The rocky relationship between safety and security

Best practices for avoiding common cause failure and preventing cyber security attacks in Safety Systems

Abstract:

An industry practice reflected in the international safety standards (i.e. IEC 61508) is the need for independence among the multiple protection layers on an industrial site "…the EUC control system shall be independent from the E/E/PE safety-related systems and other risk reduction measures…" however even the 1st generation of digital Safety Systems (Electronic/Programmable Electronic Systems) had communication ports with support for open protocols (i.e. Modbus RTU) in order to provide diagnostics and other information relevant for the operation of process (EUC).

Users have connected (interfaced) safety systems to BPCS since mid 1980s and aimed to develop tighter connectivity at least since 1995. These efforts were based on proprietary protocols until the adoption of open network protocols and Windows on industrial control systems increased the connectivity to business systems and at the same (at least in theory) exposed them to the same issues (virus, cyber attacks, etc).

This paper will discuss the methods used to ensure that the integration between the safety system and the BPCS DO NOT compromise Functional Independence and define best practices to secure an industrial system and in particular safety systems in this integrated environment.

1 Why do we care about safety (and security)?

A report published by Aberdeen Research in November 2011 (Ismail, 2011) indicates that despite the difference in motivations, Best-in-Class companies must establish a formalized risk management strategy and ingrain safety as part of the culture through executive leadership. One of their drivers is to manage and reduce the adverse event, in other words to avoid Impact on Health, Safety and Environment while staying productive and in compliance with regulation and recognized best engineering practices. Does Security deserve similar consideration?

Safety and Security had received a lot of attention in recent years. James Reason, in his book Human Error (1990), applied the concept of safety barriers which describes the isolation between the hazard and its consequence as slices of Swiss cheese, where the risk controls of people, plant and processes are shown as slices of cheese with holes representing the failures or weaknesses in each of the protective barriers in place. In such a model, the coincidental failure of several barriers designed to prevent the event escalating to a major outcome is shown as the holes in the barriers lining up to give clear line of sight to allow the escalation. The model show no single failure ever caused a major accident and as exemplified in Texas City, Deepwater Horizon, and many others; such catastrophic events can always be traced to multiple failures either in plant, people or processes. (Whewell, 2012)

As one of these multiple barriers, safety instrumented systems, which are digital systems and often connected to a network, there is a real concern that a targeted cyber attack can disable or affect its performance, causing or simply creating the opportunity for a major incident. These concerns have been proven real by a series of incidents targeting industrial sites and reported periodically on the media and specialized blogs (http://www.isssource.com/).

This paper will discuss the methods used to ensure that the integration between the safety system and the Basic Process Control Systems (BPCS) DO NOT compromise Functional Independence and define the best practices to secure an industrial system and in particular safety systems in this integrated environment.

2 Definitions

To ensure a common understanding, this paper will start by defining safety and security

2.1 Safety

Multiple sources, including International Safety Standards (i.e. IEC 61508, IEC61511/ISA 84) define Safety as freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment.

In order to control process hazards and to achieve an acceptable level of risk, process operators have the choice of being protected from the event or from the exposure to the event. On the automation front, Safety Instrumented Systems can be use both for protection from or mitigation of the exposure.

Functional Safety is the part of the overall safety of a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of unintentional but likely operator errors, hardware failures and environmental changes.

2.2 Security

Computer-based systems (generically referred to as programmable electronic systems) are being used in all application sectors to perform non-safety functions and, since the 1980's, to perform safety functions. It is the extended use of programmable electronic systems and the need for integration that has brought cyber security concerns to the plant floor.

As defined in the standard (ISA) and in the context of this document, security means the prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in industrial automation and control systems. *Electronic security (cyber security),* the particular focus of ISA 99 standard, includes computers, networks, operating systems, applications and other programmable configurable components of the system.

2.3 Different Aspects of the Same Problem

Safety focuses on the potential result of an occurrence defined as a risk. Meaning something is identified as a Safety problem if there is an unacceptable risk of damage to people, property or the environment. A Security problem is independent of the result of the action. A Security problem refers to illegal or unwanted penetration, interference with proper operation or inappropriate access to confidential information regardless of motivation (intentional or unintentional) or consequence (result).

