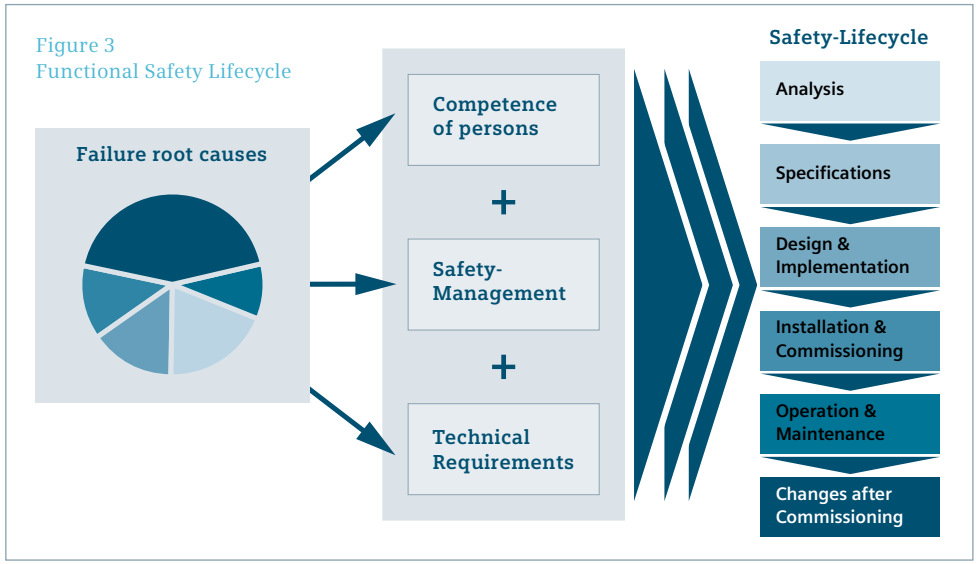


Figure 3
Functional Safety Lifecycle

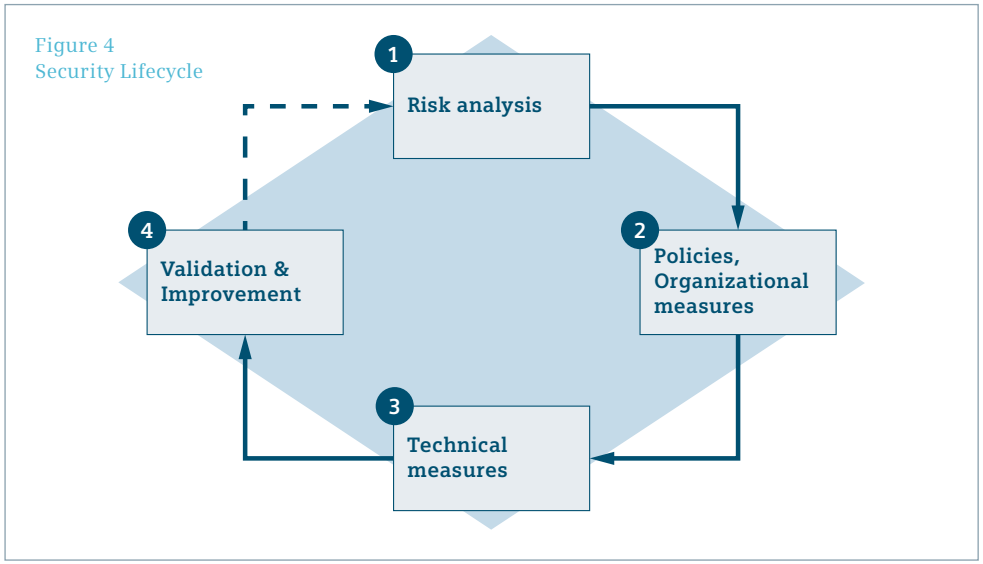


Figure 4
Security Lifecycle

3.2 The Lifecycle Approach

Functional safety and security both adopt a lifecycle approach through assessment, implementation and operate phases. They both require careful management, structuring and planning and both require that competence is addressed throughout.

3.3 The interaction

The two disciplines get in contact during the security risk assessment when the possible impact of cyber threats on safety functions (identified by the safety experts) is evaluated. If cyber threats are identified as potential risks for the integrity of the safety functions, suitable security countermeasures need to be defined and implemented.

The result of the Threat & Risk Analysis is a set of necessary countermeasures creating an effective Security Environment for any functions or systems to be protected from security threats. These countermeasures can relate, but are not limited to, perimeters, interaction and functional units of the security environment. The Security environment does not constitute a security zone, but anything necessary to prevent adverse effects on the system or solution under consideration (and may include aspects of physical security).

