CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648113

Safety & Security - Is a Physically Separation of the SIS Necessary?

Volker Hirsch*[a], Jean-Luc Gummersbach[a], Thomas Bartsch[b]

[a] Siemens AG, 76187 Karlsruhe, Siemensallee 84
[b] Siemens AG, 90745 Nürnberg, Gleiwitzerstraße 555
volker.hirsch@siemens.com

Industrial security is becoming more and more important in the process industry as plant automation systems are being increasingly connected to the office environment and internet. In the meantime, security aspects have also influenced functional safety standards such as IEC 61508 and IEC 61511 (CDV). But there are different targets for safety and security. Safety avoids accidents and damage when a fault occurs and ensures maximum safety for people, processes and the environment. Security protects a machine or plant against unauthorized access by people and against malware, and ensures the availability of the machine or plant.
Two questions arise, first, how should security aspects be considered for the Safety Instrumented System (SIS), and second, is a physically separation of the SIS from the Basic Process Control System (BPCS) necessary? The following paper describes SIS security aspects as provided in ISA TR84.00.09, and Industrial Security aspects with additional security layers for the SIS as an integrated approach for SIS & BPCS.

1. Safety & Security

Protecting critical industrial infrastructures from cyber attacks now requires the adoption of new and rapidly evolving cyber security standards aimed specifically at industrial automation and control systems. Many high-hazard process facilities use industrial automation to control both the process and also to help keep it safe. The automation often consists of Distributed Control Systems (DCS) or Programmable Logic Controllers (PLC) for control, and safety instrumented systems (SIS) for the safety aspect. To avoid confusion, the functional safety standards use the generic term Basic Process Control System (BPCS) to describe the control layer.
A cyber attack on a high-hazard process plant or on critical infrastructure could potentially affect the BPCS, the SIS or in the worst case scenario, both. This would therefore increase the risk of disruption to critical services or, more seriously, have direct consequences for people, the environment or both.
Cyber threats are increasing in number and sophistication, so it is vital that we assess the potential impact of such threats on BPCS and SIS and, where necessary, put in place the appropriate countermeasures to ensure these layers of protection are not compromised.
Basic functional safety standards such as IEC 61508 and IEC 61511 represent best practice in terms of implementing a dependable SIS. In response to the increase in cyber threats, both the latest version of IEC 61508 (Ed 2:2010) and the proposed upcoming revision to IEC 61511 (Ed 2) now include recommendations regarding the need to include security risks as part of the overall risk assessment and to take steps to mitigate any identified threats.

1.1 Main difference between Safety and Security

Information security has traditionally focused on achieving three objectives: confidentiality, integrity and availability. In the process industry the sequencing of these three objectives are reversed: availability, integrity and confidentiality.
Functional safety is, as defined in IEC 61511 Ed.2 (Functional safety – safety instrumented systems for the process industry sector (CDV)), part of the overall safety relating to the process and the BPCS, which depends on the correct functioning of the SIS and other layers of protection.

Please cite this article as: Hirsch V., Gummersbach J., Bartsch T., 2016, Safety & security - is a physically separation of the sis necessary?, Chemical Engineering Transactions, 48, 673-678 DOI:10.3303/CET1648113

The objectives of safety and security are different:

Safety protects people against a machine or plant

- malfunction of a machine or plant (safe reaction through limit monitoring)
- internal malfunction of systems (high self-diagnostic coverage)
- possible misuse of systems (to avoid dangerous situation during operation)

Security protects a machine or plant against people

- intentional misuse of systems (stopping the CPU, incorrect behaviour of functions)
- external malfunction of systems (diagnostic coverage generally not implemented)
- misuse of systems (create a dangerous or not specified situation)

There are different standards for safety and security.
One important standard for security is the IEC 62443 series “Security for industrial automation and control systems - Network and system security”.

1.2 . Safety and Security similarities

To help achieve safety and security the overall process is broadly similar. Potential risks are assessed, layers of protection identified, targets for risk reduction are set and risk is reduced to an acceptable level. Functional safety standards and cyber security advocate a lifecycle approach, and the lifecycle of each extends over a comparable timescale. Both employ a layered “defense in depth” strategy to prevent incidents. There is potential overlap in the people who are likely to be involved.
For a Safety Instrumented Function (SIF) the target for risk reduction is specified in terms of a Safety Integrity Level (SIL) in the range 1 to 4. Achieving a particular SIL is dependent, in part, on the architecture of the SIF. The comparable 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. Establishing an SIL requirement for an SIF is generally a quantitative exercise whereas assessing risk from a security standpoint is somewhat more subjective; as a consequence, deciding on an SL is a qualitative judgment.

