The challenges and recommended steps to improve cyber security within industrial control systems

(Safety & security alignment benefits for operational integrity)

Rahul Gupta

Wood Group Mustang, Kuala Lumpur (Malaysia)

Keywords

Safety Instrumented System (SIS), ISA 84 (IEC 61511 Modified) standard, IEC 61508 standard, IEC 61511 standard, ISA 99 standard, IEC-62443 standard, Functional Safety (FS), Safety Life Cycle, Cyber Security, Defense in Depth, Security, ICS, Information Technology (IT), Operation technology (OT), Risk, Human factor, Hazop, Chazop

Abstract:

"Security - Protection against attack, Safety - Freedom from risk and harm"

End users or operators of industrial control systems (ICS) are responsible for the security of the systems. Many end users, however, find a challenge in addressing simple issues, typically: What requires protection from cyberattacks and how much protection is required? Will a critical system disruption or cyber theft cause a disruption to the business? If yes, how much? What is the recovery process? What is the recovery cost?

This paper will provide insight to the challenges end users face related to cybersecurity for an ICS. It will also discuss & recommend the steps to improve the security and reliability of very critical ICS, including how maturity models can improve energy sector cybersecurity capabilities and provide options in prioritizing cybersecurity investments.

Safety and security has received a lot of attention in recent years. This paper represents a compilation of benefits based on best practice; lessons learnt and author experience if functional safety and cyber Security for an ICS are integrated.

Effective management of cybersecurity challenges and exposures in the ICS environment has emerged as an important and dynamic element in the operational safety, security and reliability of the oil and gas industry infrastructure. Management information systems (MIS) are not within the scope of this paper; solely their interfaces with ICSs are discussed.

When considering security for businesses and industry, there are three traditional areas: physical security, personal security and cybersecurity. Cybersecurity aspects are the main focus of this paper.

This paper will provide an oil and gas industry insight into cybersecurity risk management as per ISA-99/IEC-62443. It will explore the similarities / differences between IT and ICS protection plus risk management, inclusive of possible ways for the integration of safety and security in an oil and gas industry ICS.

What is an Industrial Control System (ICS)?

An industrial control system (ICSs) designates a set of devices that directly control the manufacturing processes or operate technical installations (consisting of a set of sensors and actuators). Naturally, this covers the control-command systems that we find in many operating sectors – oil and gas, energy, power, water, chemicals, pipelines, military systems, medical systems, etc.

Other frequently used terms for ICS, apart from slight differences in connotation, are distributed control systems (DCS), industrial automation

control systems (IACS), process control systems (PCS), and supervisory control and data acquisition (SCADA), intelligent electronic device (IED), digital protective relay, smart motor starter/controller, remote terminal unit (RTU), smart sensors and drives, emissions controls, equipment diagnostics, AMI (smart grid), programmable thermostats, building controls etc.

Challenges with ICS cybersecurity faced by end users

Before any end user spends time to increase the ICS plant floor security, a few simple issues need addressing by the business management:

Plant Manager

- Are there any personnel, process safety or environmental consequences to an ICS security breach, and how severe are those consequences?
- What needs protecting and how much protection is required?
- Will a critical system disruption or a data theft cause a disruption to the business?
- How long will the business be down?
- What is the recovery process, cost to recover?
- Will the business ever recover?
- And most importantly, who could threaten the business (who is the enemy?)…..the big dark underworld cyber terrorist or one of the company's best employees?

CEO

- What are the Cybersecurity risks and potential business impacts to the prime business objectives?
- What are the current Cybersecurity risk level and potential business impacts?
- Does the business risk assessment follow ALARP principle meeting current regulations, industry standards and good practices?
- What governance structures / incident response structures are in place where accountabilities and responsibilities for ICS security are clearly defined and accepted?
- Is the workforce fully aware / appropriately trained on possible cyber threats to the ICS?