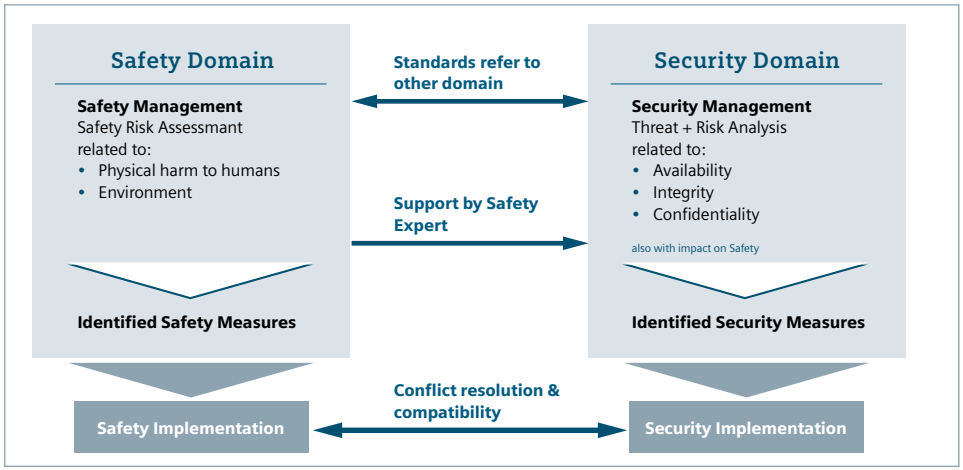


Figure 5
Interaction diagram

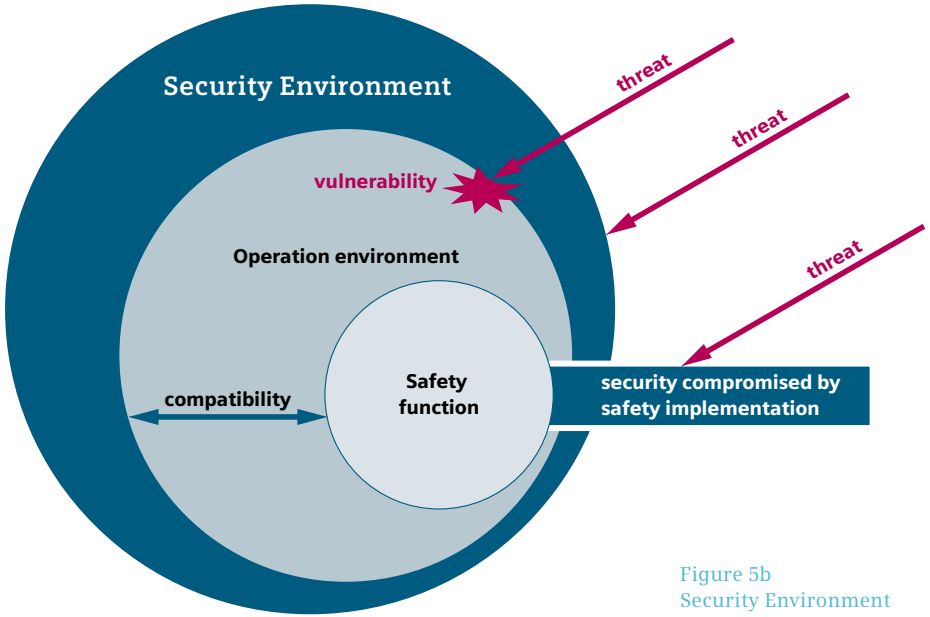


Figure 5b
Security Environment

For the treatment of safety functions within such a Security Environment the following is valid:

- Security provides an environment in which essential functions, according to IEC 62443-3-3 (incl. safety functions), are not adversely affected.
- Safety evaluations are based on the assumption of effective security measures

3.4 Safety Integrity Level (SIL) and Security Level (SL)

During the lifecycle potential risks are assessed, protection layers identified, targets for risk reduction are set and risk is reduced to an acceptable level.

For a Safety instrumented Function (SIF) the target for risk reduction is specified in terms of a Safety Integrity Level (SIL).

IEC 61511:2016 Para 3.2.69 defines safety integrity level (SIL) as a "discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS"

The measure of targeted risk reduction from a security perspective is referred to as the Security Level (SL), again on a scale of 1 to 4.

ISA-62443-1-1 Defines Security Level (SL) as a "level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit"

While broadly similar, establishing a SIL requirement for a SIF is generally a quantitative exercise whereas assessing risk from a security standpoint is somewhat more subjective so deciding on a SL is a qualitative judgment. It's important to understand that there is no correlation between a Safety Integrity Level (e.g. SIL3) and a Security Level (e.g. SL3).

The SL level relates to the security environment and results in all countermeasures necessary to ensure an effective security environment. This means within that environment any functions or systems are not adversely effected by security threats.

4 Security considerations in Functional Safety Standards

4.1 Standards overview

Best practice for functional safety is defined in IEC 61508:2010 (Functional safety of electrical/electronic/programmable electronic safety-related Systems) and IEC 61511:2016 (Functional safety – Safety instrumented systems for the process industry sector). These standards describe functional safety as that part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers.

Security for industrial control systems is a relatively new field and this is reflected in the maturity of the aforementioned standards. The IEC 62443 (Security for industrial automation and control systems) series of standards is still very much a work in progress with some parts of the standard series having being issued while others are still being worked on but the functional safety standards are, by comparison, well established.

4.2 What does IEC 61508:2010 say about Security?

Functional safety standards such as IEC 61508:2010 and IEC 61511:2016 represent best practice in terms of implementing a dependable safety system. In response to the increase in cyber threats both IEC 61508:2010 and the newly released IEC 61511:2016 now contain recommendations regarding the need to include security risks as part of the overall risk assessment and to address these in a dedicated Security Threat & Risk Analysis.

The IEC 61508:2010 standard generally does not cover security aspects in its scope, but there is a reference to conduct a security threats analysis, as it is commonly done in the security domain. IEC 61508-1:2010 Para 7.4.2.3 states "If the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out". IEC 61508-1:2010 Para 7.5.2.2 goes on to point out that "if security threats have been identified then a vulnerability analysis should be undertaken to specify security requirements". It then suggests the IEC 62443 series of standards as relevant guidance on the topic of security.

4.3 What does IEC 61511:2016 say about Security?

IEC 61511-1:2016 Para 8.2.4 requires that "a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS".

The risk assessment shall result in:

a) A description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);

b) A description of identified threats that could exploit vulnerabilities and result in security attacks (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);

c) A description of the potential consequences resulting from the security events and the likelihood of these events occurring;

d) Consideration of various phases such as design, implementation, commissioning, operation, and maintenance;

e) The determination of requirements for additional risk reduction;

f) A description of, or references to, information on the measures taken to reduce or remove the threats.