3 Why the increased emphasis on security?

As indicated in the security standards (ISA), several trends contribute to the increased emphasis on the security of industrial automation and control systems:

a) In recent years there has been a marked increase in malicious code attacks on business and personal computer systems. Businesses have reported more unauthorized attempts (either intentional or unintentional) to access electronic information each year than in the previous year.

b) Industrial automation and control systems are moving toward COTS operating systems and protocols and are interconnecting with business networks. This is making these systems susceptible to the same software attacks as are present in business and desktop devices.

c) Tools to automate attacks are commonly available on the Internet. The external threat from the use of these tools now includes cyber criminals and cyber terrorists who may have more resources and knowledge to attack an industrial automation and control system.

d) The use of joint ventures, alliance partners, and outsourced services in the industrial sector has led to a more complex situation with respect to the number of organizations and groups contributing to security of the industrial automation and control system. These practices must be taken into account when developing security for these systems.

e) The focus on unauthorized access has broadened from amateur attackers or disgruntled employees to deliberate criminal or terrorist activities aimed at impacting large groups and facilities.

f) The adoption of industry standard protocols such as Internet Protocol (IP) for communication between industrial automation and control systems and field devices has introduced additional risk. Implementing IP exposes these systems to the same vulnerabilities as business systems at the network layer.

The combination of these trends increase an organization's risks associated with the design and operation of their industrial automation and control systems. At the same time, cyber security of industrial control systems has become a more significant and widely acknowledged concern.

4 Is there a difference between Functional Safety and Cyber Security?

As mentioned earlier, Safety (and Functional Safety) deals with random and unintentional events (accidents and failures). Statistics can be used and Mean Time Between Failures (MTBF) can be calculated. Additionally, Security also deals with intentional acts, targeting a subject, statistics are not applicable as Mean Time Between Attack can not be calculated.

With the advant of computer based systems, networking and corporate wide data access, both Safety and Security issues can cause potentially dangerous events within a plant. As a result, Cyber Security is covered in the recent edition of Functional Safety Standard IEC61508 (IEC) (Edition 2, Section 7.4 Hazard Analysis). The revised standard requires that in the case where the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, is reasonably foreseeable, a security threat analysis should be carried out. Section 7.5. (Overall Safety Requirements) recommends undertaking a vulnerability analysis in order to specify security requirements.

It can be said that both Safety and Security imply the need for protection, however the chosen protection must address risks that are radically different in nature. However, there is an important similarity; neither Safety nor Security is a onetime event. As indicated in IEC61508 (IEC) and ISA 99 (ISA), a common mistake is to address safety and cyber security as a project with a start and end date. When this occurs, the safety and the security level will tend to decline over time. Particular to Cyber security, risks constantly change as new threats and vulnerabilities surface along with ever-changing technology implementations.

It is no longer possible to be truly Safe without also being Secure. However, the challenge is to not only address security issues, but to get the most from the ability to connect systems and share data. There seems to be a fine line between security and productivity.

5 The Value of Certification

5.1 Value of Certification in Safety

Third party certification of compliance to national and international safety standards is very common in the Safety Automation Market and has become a common requirement across the industry. This certification is valuable to users because the third party agency conducts standardized tests that

demonstrate the systems' ability to meet the criteria defined in a given standard and operates independently from vendor and the users/buyer.

This independent test typically reduces the scope of corporate or project specific test requirements from the buyer. However, certification can't be assumed as proof that the system will never fail. Buyers/users should avoid feeling overconfident simply because they chose a product backed by the third party certification by a recognized entity. A formal safety and security policy, implemented corporate wide, will help drive the safety culture necessary to ensure a truly safe and secure operation.

As a matter of fact, IEC61511/ISA 84 defines a safety lifecycle process and a Functional Safety Management System which identifies a series of tasks and processes required to ensure safe implementation and minimize faults that might impact the safety of the installation in the same way as a product fault.

5.2 Value of Certification in Security

Similarly, security certification by independent assessors is important, but should be the beginning of a journey rather than the end of it. While the certification programs include many types of assessments geared towards handling known as well as unknown threats, there is are new threats appearing every day. Certification is a good start, but constant vigilance is required to minimize risk.

As in the case of safety certification, this independent test and certification typically reduces the scope of corporate or project specific test requirements from the buyer. However, certification can't be assumed to provide an absolute shield, buyers/users should avoid a "False Sense of Security" simply because they choose a product backed by the third party certification. One of the major challenges with certification is knowing exactly what has been certified by each vendor (which is not always apparent in the high level certification documents).

Similar to the case of Safety Certification, ISA 99 (ISA) also introduces the concept of a Security Management System which defines a security lifecycle that will assist the users in establishing and maintaining the installation security level over time.