1.3 Sequence of the risk analysis

In the process industry there are many common-to-use package units with their own automation and sometimes, separated control system for different parts of the plant. Therefore, different automation / control systems may be used in the plant and may also be supplied by different vendors.
It makes sense to start with the risk analysis for the machine / functional safety, including security threats for the different parts. If safety is required, the safety measures, including basic security functions, will be implemented in the relevant automation / control system.
A security risk analysis that takes into consideration the complete automation / control system should be run after a FAT has been conducted or a CE Mark has been issued. The required security measures must be implemented, if necessary with consequences for the safety risk analysis.

2. Architectures of industrial automation control & safety systems

Annex A of ISA-TR84.00.09-2013 includes a series of example security architectures. These architectures are conceptual, and not intended to serve as a template for every system. Instead, the objective is to represent different approaches an end user might elect to implement an SIS.
Four examples are presented in this Annex representing different levels of management based on differing degrees of interconnection between the SIS zone and other zones in the architecture.
Each successive example represents increasing challenges to designing and maintaining security.

2.1 Air-gapped

Figure 1 illustrates an “air-gapped” conceptual design for the SIS integration. From an external threat perspective, this design represents the highest level of independence between the BPCS and the SIS. In this design, the SIS is both logically and physically isolated from communicating with the rest of the zones. Discrete wiring connections are maintained between the SIS and BPCS for monitoring purposes only and do not contain any communication information. Separate IAMS (Instrument Asset Management System) and human machine interface (HMI) systems are maintained for the SIS and BPCS zones.
In addition, separate engineering workstations, IAMS and HMI systems are maintained for the SIS and BPCS zones.