For further guidance the ISA TR84.00.09, ISO/IEC 27001:2001 and the IEC 62443:2010 standards are referenced as representing best practice.

IEC61511-1:2016 Para 11.2.12 goes on to require that "The design of the SIS shall be such that it provides the necessary resilience against the identified security risks ".

Users of the standards are directed to guidance related to SIS security provided in IEC 62443 series.

It has to be pointed out, that it is not necessary to address the security aspects specifically within the safety project. A reference to the work results of the security threats analysis is possible.

5 Security Standards

Siemens focuses on the following guidelines as being most applicable:

- IEC 62443 (under development) internationally supported, it involves the component supplier, asset owner and systems integrator in the solution and supports a defense-in-depth approach. It gives a holistic perspective of industrial security.
- NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection). NERC Standards CIP-002-3 through CIP-009-3 provide cyber security framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system.

Of these Siemens views IEC 62443 as a leading standard because it is international in scope, vendor neutral, and incorporates important elements from other relevant standards including WIB M-2784 and NERC-CIP. It supports a defense-in-depth approach and promotes involvement of all stakeholders including the asset owner, system integrator and component supplier. IEC 62443 covers the following aspects.

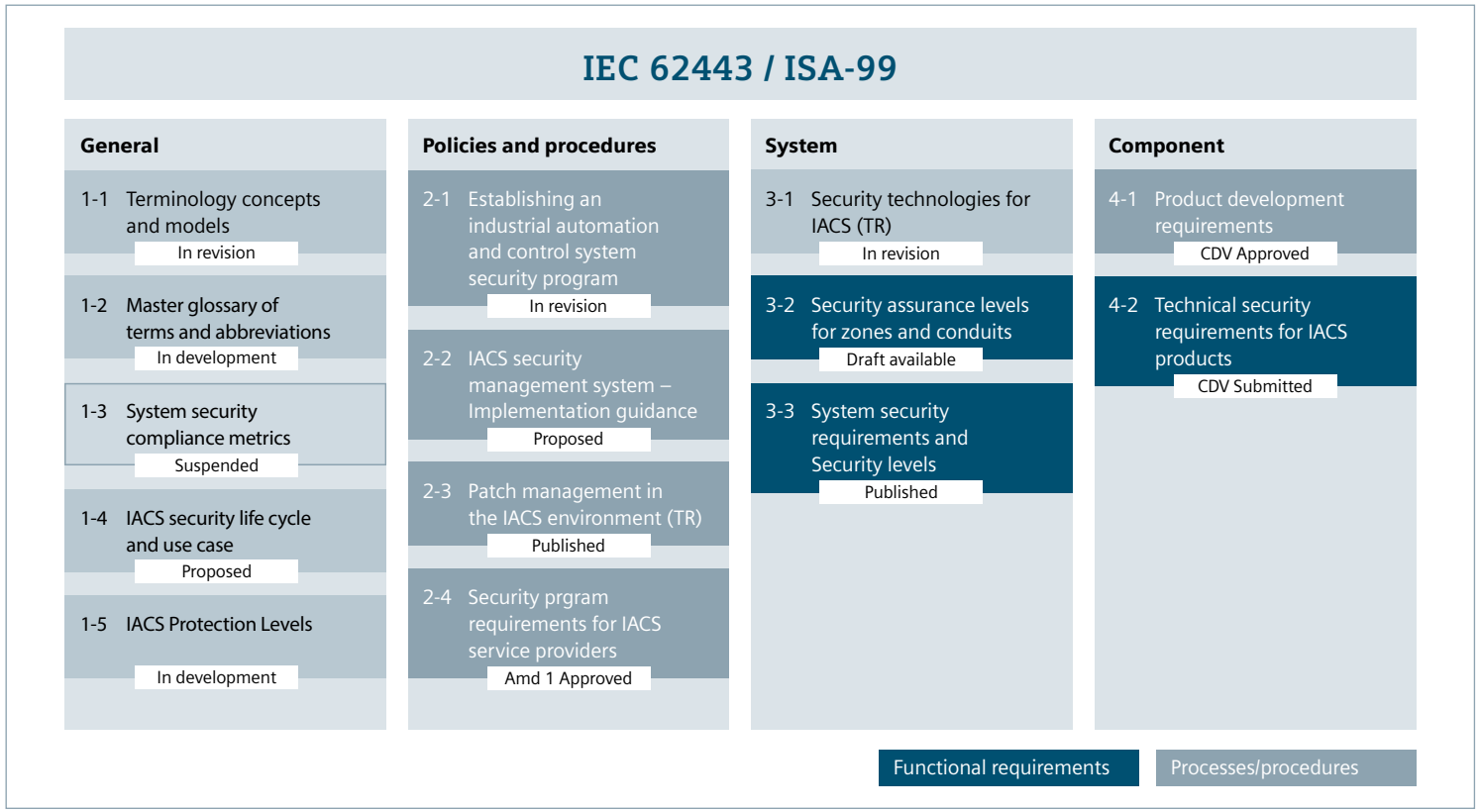
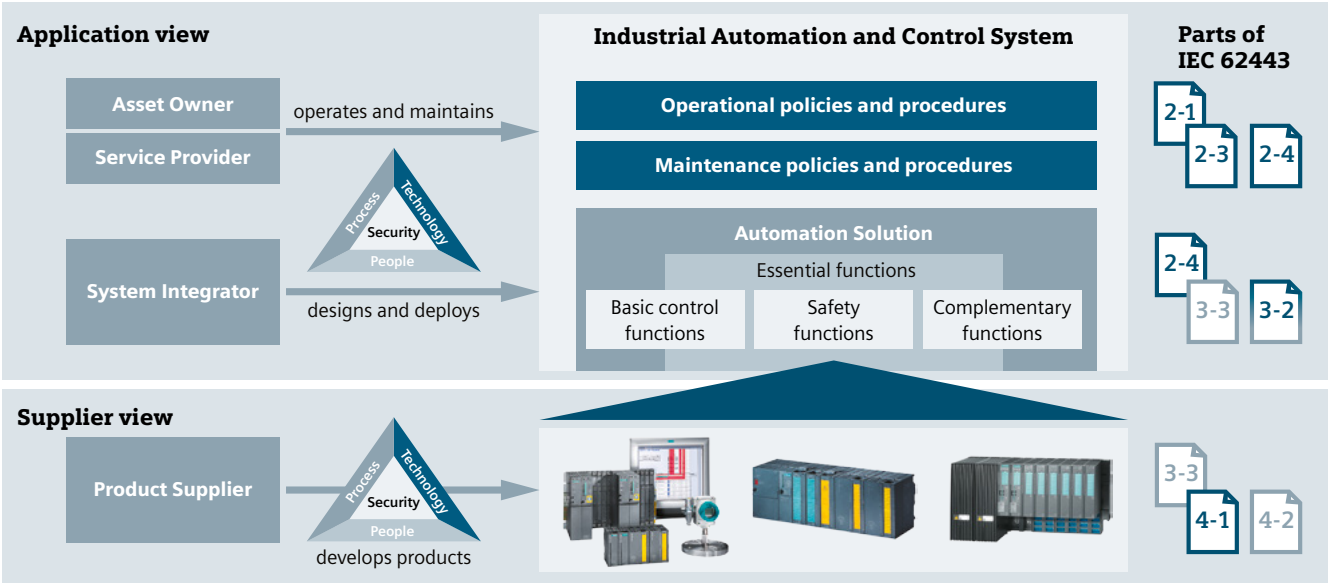