6 The Challenge of Legacy Safety Systems

Basic Process Control Systems (BPCS) and Safety (SIS) implementations were based on different technologies operating independently, however the need to present the operator with critical information including information from the safety critical systems has always been present.

The authors would like to differentiate three cases and their respective risk profiles in order to discuss the positive and negative aspects of each:

1. Independent Systems or "Absolute Air Gap"
2. Secured Open Network Interfaces
3. Integrated Control and Safety Systems

6.1 Independent Systems or "Absolute Air Gaps"

Early Programmable Electronic Systems (PES) were conceived as isolated units and not designed with cyber security in mind (Schweigert, 2012) but can actually be considered the example of an ideal "air gap" (Byres, 2012). The reality is that users have connected (interfaced) safety systems to BPCS to satisfy the need for information; therefore this ideal case is rare.

Even when a network interface between the two systems is not available, the system can be exposed to cyber security threats. A clear example is the computer used to program the safety system can be affected by a virus or malware and affect the plant system. In summary, isolating a computer from the system network as a security plan does not address recommended security measurements like:

- Updating the operating system to mitigate recently discovered threats,
- Updating antivirus definitions,
- Establishing backup procedures that were not common in early systems or left to the user to define or adopt as part of their corporate security practices.

In short perception is not always reality.

6.2 Secured Open Network Interfaces

Since both systems (BPCS and SIS) will be interfaced to provide the operator with critical information including information from the safety critical systems, the responsible action would be to:

1. Perform a full vulnerability assessment/threat modeling and testing of the different subsystems of the interfaced architecture
2. Define the best security mechanism for each of those subsystems to cover any identified gaps
3. Perform a full vulnerability assessment/threat modeling and testing of the entire interfaced architecture

Establishing a Security Management System of the interface architecture and supporting it over the system lifecycle will represent a challenge. One possible way to address this in an open interface environment is to implement a Management of Change Program.

A management of change (MOC) program (ISA), as defined for safety applications, reviews any future process or control and instrumentation changes with a wide variety of stakeholders to see if the proposed change will cause unforeseen and negative safety side effects.

A management of change security program is similar, except that prospective changes are reviewed for unforeseen and negative effects of process or control and instrumentation changes on the security of the system. When implementing a security management of change program, changes to control systems must be examined for their possible effects on safety, and vice versa. The security management of change program should be integrated into the Process Safety Management program at the site so that a holistic assessment is made of any changes to the Manufacturing and Control System.

6.3 Integrated Control and Safety Systems

This paper will discuss the methods used to ensure that the integration between the safety system and the BPCS DO NOT compromise Functional Independence and will define best practices to secure an industrial system and in particular safety systems in this integrated environment.

The perception is that Integrated Systems cannot be secure. Comments such as too much integration might compromise the required Functional Independence or that sharing the network exposes the SIS to cyber attacks are only scratching the surface of the problem.

The authors support the SD^3+C security framework for security of Industrial Automation and Control Systems (IACS) or Integrated Control and Safety Systems (ICSS).

From the vendor's point of view, this security framework is based on four elements:

1. **Secure by design:** The architecture and code have been developed according to processes that specifically address security, and conscious efforts have been made to analyze threats and to identify and remove vulnerabilities. The products include relevant features and mechanisms that help ensure secure operation.

2. **Secure by default:** After installation the system by default presents a minimal attack surface. This is accomplished by secure default configuration settings and by automatically disabling unused functions.

3. **Secure in deployment:** User documentation and training is sufficient so that the system can be installed, configured, and operated in a secure way, with adequate features for detection of and defense against attacks, for disaster recovery, and for efficient and secure system management.

4. **Communication:** Responsible communication about important security related information to relevant individuals and organizations.

This paper will cover a few of the SD^3+C elements, as not all IAC/ICSS will have the same functionality, to later emphasize the User side of Secure by Deployment over the system lifecycle.

7 Standard Practices

The industry standard practice reflected in the international safety standards (i.e. IEC 61508) is the need for independence between the multiple protection layers on an industrial site; “the EUC control system shall be independent from the E/E/PE safety-related systems and other risk reduction measures”. There are a number of standard practices that can be used by the vendors and users to mitigate the risk of a security driven incident.

7.1 Secure by Design

Secure by Design focused mainly on the product development process. World class product organizations will already have this concept embedded into their processes and organization. The developers’ Quality Management System should address the security aspects in the product development process. In addition to general quality assurance methods, it should prescribe the usage of threat modeling, secure coding guidelines and security testing.