Information Security Officer (ISO)

- What strategies are in in place to identify and manage the cybersecurity risks to the ICS?
- How are cybersecurity maturity and compliance levels measured?
- Has an effective set of controls that will reduce the risk to ICS to ALARP been selected?
- How comprehensive is the ICS incident response plan? How often is it tested?
- How many and what types of cybersecurity incidents to the ICS occur per reporting period? What is the threshold for notifying the executive leadership about a cybersecurity incident?
- How well do the IT and process automation / production departments communicate and collaborate on cybersecurity?

Maturity Models

A maturity model is a framework that allows an organization to assess the rigor of its security practices and processes according to industry best practices. The U.S. Department of Energy (DOE) has developed a maturity model specifically for the oil and gas industry - the Oil and Natural Gas Cybersecurity Capability Maturity Model (ONG-C2M2). This model, part of a broader effort to improve security in the energy sector, is one of the few that includes both IT and OT and provides a mechanism to help evaluate, prioritize and improve cybersecurity capabilities in both areas.
It is intended to help:

- Strengthen cybersecurity capabilities in the oil and gas subsector.
- Enable oil and gas organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities.
- Share knowledge, best practices and relevant references within the subsector as a means to improve cybersecurity capabilities.
- Enable oil and gas organizations to prioritize actions and investments to improve cybersecurity

The ONG-C2M2 model is descriptive rather than prescriptive, allowing companies to select their own goals and establish the appropriate controls and policies for meeting them.

IT /OT and their relationship to ICS:

ICS vendors have traditionally functioned most often as comprehensive vendors, meaning that they have both designed and built the systems

they supplied. These days, increasingly standardized technologies and components from the traditional IT world (often referred to as commercially available off-the-shelf, (COTS) are being used in ICS. Some examples of COTS products used are Microsoft operating systems, IP-based communication technology (Ethernet/IP, TCP/IP etc.), MS-SQL and Oracle database solutions. This shift to standard components is changing the role of the vendor from system supplier to system integrator. This, in turn, can lead to a reduction in vendor insight and control of important components of the integrated system. Subsequently, increased knowledge of ICS security is required by the end users of the systems.
Let's first look at IT and OT and their relation to ICS:

Operational Technology (OT) is an umbrella term used for various technologies that support operations. It consists of hardware and software systems that monitor and control physical equipment and processes for safe & reliable operation, often found in industries that manage critical infrastructure, such as water, oil & gas, energy, and utilities, but also in automated manufacturing, pharmaceutical processing and defense networks.
This technology uses many specialized terms such as PCD, PLC, DCS, SCADA and SIS, often collectively referred to as industrial control systems (ICS).
The operational technology (OT) systems that oversee the volume, velocity, location and other vital activities in the production and distribution of various industries such as oil & gas, not only produce a wealth of sensitive and proprietary information, they are also essential to the economic health and physical safety of the company, its facilities and its people.

While the technology is familiar to operators and engineers in these sectors, outside of people working in or with these specialized environments, there is a limited understanding of what's involved. Within the control systems industry, ICSs are often referred to as OT systems.

In contrast, **Information Technology (IT)**, managed by information officer (IO) and IT departments, is the application of computers to process, transmit and store data, typically in a business or enterprise environment. IT systems are in place to allow machines to exchange information directly with humans, usually within seconds. Various industries have experienced an exponential increase in both quantity and quality of IT systems. Improved enterprise resources planning (ERP), geographic information systems (GIS), and customer relationship management (CRM) systems, along with office-based productivity tools and mobile computing devices, have permeated the business workplace.