Figure 6 IEC 62443

IEC 62443 addresses all stakeholders for a holistic security concept as depicted in the picture below.

Figure 7
IEC62443 addresses all stakeholders



Asset Owners and Service Providers are mainly focused on plant operation and maintenance in their daily business. The policies and procedures that have to be considered are part of an overall IACS (Industrial Automation & Control System) security management system which is described in:

- IEC 62443-2-1 Establishing an industrial automation and control system security program
- IEC 62443-2-3 Patch management in the IACS environment
- IEC 62443-2-4 Security program requirements for IACS service providers

System Integrators are involved in the design and deployment phase and therefore have, beside the policies and procedures described In IEC 62443-2-4, a more direct focus on the IACS itself. They have to do a security risk assessment and have to ensure that security requirements related to the system are met as described in

- IEC 62443-3-2 Security assurance levels for zones and conduits
- IEC 62443-3-3 System security requirements and Security levels

Product suppliers act independently of the actual plant solution. They have to meet requirements assigned to a specific system/product described in:

- IEC 62443-3-3 System security requirements and Security levels
- IEC 62443-4-2 Technical security requirements for IACS products

Policies and procedures that have to be met during the product development are described in:

- IEC 62443-4-1 Product development requirements

6 The challenge to focus on essential functions

According to IEC 62443 an essential function is a function or capability that is required to maintain health, safety, the environment and availability for the equipment under control. [IEC 62443-3-3 Edition 1. Para 3.1.22].

In recent years both BPCS and SIS have increasingly adopted commercial off the shelf technologies (COTS) and open standards and this, in turn, has facilitated a trend toward increased integration of control and safety. Additionally, there has been a trend to see BPCS and SIS as two elements which require different treatment regarding safety and security. In fact, threat & risk analysis conducted to investigate security focuses on essential functions necessary to ensure a secure as possible operation. One aspect of that investigation is to consider the effect of security attacks on the safety functions of the system. However, there are areas to be protected beyond the borders of SIS and therefore it is not advisable to look at security with a strong relationship to BPCS and SIS only.

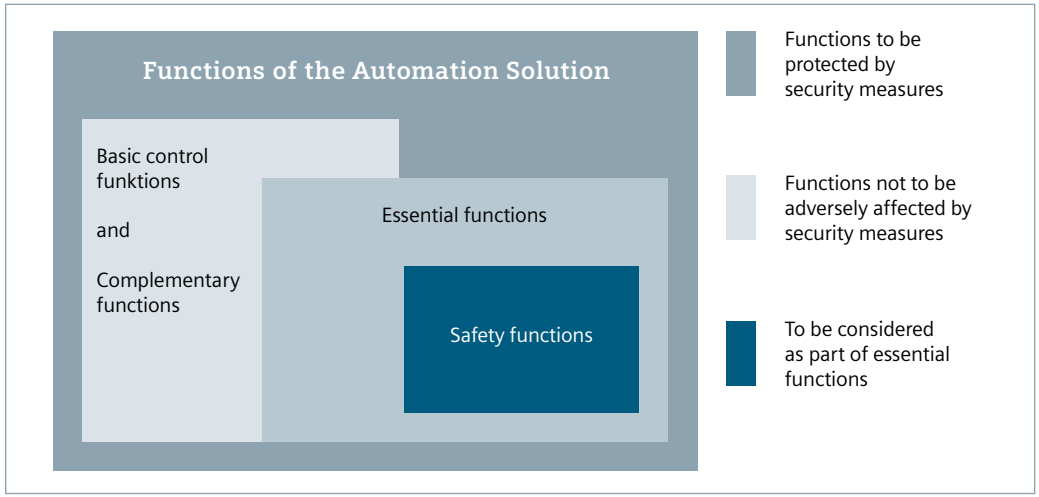


Figure 8
Concept of essential functions

There has to be a holistic approach towards security taking into account all security targets (related to essential functions) necessary for the automation system. Experience shows that there is a high demand for security, not only for safety, but also for functions of availability, integrity and confidentiality.