7.1.1 Threat modeling

Threat modeling is a method for assessing and documenting the security risks associated with a computer system or application. It helps development teams during specification, design, development, and maintenance of the system to identify security weaknesses and set priorities on fixing them, thus ensuring the security objectives of the system throughout its life cycle.

Threat modeling in early stages of the development process provides the basis for security requirements and design principles for the system. When revising the threat model in later stages vulnerabilities may be found. Like other bugs, these are reported and tracked in the R&D organization’s defect tracking system with the goal to be corrected.

7.1.2 Secure Design and Coding

During development, all new functions are documented. Functional descriptions are reviewed to ensure that the requirements are fulfilled. Design descriptions are reviewed to ensure that the design implements the intended function. Test descriptions are reviewed to ensure that they include all relevant test cases for non-functional as well as functional aspects of the product.

Developers use programming guidelines for improving the quality of program code. This includes guidelines that focus on how to avoid mistakes that can cause security problems. These guidelines are based on commonly accepted recommendations such as the US CERT secure coding guidelines.

Program code is reviewed to ensure that it implements the intended design and that the coding guidelines are followed. Design and code reviews are based on checklists to ensure that important aspects including security are covered.

7.1.3 Quality assurance testing

All functions are tested to ensure that they work as expected during use under both normal and abnormal conditions. This includes for example testing of communication robustness and scanning for vulnerabilities. This testing is done by the development teams.

7.1.4 Device Security Assurance Testing

In addition to the testing performed by the development teams, all new products and product versions should be tested by a Device Security Assurance organization. This is a laboratory run by dedicated personnel, not part of the development teams, using several specialized tools (e.g. Achilles Satellite Unit, Mu8000) for security testing. Some of the test principles are:

- Profiling to verify the attack surface
- Scanning for known vulnerabilities
- Denial of Service attacks
- Robustness testing using protocol fuzzing, i.e., the test tool creates randomly malformed packets that break the rules of the protocol, to verify that such errors are handled in a robust and secure way. This is a way to test for unknown vulnerabilities.

The test results should be presented to the product responsible group which takes care of any detected vulnerabilities.

7.2 Secure by Default

Secure by Default is based primarily on the concept of Defense in Depth, which is a common term applied to describe the goal of a practical multi-layered security implementation. This provides guidelines for creating a minimal attack surface, a standard installation and securing the default and system settings.

7.2.1 Defense in Depth

The principle of Defense in Depth means creating multiple independent and redundant prevention and detection measures. The security measures should be layered, in multiple places, and diversified. This reduces the risk that the system is compromised if one security measure fails or is circumvented. Defense in depth tactics can be found throughout the SD^3 + C security framework.

Examples of Defense in Depth tactics include:

- Establishing defenses for the perimeter, network, host, application and data
- Security policies and procedures
- Intrusion detection
- Firewalls and Malware protection
- User authentication and authorization
- Physical security

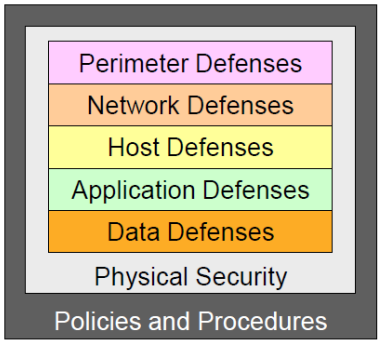

Figure 1: Defense in Depth

These types of tactics will provide yet another “layer of protection” for a plant, complimenting the existing layers (see diagram below).