	Information Technology	Operational Technology
Purpose	Process transactions, provide information	Control, monitor, or protect physical processes and equipment
Operating environment	Offices, data centers, control centers	Field equipment, substations, control centers
Architecture	Enterprise-wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (customized), highly distributed data processing and control
Interfaces – inputs and outputs	GUI, web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices as well as GUI / human-machine interfaces
Ownership	CIO and computer graduates, finance and administration departments.	Engineers, technicians, operators and managers
Connectivity	Corporate network, IP-based	Proprietary and industry standard control networks, hard-wired twisted pair and IP-based
Role	Supports people	controls machines and process conditions
Security objective priority	Confidentiality, integrity, availability	Availability, integrity, confidentiality

Table 1 – Security focus and other performance parameters in IT versus OT

IT versus OT

Historically, OT and IT have not overlapped and were managed as separate organizational silos. IT

and OT have long, isolated histories with many examples of failed attempts to integrate them or even use tools from one environment to the other.

OT and IT were developed to accomplish two distinctly different missions, with contrasting agendas and dissimilar tools and priorities. There are several other similar differences between IT and OT [Refer table-1].

ICS cybersecurity- organization challenge IT or OT

The hurdles, however, of ensuring good cyber safety do not stop at choosing the right technical protection. It is the organizational structure of companies that holds a whole new set of challenges.

The difficulty in the oil and gas industry is that invariably there are two organizations: the IT organization that is traditionally responsible for security and the engineering organization, which is traditionally responsible for operation technologies. In order to achieve effective cyber safety it is imperative that these two organizations work together and learn to understand each other's objectives / start speaking the same language.

The IT organization is used to the concept of cybersecurity and building security into their solutions. Whereas, the engineering organization, which is focused on the reliability and availability of its plants, invariably has no or only a limited understanding of cybersecurity.

The responsibility for cybersecurity often lies with the IT department, which fails to understand the embedded IT in the ICS. At the OT working level there is a certain amount of push-back due to the concern about how cybersecurity measures may impact operations safety and efficiency. Not recognizing that, nor implementing these measures, may have a greater potential for impacting safety. The end result is that the organization may fail to adequately manage the cybersecurity risks to the ICS.

Since the turn of the century, however, business demands and economics have had a major impact on these problems. For example, in the energy sector the introduction of real-time energy trading markets has demanded responses that have necessitated more convergence between the two systems. The OT community needs the IT community because they are able to identify issues that OT doesn't see but, IT does not understand the OT environment so bridges between the two groups are required.
OT and IT certainly have significant hurdles to overcome in pursuit of collaboration, none greater than the challenge of achieving security and interoperability without disrupting critical services or diverting excess capital from the enterprise.
How cyberattacks are identified also looks vastly different. Enterprise IT owners know they've been hacked whereas OT owners must recognize a physical event (e.g. a pipe breaks) and work it backward to find the culprit, cyber or otherwise. So the ICS needs forensics and cyber logging.

Integrated IT and OT security - New trend

Integrated IT and OT security is a new trend in the oil and gas industry, although there are varying levels of awareness and implementation:

- Some organizations have little or no awareness of, or interest in, the issue,
- Some are aware of the need but are unsure how to proceed.
- Some are addressing security but are not as advanced as they believe,
- Whilst others have misplaced confidence in IT perimeter defenses that cannot adequately protect OT systems.
- A very few have established a robust and on-going security program and management system.

There still exist misconceptions with ICS being monitored by IT professionals resulting in many oil and gas companies that are poorly protected against cyber threats, at best. They are secured with IT solutions that are ill adapted to legacy control systems Or OT being negatively impacted by IT Cyber Security measures that are not aligned with the criticality of Availability and Integrity in OT systems.