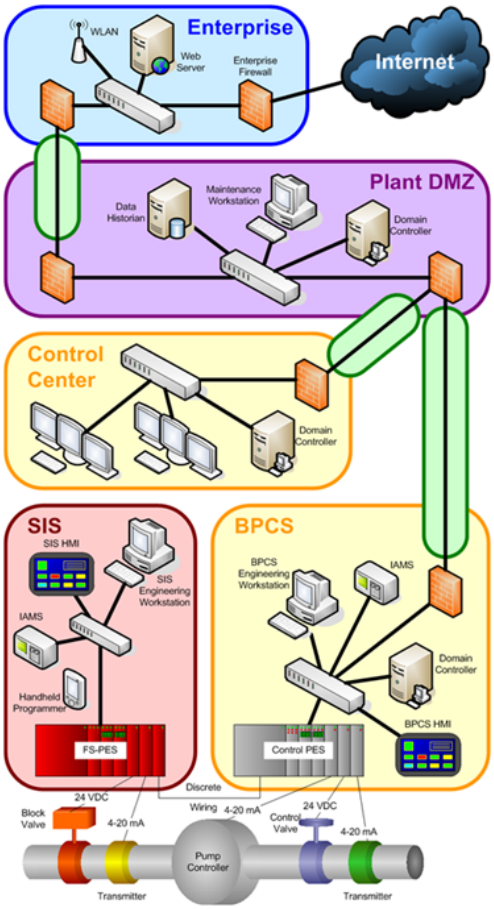

Figure 1: Example with Air-Gapped SIS

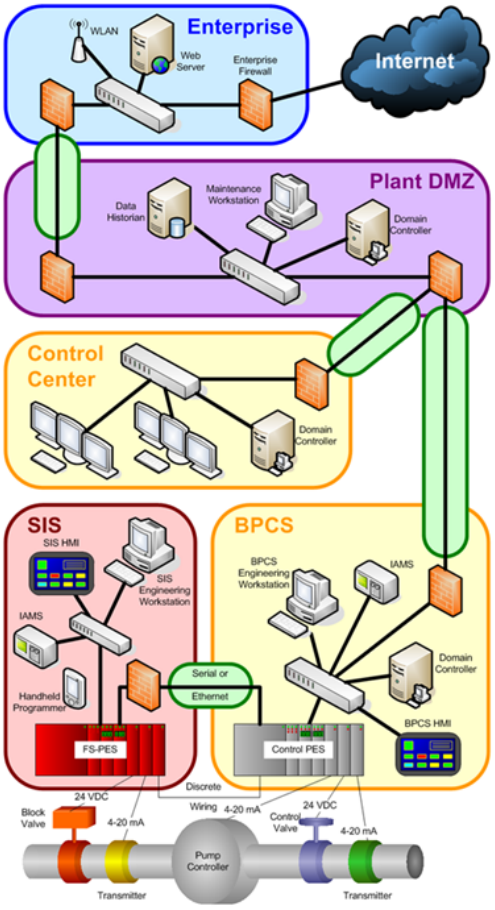

Figure 2: Example with Interfaced SIS

2.2 Interfaced

Figure 2 illustrates an “interfaced” conceptual design. In this example, the SIS and BPCS are still connected using discrete wiring, but they now include a direct point-to-point communication connection. This point-to-point connection does not travel over the same network interface that is used for other communications (for example, to the engineering workstations or HMI). These types of point-to-point communications may use either serial or Ethernet connections depending on the specific protocol being used. Interfaced designs should have the following attributes: BPCS outputs to the SIS (for example, shutdown via discrete output card) should be communicated via discrete wiring.

2.3 Integrated 2 zone

Figure 3 illustrates an “integrated 2 zone” conceptual design. In this example, the SIS and BPCS are fully integrated and provide direct, real-time communication between the systems. Information from the SIS zone is communicated to the BPCS and higher -level systems for monitoring purposes. This information should be read-only flowing from the SIS zone out to other systems.

This example also allows for systems in the SIS zone to pull information from other systems on the network (for example, operating system or software updates) in a controlled way over the network instead of using physical media. Information pulled into the SIS zone should not come directly from the Internet, but some intermediate location from within the DMZ or lower-level system.