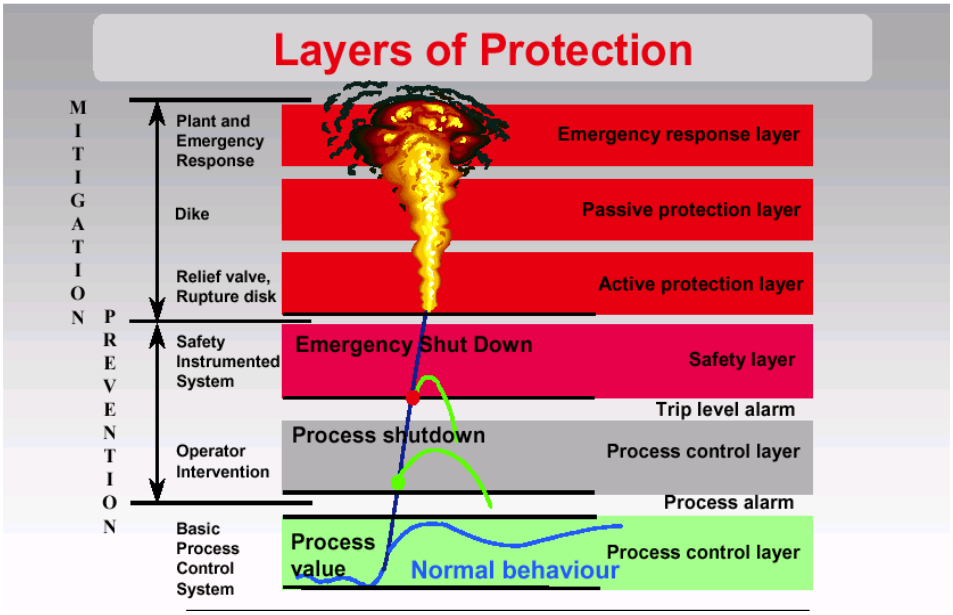

Figure 2: Typical Layers of Protection

7.2.2 Default Settings

One simple way to further secure a Control System or SIS is to secure the default setting of the systems during installation and commissioning. This includes:

- Automate installation for a consistent and repeatable load (system installation)
- Disabling or not installing unnecessary services
- Enable and configure Windows firewall setting for the installed services
- Secure the default settings for user privileges
- Limited embedded operating systems to only the needed features

7.2.3 Secure Architecture / Network Defenses

The system architecture is based on the well established security principles such as Defense in Depth and Security Zones.

The principle of Security Zones means segmenting a system into different zones for different security levels. All resources in the same zone must have the same minimum security level, and access between zones shall only be allowed through secure conduits.

In client server architectures, it can also be important to protect communications with the IPSec protocol for authenticating and encrypting each packet of a communication session. This will help eliminate security issues arising from unauthorized devices communicating on the client server network.

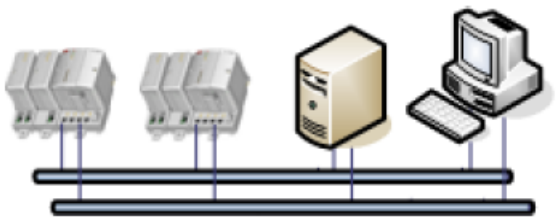

Figure 3: Redundancy with Separated Networks

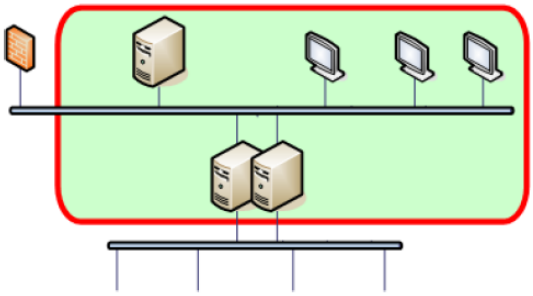

Figure 4: Client Server Network w/ IPSec

7.2.4 Communication with Safety Systems

Communication with safety certified functions in the system complies with SIL 3 according to IEC 61508. The SIL3 certified communication concepts are:

- Access Control using a physical key switch for controlling configuration changes
- TUV Certified SIL3 Peer-to-peer communications between safety controllers
- Safe Online Write from Operator workplace (not a standard feature on Interfaced Systems)
- Network filter in Controllers and Communications modules blocks unsupported traffic

These functions should be designed to handle unintentional communication problems or mistakes. They also provide basic protection against intentional attacks.

7.2.5 User Authentication and Access Control

User authentication and access control are more examples of the Defense in Depth security concept. These features enable users to specify who can do what. There are additional features that support SIS systems to ensure only authorized users can make safety related changes. Best practices include implementing any or all of the following functions:

- User Authentication based on Windows active directory or workgroups
- IAC/ICSS access control settings based on User, Role and Location. On some systems, these can be set on the Structure, Object and Attribute level providing even more granular control.
- Re-authentication or double authentication on certain functions
- Log over function to ensure one person is responsible for the system (on shift change etc.)
- Audit trail of user actions for history and root cause analysis
- Digital signatures

These features can not only provide “gated” access to system functions, but can also capture information for audit trail as well as troubleshooting and incident reporting.

7.3 Secure in Deployment

IAC/ICSS Vendors' User Documentation should present recommended network architecture and reference designs for the user to select based on their needs, including the required system connectivity (interface, integrate or combined) and their security policy.

7.3.1 Protection against Malware with Antivirus Solutions

The vendor should recommend the virus scanner to be used on the IAC/ICSS servers and workplaces, and provide technical descriptions describing how to configure the virus scanners to ensure that they do not interfere with the system's operation.