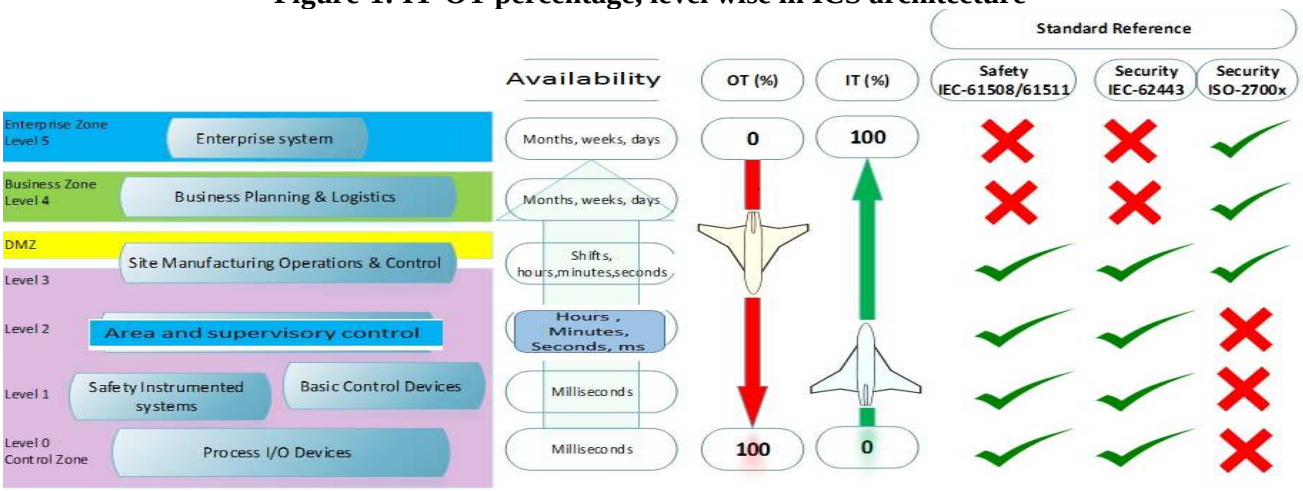
To those not directly involved it may seem that the ICS falls under the umbrella of the IT experts, but typically, that is not the case.

ICS architecture-combination of IT and OT

The ICS-level architecture is used to define the accreditation boundary for OT systems and is a logical representation of the OT network. The actual physical system can span many miles; for example, pipelines, electric transmission and distribution systems can have many non-contiguous components, and there are a number of protocols commonly used by ICSs to allow the devices within the layers to communicate both horizontally and vertically.

The ICS architecture is described in five levels (and multiple sub-levels), where each level represents a collection of components that can be logically grouped together by function. Generally this is the preferred reference model as per ISA 99/IEC 62443. This model has become the standard for networks in industrial companies being adopted from the Purdue model that was developed to define and segregate the systems, components and activities in an industrial company. This ensured that higher level activities, such as reporting, would not interfere with the control and data acquisition of the process. As cybersecurity risk management needs emerged, the reference model facilitated the clear identification of segregation points where network protection/ isolation devices could be installed. It is worth noting that not every implementation of an ICS makes use of every level and that the same device may reside in different levels, depending on its configuration. A composition of IT & OT components in a level (as shown in figure-1) is for discussion purposes and may vary depending on system architecture, application etc. Most current ICSs and subsystems are now a combination of OT and IT.

Figure-1: IT-OT percentage, level wise in ICS architecture



ICS cybersecurity - recommended actions for end users:

It is important that ICS cybersecurity requirements are defined at the start of the project such that system manufacturers are informed from the outset.

ICS manufacturers are starting, and soon it will be mandatory, to include security requirements in the design phase of ICS components and applications. Operators, however, indicate that independent evaluations and tests are missing to effectively guarantee that these devices are secure, and interoperability has also been considered when new security features/ capabilities are included.

ICS operators, must understand the relevant dependencies, including managing the cyber risks across interfaces with third parties. The following good practices should be adopted:

- Include cybersecurity requirements in the system requirements presented to suppliers. These cybersecurity requirements should be derived from cybersecurity risk assessments and analysis of possible mitigating controls.
- When possible, contractually demand that suppliers and their subcontractors comply with end user's cybersecurity approach and policies. Owner/Operators also need to be cognizant of how different parts of their control systems have different functions, risks, and potentially exposed edges that must be communicated to the control systems designer

and provider. Otherwise, the threats cannot be properly identified, evaluated and mitigated.
- Mandate that suppliers demonstrate their teams have relevant cybersecurity qualifications for the required tasks and responsibilities. Where required, awareness training on relevant security policies should be provided.