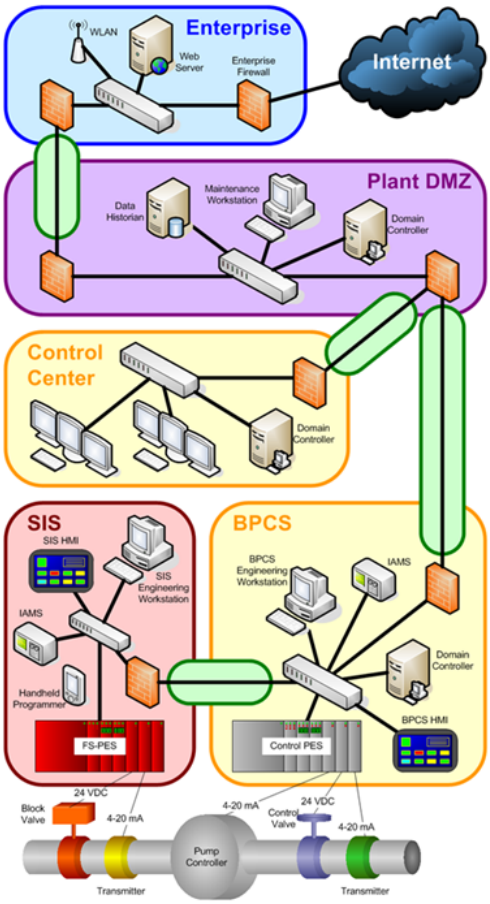

Figure3: Example with Integrated 2 Zone SIS

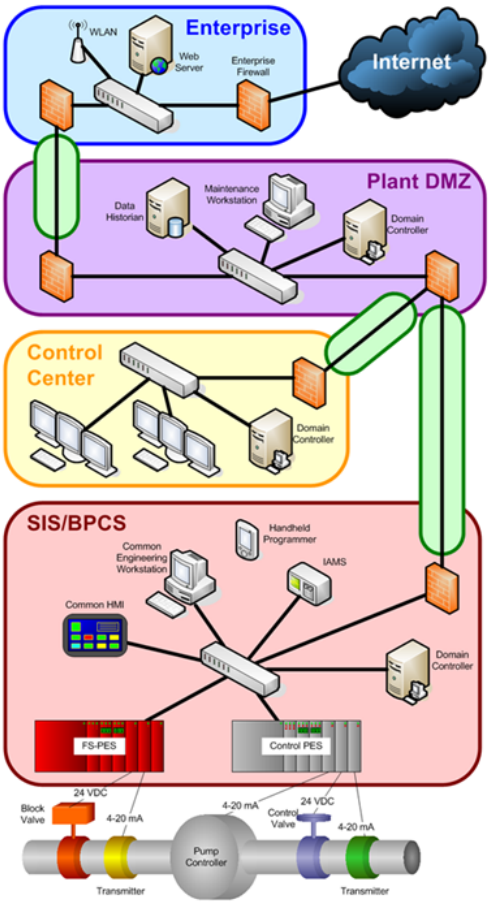

Figure 4: Example with Integrated 1 Zone SIS

2.4 Integrated 1 zone

Figure 4 illustrates an “integrated 1 zone” conceptual design. This example is similar to the integrated 2 zone example in section 3.3. The SIS and BPCS systems are integrated providing much greater communication between those systems and higher-level systems in the architecture. For the integrated 1 zone example, there is only a single HMI, IAMS and engineering workstation. These systems are able to communicate and control both the SIS-PES and the control PES. This type of situation can exist when an organization decreases capital expenditures by reducing the duplication of equipment. In this case, the standard BPCS components of the system should be designed and maintained at the higher security requirements necessary for the SIS zone. As the engineering workstation on is common to both the BPCS and the SIS, it needs to be managed per SIS security requirements.

3. Industrial Security

In their security advisories, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourages plant operators to take additional defensive measures to protect against cybersecurity risks. 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.

3.1 Concept of “defense-in-depth”

The concept of defense-in-depth is a security strategy in which several defense layers are positioned around the system to be protected, in this case, the automation system (like "peeling an onion").
The implementation of a defense-in-depth requires a combination of various security measures.
The physical and organizational security measures are summarized under the heading "Plant Security".
The 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 "Integrity Protection or Endpoint Protection".

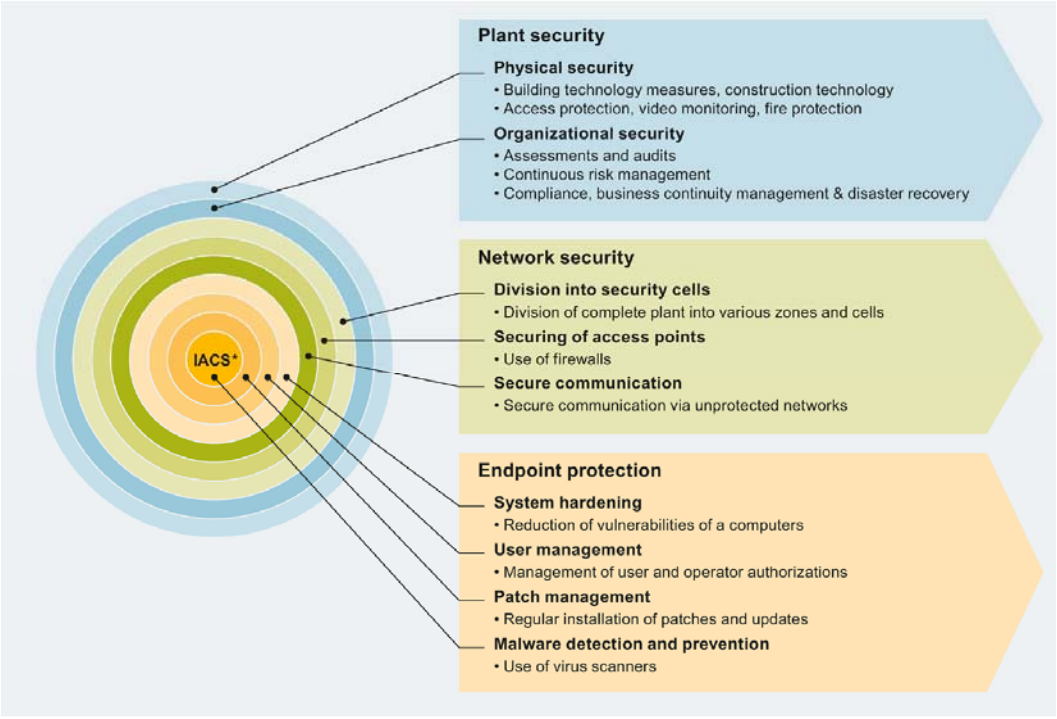

Figure 5: The figure shows the "defense-in-depth" strategy

4. Security aspects of an integrated approach for SIS & BPCS

All four configuration examples from the ISA-TR84.00.09-2013 can be realized with the SIMATIC PCS 7 process control system. The benefits for operation and maintenance with common IAMS and HMI for BPCS and SIS can be achieved with the integrated 1 zone concept.
With the defense-in-depth strategy it is possible to attain a high level of security. Access to the SIS for the purpose of making approved configuration changes, to facilitate mechanical integrity program requirements, or repair should consider utilizing one or more compensating controls.
Using the example of a SIMATIC PCS 7 configuration with integrated 1 Zone SIS (see figure 6), some of the compensating controls for the SIS are explained.