The vendor should also validate virus definition files (i.e. for McAfee and/or Symantec) to minimize the risk that false positives are detected in IAC/ICSS. Users should await this validation before installing new virus definition files.

7.3.2 Disaster Recovery

IAC/ICSS should provide features to assist in the recovery of a system failure.

- It should be possible to create total and/or selective application data backups and disk image backups during normal operation of the IAC/ICSS.
- Restoring data from an application backup should be possible.
- Restoring data from a disc image backup should be used for restoring from a failure of a server or workstation.
- It should also be possible to perform backups for Network equipment, such as routers and switches, from a central location in the system.

Tools and procedures for Backup and Restore should be described in user documentation.

7.3.3 Patch Management

This section describes processes and tools for software updates on the IAC/ICSS and related 3rd party software products.

In addition to the IAC/ICSS specific software, all Microsoft and other 3rd party software security updates should be evaluated when they are released:

- All relevant updates should be tested for compatibility with the IAC/ICSS
- Testing should be done when Microsoft releases Security updates. This normally means once per month, but out-of-band releases are normally also tested as soon as they are released.
- The testing should be done in a dedicated Security Test Lab, in different system configurations, covering all supported IAC system versions.
- Result should be published as an update for users with a software maintenance contract.
- 3rd party software includes products such as Adobe Reader.

7.4 Developing a Security Program

Effectively integrating security into a Manufacturing and Control System environment requires defining and executing a comprehensive program that addresses all aspects of security, ranging from identifying objectives to day-to-day operation and ongoing auditing for compliance and improvement.

Selection of activities and practices for a given system is the responsibility of the system's owner and although following the recommended guidance in ISA 99 (ISA) will not necessarily ensure that optimized cyber security is attained for IACSs, it will help to identify and address vulnerabilities. A security policy will also help reduce the risk of undesired intrusions that could compromise or cause disruption or failure of control systems and the critical infrastructure assets they automate and control and may aid in reducing the risk of any human or environmental harm that may result after the cyber compromise of an automated control system, or its associated industrial network.

Some basic steps for implementing a Security Management System are as follows:

- Use the security standards as guidelines: IEC27000, ISA / IEC 62443 (ISA99)
- Perform a security risk assessment (in addition to the standard safety system risk assessment)
- Develop a security policy and define clear organizational responsibilities
- Select security countermeasures:
    - Define who should use the system for what (including humans, software and devices)
    - Protect the system from problems or inappropriate access
    - Detect problems and provide timely response to events
    - Manage system resource availability (backup/restore, power, system hardening, component inventory and spares)
- Plan for incident response and disaster recovery
- Audit security systems and procedures for compliance with the security policy

8 Summary

Safety and Security deserve similar consideration as key drivers to manage and reduce adverse events, and avoid Impact on Health, Safety and Environment while maintaining a process productive and in compliance with local and global regulations.

The concerns that a targeted cyber attack can disable or affect the safety instrumented systems performance and cause or create the opportunity for a major incident are real. Assuming that Integrated Control and Safety Systems cannot be secure or exposes the SIS to cyber attacks are only scratching the surface of the problem. Even when a network interface between BPCS and SIS is not available, the system can be exposed to cyber security threats.

Similarly, safety and security certification by independent assessors is important, but should be the beginning of a journey rather than the end of it. While the security certification programs include many types of assessments geared towards handling known as well as unknown threats, there are new threats appearing every day. Certification is a good start, but constant vigilance is required to minimize risk.

Certification can't be assumed to provide an absolute shield; buyers/users should avoid a "False Sense of Security" simply because they choose a product backed by the third party certification, more is required from them. ISA 99 (ISA) introduced the concept of a Security Management System, which, in a similar fashion to IEC61511/ISA84 Functional Safety Management System, defines a security lifecycle that assists the users in establishing and maintaining the installation security level over time.

The authors support the SD^3+C security framework for security of Industrial Automation and Control Systems (IACS) or Integrated Control and Safety Systems (ICSS). From the vendor's point of view, this security framework is based on four elements design, default, deployment and communications. Those four elements support users in the design and implementation of a sustainable solution over the lifecycle of the production asset.

Although Safety and Security focus on different problems, causes and consequences, it is no longer possible to be truly Safe without also being Secure. However, the challenge is to not only address safety and security issues, but to get the most from the ability to connect systems and share information conducive to effective and efficient decision making. There seems to be a fine line between safety, security and productivity.