During the specification phase:

- Define the means for conducting preventive and curative maintenance operations
- Specify the location of devices to ensure their physical security; specify the security level requirement of each zone in the required control system. At a minimum, specify who will have access to each zone, area or segment of the physical network.
- Require that software provided be not exclusively compatible with a specific version of another software platform
- Require that software not essential to the running of a system be installed on other machines

During the design phase:

- Reduce system interfaces and complexities to limit the introduction of vulnerabilities during implementation;
- Select components offering the best characteristics to meet security requirements,
- Clearly distinguish user profiles from administrator profiles;
- Make provision for mechanisms to standardize changes on a group of machines

During the integration phase:

- Change default configurations (for example, passwords);
- Delete or deactivate functions that are not used but activated by default;
- Consider deleting debugging functions such as tracking used to analyze ICS behavior.

During the test phase:

- Conduct functional security tests; error tests for business functions and check exceptions
- Test threat scenarios (penetration tests and attempts to gain control)
- Test ways of carrying out maintenance operations at the cybersecurity

Safety and security integration- can we relate functional safety and cybersecurity?

Now we understand that the ICS is a combination of IT and OT but that both IT and OT are different and so is their related security.

Security has not been a crucial factor in the development of industrial control systems or OT. Also OT has one more critical aspect of importance – safety.

An ICS is actually a system of systems. A crude distinction between mainstream IT and control systems is that IT uses physics to manipulate data while an ICS uses data to manipulate physics. The potential consequences from compromising an ICS can be devastating to public health and safety, national security, and the economy. Compromised ICS systems have led to extensive cascading power outages, dangerous toxic chemical releases, fire, floods, chemicals spill, and explosions. It is therefore important to implement an ICS with security controls that allow for reliable, safe and flexible performance [Refer Table-2 for more details of comparison of IT vs ICS].

As systems are becoming more complex and integrated, the distinction between safety and security is beginning to weaken. ISA has also identified a need of alignment between safety and security and defined in ISA-99 (IEC-62443) and ISA-84 (Modified IEC-61511)/IEC-61508. Safety and security are two key properties of the ICS; they share identical goals – protecting the ICS from failures. Safety is aimed at protecting the systems from accidental failures in order to avoid hazards, while security is focusing on protecting the systems from failures thru intentional attacks.

Due to safety traditionally being the primary objective of OT systems, and that safety largely depends on the stability of the systems, Cybersecurity has been a secondary consideration for OT systems, if it has been considered at all. This is changing, however, with the integration of IP networking and the adoption of other standardized protocols in OT, Cybersecurity, with the ability of cyber-attacks to produce physical world results, is now becoming essential to safety.

Weak alignment between security and safety may produce inefficient development and partially-protected systems. A given system is only as Safe as it is Secure" (if the availability or integrity of a safety system or other layer of protection is reduced by a security risk or breach, its ability to provide the required protection is also summarily reduced).

For example, excess costs could be spent on redundant safety and security countermeasures. Furthermore, security counter-measures may weaken ICS safety, or vice versa – safety countermeasures may weaken security. If there is no alignment between safety and security countermeasures, these interdependencies are not detected in the early system development phases and may lead to a number of problems that affect later ICS development or even in the operation phases.

Safety and security are interdependent, and these dependencies have to be considered during ICS design phase.