7 Architectures of Industrial Automation Control & Safety systems

The typical BPCS & SIS architectures can be categorized as air-gap, interfaced, integrated and common. Each approach has its advantages and disadvantages from a safety point of view, as well as presenting different security challenges. The various architectures are described below along with some discussion of the associated security considerations.

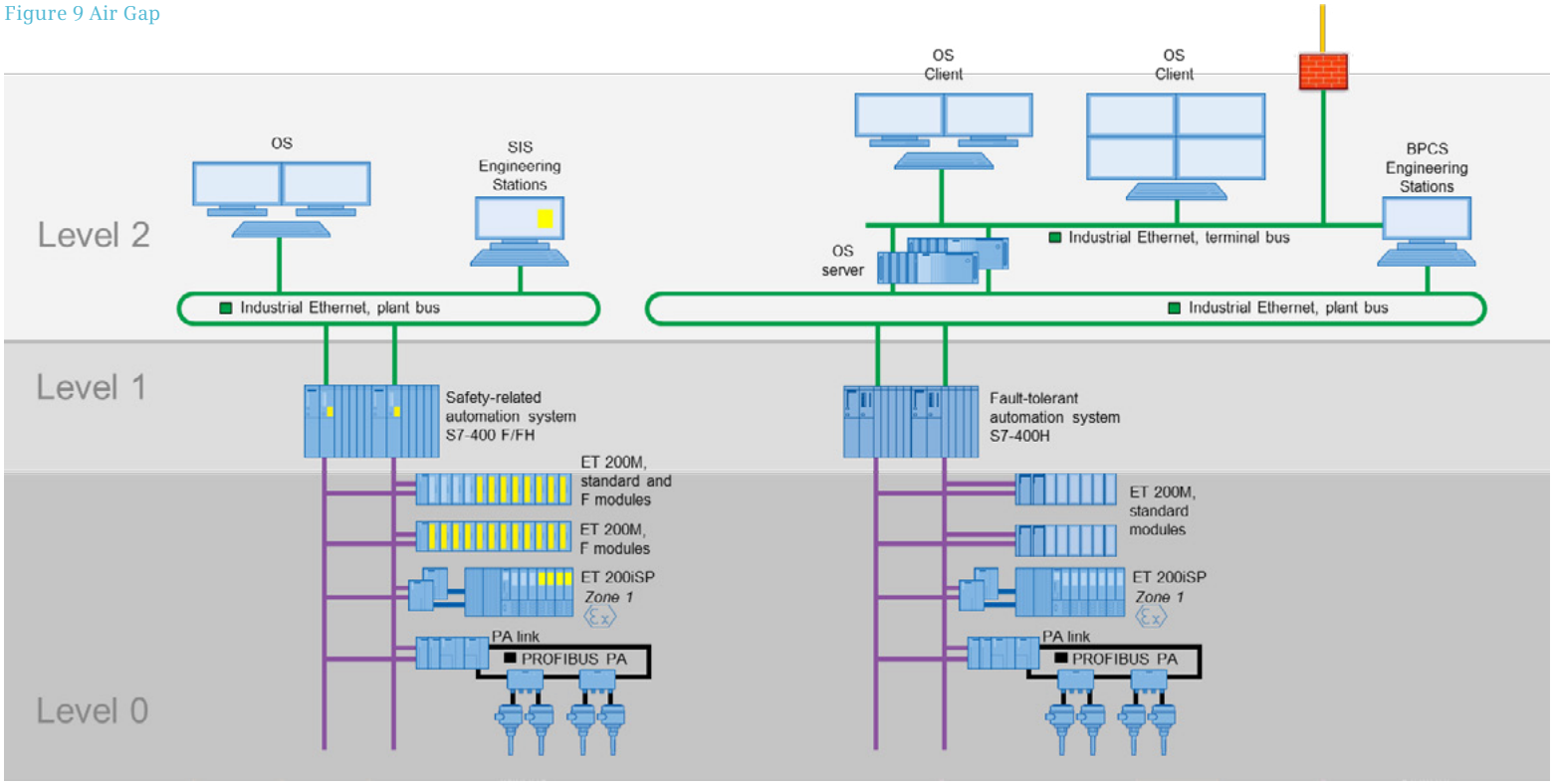
7.1 Air gap

As the name implies the air-gap architecture has no data connection between BPCS and SIS. In older systems the BPCS and SIS typically uses diverse hardware from different suppliers.

This approach is often perceived as offering good protection, but it can give a false sense of security. Legacy systems may not have addressed security when they were developed and deployed, and they may therefore be less inherently secure in their own right.

Security can't be taken for granted. The perceived inherent security of an air gap can cause users to 'let their guard down' and take actions to address the lack of connectivity which then compromise the air-gap. There are several common scenarios where an isolated system can become compromised. These are consistent with documented cases of actual cyber security incidents. For example, an engineer transferring data onto the SIS engineering station by copying files from a USB memory stick increases the possibility of infection by a worm or virus. Despite a very significant air gap the International Space Station has been infected by malware on several occasions.

Figure 9 Air Gap



Another disadvantage of the air gap approach is that it eliminates the potential benefits of integration and, if the BPCS and SIS are from different suppliers, this often results in a higher lifecycle cost in terms of engineering, training, maintenance and spare parts.

If an air gap approach was seen as essential for a new system then it may still be beneficial to implement this using BPCS & SIS from an integrated single vendor offering. This would still present some challenges in terms of passing data between systems and giving visibility of the SIS on the HMI, but it would give commonality of hardware for spares and would also reduce the training and knowledge requirements.