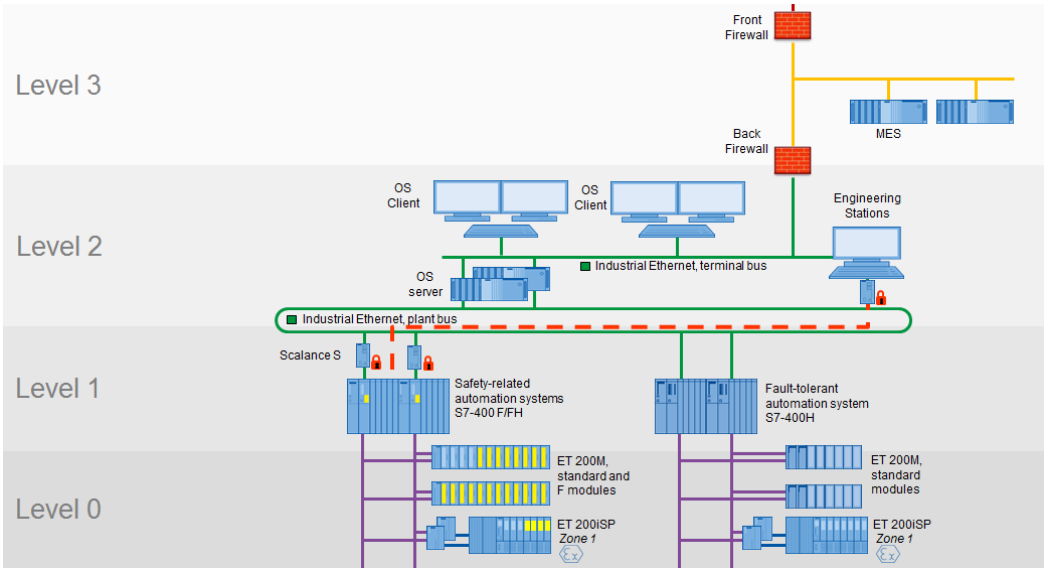

Figure 6: SIMATIC PCS 7 configuration example with Integrated 1 Zone SIS

As part of the defense-in-depth strategy, the SIMATIC PCS 7 configuration is in a security cell with double firewalls. Measures such as "system hardening", "user and patch management" as well as "malware detection & prevention" protect the engineering station (ES).
In the user management, the SIS is protected in the ES and on the CPU level with independent layers:
In ES, the SIS project (embedded in a multi-project) has access protection based on the SIMATIC logon tool. For changes in the SIS project, an F-Password is necessary as part of the safety engineering tool. Access to the safety automation system requires the CPU password. An additional physical key-operated switch for access protection to the CPU can be used.
Further, communication to the SIS can be limited to just a few participants on the plant bus or via personalized firewalls or VPN (e.g. using Scalance S) as part of the secure communication strategy.
If the security risk analysis requires a separate ES for the SIS, an ES client can be used for the SIS application, which is still part of the common data base for the HMI.

5. Conclusions

There are several common scenarios where an isolated system can become compromised, e.g. when using a USB memory stick. This means that a security risk analysis for the SIS is required, also for air-gapped architectures.
A check must be made that an air-gapped architecture really does exist. Today, SIS also has connections to data management systems and the internet (e.g. alarm management systems and production management systems).
The defense-in-depth strategy and the additional security layers for the SIS should satisfy all security requirements identified from a risk analysis. All benefits of an integrated approach for SIS & BPCS, so that alarming, diagnostics and visualization are generated automatically, can be used when considering the security aspects

Reference

IEC 61508 Ed.2, 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511 Ed.2, Functional safety – Safety instrumented systems for the process industry sector (CDV)
IEC 62443 series “Security for industrial automation and control systems - Network and system security”
ISA-TR84.00.09, 2013, Security Countermeasures Related to Safety Instrumented Systems (SIS)
Process Control System PCS 7 Compendium Part F- Industrial Security (V8.1), 04/2015, A5E35032082-AA, https://support.industry.siemens.com/cs/ww/en/view/109476100