Why to deal cybersecurity & safety together:

SECURITY TOPIC	INFORMATION TECHNOLOGY	INDUSTRIAL CONTROL SYSTEM (ICS)
Anti-virus/Mobile Code	Common widely used	Uncommon/difficult to deploy effectively
Support Technology Lifetime	2-3 Years diversified vendors	Up to 20 years single vendor
Outsourcing	Common widely Used	Operations are often outsourced, but not diverse to various providers
Application of Patches	Regular scheduled	Rare, unscheduled, vendor specific
Change Management	Regular Scheduled, higher risk tolerance for untested changes in commodity user systems	Highly managed and complex
Response Time	Response time generally not critical. Components may be rebooted	Response time may be part of safety case Availability is paramount to operation
Availability	Generally delays accepted 95 – 99%	24 x 7 x 365 (continuous) 99.9 – 99.999… %
Security Awareness	Moderate in both private and public sector	Poor except for physical
Security Testing/Audit	Part of a good security program	Occasional testing for outages
Physical Security	Secure (server rooms, etc.)	Remote/unmanned secure
Primary subject for protection	Information	Physical process
Primary risk impact	Information disclosure, economic	Safety, health, environment, economic
Security focus	Central server security	Control device and process stability
Operating environment	Interactive, transactional	Interactive, real-time
Problem response	Reboot	Fault tolerance, on-line repair
Authentication	Often centrally managed user accounts	Often local to each device. May be very basic
Performance requirement	Not real time, response must be consistent, delay acceptable	Real time, response is time –critical, delays can create serious problems
Risk management	Data secrecy (confidentiality) and correctness (Integrity) are most important, fault tolerance not serious	Safety is important for both people and production systems, fault tolerance are very important.
Security solutions	Designed for typical IT systems	Security tools and updates must be tested to guarantee that they don't jeopardize the ICS operations
Communications	Communication protocols are standard types and primarily using telephone network/wireless networks	In addition to standard protocol, proprietary protocols are in use. Different media is used - radio links, optical fiber, satellites, VPN etc.

Table 2 – IT versus ICS Comparison

To cover all risks, cybersecurity and safety must be dealt with together, using a joint approach. For example:

1) The potential causes of a temperature increase at a plant above its nominal threshold may be:

- A reading issue linked to the failure of a sensor:

- Physical failure of a sensor,
- Incorrect calibration of the sensor,
- An intentional change e.g. sensor value, range parameter units, time, location hierarchy, etc. made to the parameters of a sensor by an unauthorized person (gaining control by a hacker or a virus) or as a result of negligence;

- A problem associated with a cooling circuit valve:

- Mechanical failure,
- Servo-motor failure,
- Results of an act not undertaken - e.g. remote-auto, intentional forcing of the command valve value by an unauthorized person (gaining control by a hacker, a virus) or as a result of negligence,
- A problem with the setting of the set point for regulating the cooling system,
- An input error made by an operator,
- A change made to the set point by an unauthorized person.

2) The worst scenarios for an ICS are:

- Introduction of malware into the ICS;
- An intrusion into the ICS.

This malicious action may be carried out by an individual on site, remotely via the MIS or via a compromised work station or inadvertent malware injection by portable media or computers connecting to the ICS.
The scenario results in either the loss of one or more operator stations or HMIs (e.g. black or frozen screens, erroneous information displayed) or commands being sent with the intention of causing malfunction.This incident would result in downtime for some units, commonly lasting one to three days until the source of the problem is isolated and remediated.

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.

Safety (and functional safety) deals with random and unintentional events (accidents and failures). Statistics can be used and mean time between failures (MTBF) rates can be calculated. Additionally, security also deals with intentional acts, targeting a subject; statistics are not applicable as mean time between attack can't be calculated. However, the prevalence of persistent threats (e.g. malware and active threat actors) raises these threats to high relative probability. It has been advocated that the threat probability is a 1.0, and the only factor in the Cyber risk equation to really focus on is the Vulnerability, and assessing or assigning a coverage factor (or confidence factor, highly subjective) for how well common threats are being mitigated by a given system design and the owner/operators systemic capability to maintain the mitigation in sustained operation.

Both safety and security issues can cause potentially dangerous events within a plant. As a result, cybersecurity is covered in the recent edition of Functional Safety Standard IEC61508 (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. Similarly security requirements are specified in Clause 8.2.4 and 11.2.12 of IEC-61511 -1:2015.
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 but there is an important similarity; neither safety nor security is a one-time event. As indicated in IEC61508 and ISA 99/ IEC 62443, a common mistake is to address safety and cybersecurity as being similar to 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 cybersecurity, 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. The challenge though, 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.