7.2 Interfaced

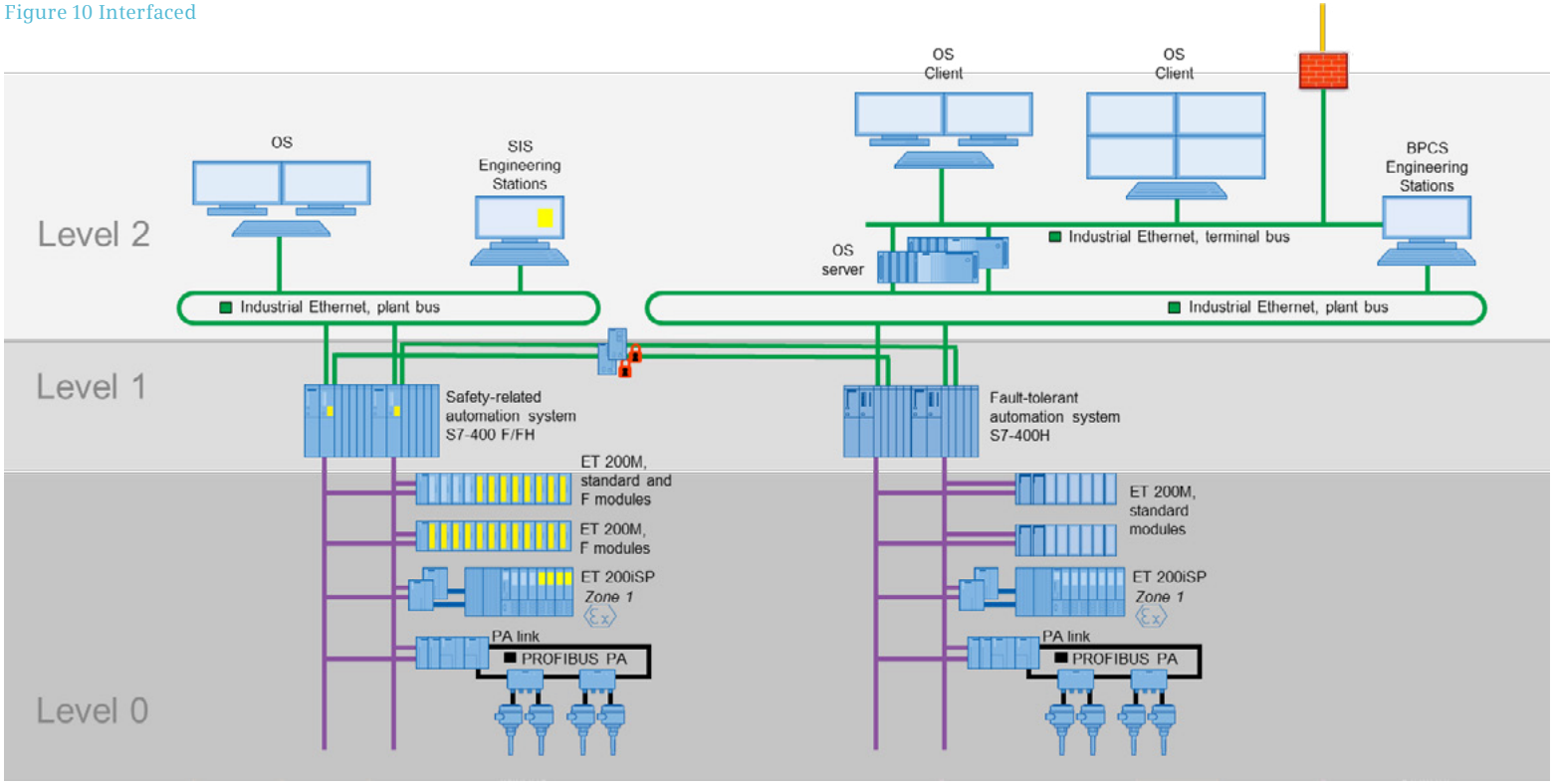
The interfaced architecture typically uses gateways between BPCS and SIS to allow some data to be communicated. In many systems using this architecture the BPCS and SIS use diverse hardware, often from different suppliers. As a result they typically have separate engineering tools and their own dedicated operator interfaces and engineering workstations.

The interfacing of these systems often involves the use of proprietary protocols. These have some inherent de-facto security because they are typically non-routable, point to point protocols to avoid allowing access to the SIS via the BPCS network. However the protocols used are general purpose and are not well suited to safely communicating safety data such as overrides and bypasses.

The Interfaced architecture again misses out on many of the potential benefits of integration and can also prompt the same behaviors as could compromise the security of the air gap.

If an Interfaced approach was seen as essential for a new system then it may still be beneficial to implement this using BPCS & SIS from an integrated single vendor offering. As with the air gap approach this would still present some challenges in terms of passing data between systems, but it would be possible to present selected SIS data on the operator HMI, and it would at least give commonality of hardware for spares and also reduce the training and knowledge requirements.