As today's cyber threats become increasingly malicious with the focus now firmly on automation systems, the continued evolution of the threats suggests that we battle them with the combined force of both the IT cybersecurity approach and an engineering functional safety approach.

Functional safety and IT assessments

Functional safety assessments typically focus on the failure of a piece of equipment, addressing the probability of failure, the potential consequences, and the impact on safety, the environment, and the business.

IT assessments are very similar, but the consequences of a system being compromised would more likely be the massive economic impact of a production interruption, rather than loss of life.

Following corporate IT practices, tools have been created for use on process control engineering networks that scan the system for details such as asset identification, protocols in use, operating system status, version levels, patch levels, service pack installation, etc. If not applied with cybersecurity concerns in mind, however, these same tools, by the nature of the network design, might provide potential hackers with intelligence that was not previously accessible to them. For this reason a combination of skillsets or departments should be employed in all aspects of security from the field device to the corporate firewall that connects to the Internet.

One commonly suggested security solution is to isolate the ICS from the corporate and Internet systems through the use of firewalls. Unfortunately, while firewalls are widely used in the traditional IT sector, their effectiveness in ICS environments is still under development. IT firewalls are generally unaware of ICS protocols and may introduce unacceptable latency into time-critical systems that face operational constraints not typical in the IT world. To make matters worse, many end users are not knowledgeable exactly how these firewalls should be deployed in terms of architectures, configuration and management.

IT systems evolved with a tactical mentality in their approach to security, whereas process control has taken a more strategic approach. Only now are they becoming more tactical, making it essential that both IT and engineering skills and practices be combined in the assessment of today's plant risk.

Is human factor common in safety and security?

When new technology is introduced, it still has to be managed by people, so people have to understand that technology in terms of its capabilities and limitations to ensure the correct application; for that people require procedures and training.

If we look at the rise in recent attacks, the Stuxnet virus is probably the most well-known due to the surrounding publicity, in-depth reporting and the fact that it specifically targeted process automation systems. This threat was created outside the plant and designed to cause disruption to the routine running of a process or processes. The virus was designed with the specific knowledge of the protocols used on the process control network, enabling it to wreak havoc. It would be interesting to know if any pre-HAZOP or risk and threat assessment considered this type of attack when the systems were designed and implemented.

But Stuxnet wasn't just about technology; it also involved human weakness and error. One of the principal vectors for introduction of the virus was reportedly via a USB device that was left where employees would find it. Did the persons finding such a device consider the risk, impact, and consequence of using the device in the process control domain? Probably not.

So which department's safety, security, risk, and threat assessment should be responsible for addressing this type of threat? The answer should be both!

In retrospect it is easy to see that from an IT perspective, better management of the USB ports

would have helped. Had cybersecurity been considered during the functional safety assessment, then the consequences and impact might have been assessed and understood, driving the relevant risk reduction measures to be implemented. These could have included disabling USB ports, ensuring that policies and procedures are implemented, and training personnel on the risks of using rogue USB devices, and so on. It is worth noting that USB attack case for Stuxnet is just only one (but the simplest) viable route for seeding the attack but there were many other secondary attack vectors.

How should we measure security risk and carry out risk assessments?

Before acquiring ICS, cybersecurity requirements should be derived from cyber risk assessment. There are numerous definitions and equations for risk, and they change depending on the industry and the discipline. A common risk equation can be defined as:
Risk = threat × vulnerability × target attractiveness × consequence
The problem with this is it is difficult to assign actual numbers to the equation e.g. the probability of any risk scenario involving a terrorist attack is effectively unknown; and predicting isolated and rare events is generally accepted as virtually impossible to calculate. Threat and vulnerability (both very qualitative terms) are used to represent probability without specifying the mathematical formula. In addition, it would likely need to be recalculated on a regular basis due to external changes. For instance, Microsoft releases patches to their operating systems every month; these may directly affect the vulnerability of one or more control systems and hence drive the risk up. Asset owners have to decide if the increased risk is worth accepting, eliminating (by installing the patch), or mitigating by other means.