Figure 10 Interfaced



7.3 Integrated 2 Zone

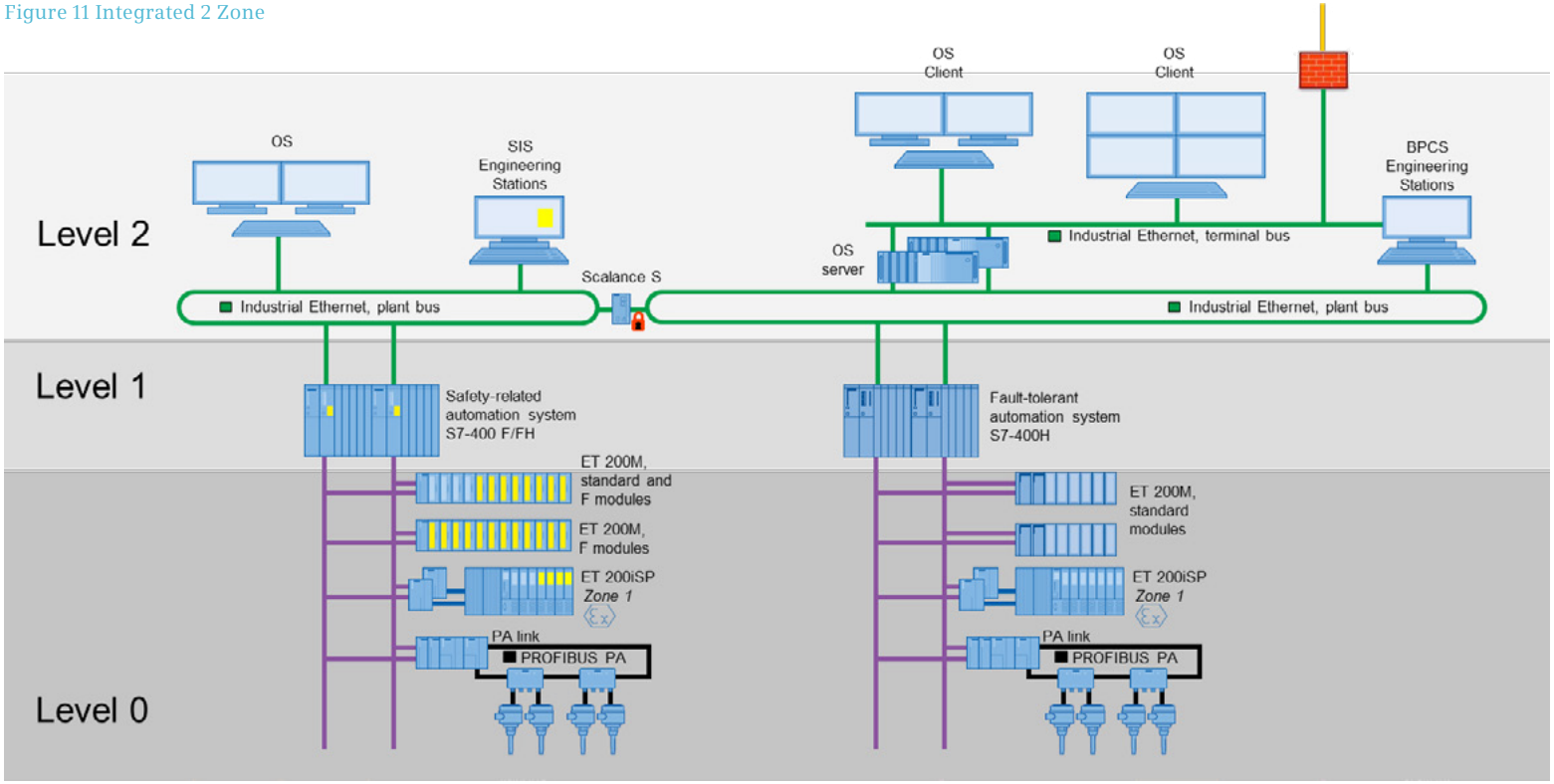
In this architecture the BPCS and SIS are typically from the same vendor. The BPCS and SIS network are segmented with the boundary being the interposing firewall. The firewall manages the data flow restrictions between the two network zones (e.g. which stations on the BPCS network are allowed to talk to stations in the SIS network). The level of integration differs between vendors but will typically have extensive commonality of hardware, engineering tools, engineering workstations and operator interface. This brings many advantages such as simplified engineering, reduced training, reduced spares, etc.

Integrated systems also take advantage of certified safety communications which provide a safe and secure method for connectivity, and enable owner/operators to reduce costs and improve overall operational efficiency. An example of this would be safety communications from the operator station to the SIS for managing bypasses, maintenance overrides etc.

Some vendors are also able to offer networking hardware with built in security features and these can be supplied with default settings tailored to meet the vendor security concept thus making it easier to achieve safety “out of the box”.

There are many benefits for integration and they are designed to be integrated, safe and secure. If vendor guidelines and a defense in depth approach are adopted then the requirements of the standards can still be met.

Figure 11 Integrated 2 Zone



7.4 Common or Integrated 1 Zone

In this architecture the BPCS and SIS are based on a common platform. There is commonality of hardware, engineering tools and operator interface. Standard and safety-related programs can still be separated in dedicated controllers (integrated 1 zone) but optionally can also be combined on one controller (common). It is important in this context that the standard and safety-related program are executed independent of each other.

Systems which are designed to be integrated in this way offer many features to help keep control and safety separate and these also help in achieving security goals. For example access protection is built in, safety programs are protected from standard control, and data signatures can be used to check for corruption of communications or un-authorized, uncontrolled program changes. Correct program flow and timely program execution is routinely monitored.

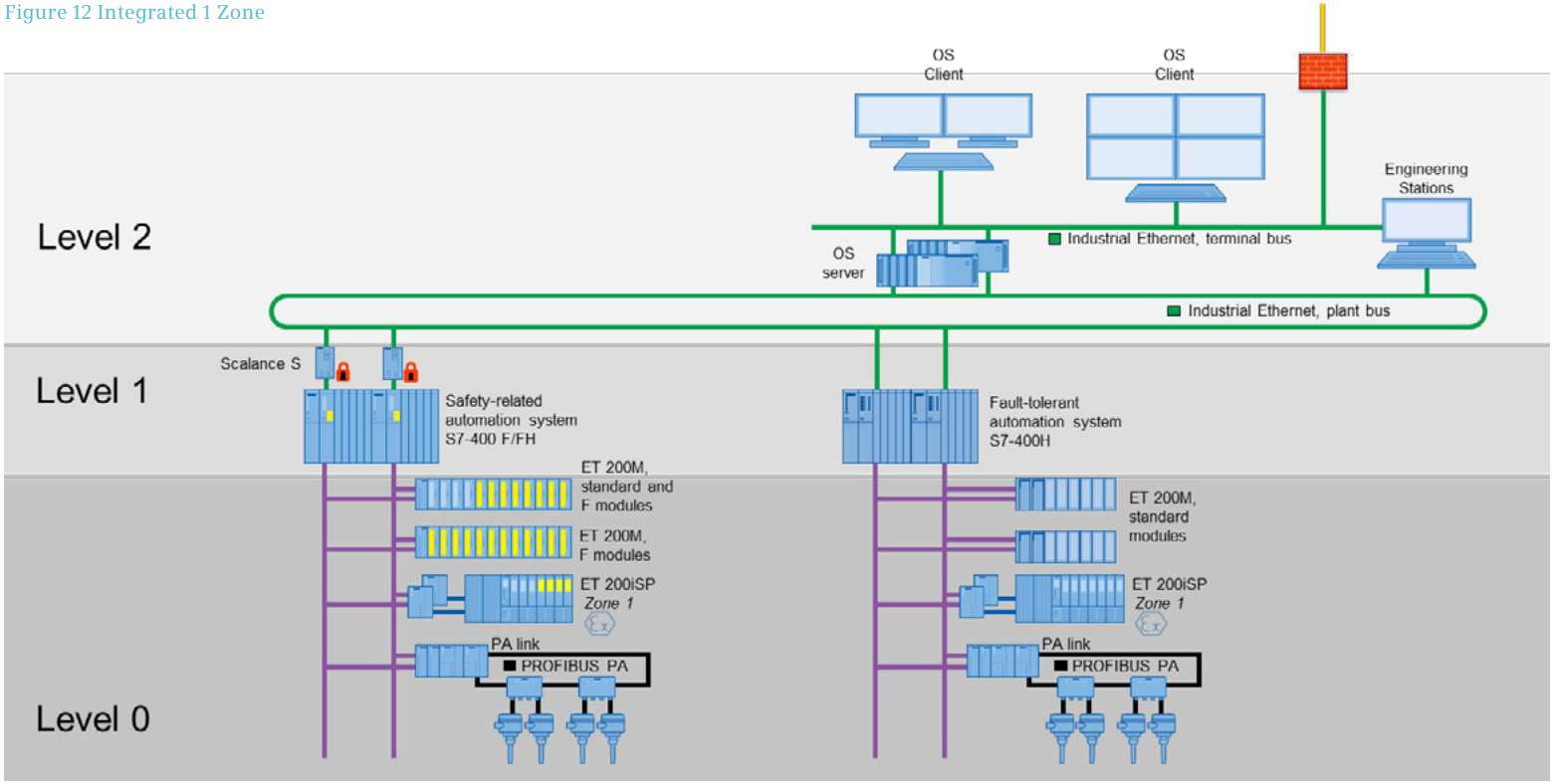
In this integrated approach is it also possible to use a separate engineering station for the SIS.

The common architecture achieves separation of control and safety in much the same way as in an integrated system.

Although on the same network the SIS logic solver can be logically separated with an interposing firewall that limits the access to the device. Also for this architecture it can be stated that if vendor guidelines and a defense in depth approach are adopted then a high level of security can be achieved and the requirements of the standards can be met.

Both approachs offers lower hardware costs and the need for fewer spare parts.

Figure 12 Integrated 1 Zone



8 Conclusion

Cyber security vulnerabilities can open the door to attacks which compromise the effective operation of a whole plant, either causing nuisance trips fo the SIS or potentially impacting on the ability to respond when there is a real demand.

The implementation of cyber security and functional safety have some similarities (e.g. dedicated lifecycle approach, defined stakeholders, requirement for FSM / SM, continuous monitoring) but the differences prevail due the fact that different experts and methods are involved, different processes and timelines exist and both disciplines are based on different technical regulations and standards.

It's highly recommended to apporach both domains individually and focus on the these steps where the experts have to communicate and interact (e.g. security threats analysis).

What should be avoided is that the FSM (Functional Safety Manager) also takes care of the security domain. This approach would not sufficiently meet the complexity and importance of this topic.

It is important that both should be considered in parallel during risk assessment, design, implementation and operation.

Recent high profile industrial accidents highlight the need for continuing improvement in safety culture and functional safety management is increasingly a focus for senior management in successful high-hazard companies. A similar approach needs to be taken with cyber security management to bring it up to the same level of maturity as an own discipline.

Implementing security in a Industrial automation and control system is just the start. Keeping such a system on a high security level requires awareness of security issues, a security culture and implementation of a security management system to assist in establishing and maintaining security over time.

Relying on air-gapped and diverse systems as a defense against cyber threats is not sufficient. Today's world grows ever more connected and this expectation in terms of connectivity will inevitably mean that any air-gap will be breached at some point. To rely on assertions that air gapping and diverse systems are the most effective form of defense is misguided.

BPCS and SIS can be both integrated and compliant with best practice for security by following holistic security concepts, using a defense in depth approach and employing system architectures comprised of products which are secure by design.

9 Glossary

BPCS	**Basic Process Control System**
COTS	**Commercial Off the Shelf**
FSM	**Functional Safety Management**
IACS	**Industrial Automation and Control System**
ICS	**Industrial Control System**
IPL	**Independent Protection Layer**
SIF	**Safety Instrumented Function**
SIL	**Safety Integrity Level**
SIS	**Safety Instrumented System**
SL	**Security Level**
SM	**Security Management**
USB	**Universal Serial Bus**

Find out more:

siemens.com/simatic-pcs7/process-safety

Siemens AG
Process Industries and Drives
Automation and Engineering
76181 Karlsruhe
Germany

Subject to change without prior notice
Produced in Germany