The Confidentiality, integrity and availability (CIA) triad is used widely within IT security circles, but the importance is often reversed in control systems as availability is usually far more important than protecting actual information. For critical safety and control system it would be totally different and priorities would be in the order of safety, integrity, availability and then confidentiality.

The increase in news channels around hacking critical infrastructure obviously also raised the target attractiveness index.

The final factor, consequences, needs to be very carefully considered. Disaster at the Deepwater Horizon drilling rig in the Gulf of Mexico in 2010 etc. showed how easy it is to underestimate the consequences of any incident. Apart from the human and environmental cost, the industry as a whole will likely be impacted by increased regulation.

Technology is not the main protector of an organization. There is an illusion that if as much technology as possible is bought that will guarantee safety but that is not a possible and effective solution.

Managing risk assessments correctly can often make the difference between suffering millions of dollars in damages and keeping assets safe. Referring to Figure 1, level-0 may include standalone TCP/IP devices, which require to be updated, causing an issue with process data going out to a L1 controller or PLC to control the process, but the TCP/IP devices being updated from level 3. Note, this is not supported in the ISA 99/IEC 62443 standards, proving there will always be exceptions in a network and so a risk analysis must be made.

As per ISA 99/IEC 62443 standards securing the process environment from the inside is about working with zones and conduits. By identifying the zones in the network infrastructure it is possible to keep data transfer within these zones or transfer limited data between zones via the conduits.
The cyber risk assessment study can be performed with the following approach and be seen as an iterative and continuous process:

- Define the risk analysis methodology
- Identify major items and their security impacts in term of availability, integrity, confidentiality and data loss.
- Identification - evaluation of the threat scenarios with their impact and likelihood.
- Reduce the risks by designing adequate countermeasures.
- Summarize the results in a risk register.

Relationship between Safety Integrity Levels (SIL) and Security levels (SL)

SIL - As per IEC-61511 - 1:
Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems.

SL- As per IEC 62443-1-1:
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.

1. **Safety examines** by assessment of whether the SIS meets the SIL requirement
2. **Security examines** the vulnerability of components that interfere with or disrupt the ICS operation. This again is a failure analysis, but the process of analysis is significantly different. The result requires improvement of security mitigation functions, but does not require an improved SIL.

The relationship between SIL and SL comes from the similarity of possible consequences but with completely different root causes.
The failure of a safety system could be severe, such as damage to equipment, the environment or even loss of life. A cyber-induced attack could do the same by either altering the database or disabling the safety system.

Some requirements for SLs are already covered in IEC-61508/61511.

How can we integrate practices and procedures for safety and security?

Just having IT and engineering groups in communication is not enough. Effective collaboration requires a close analysis of the practices and procedures for both departments to see if there are any contradictions. Synergy is good, but any contradictions could be a potential weakness in the system.

The time has come to combine the best of the IT world and the functional safety world. The next time that a HAZOP is performed, consider not just the process hazards, but also the IT hazards, consequences, and impact. ISA has life-cycle models for security and safety, defined in ISA99/IEC-62443 and ISA84, respectively. In the ISA99, a process is defined to assess the security of control systems (and IT systems) using a scale very similar to that used in the safety industry. Asset owners can start to look at the security of control systems today using another process taken from the safety industry — the HAZOP (hazards and operability analysis). This can be used as a basis for a Control hazards and operability analysis methodology (CHAZOP), which is being used by a number of enterprises in the control systems space. The time taken to fully complete a CHAZOP cannot be underestimated, especially on large interconnected systems.

Within the security world, the phrase “defense in depth [DID]” is used widely, and is a means to deploy numerous defensive mechanisms throughout the control systems to block (or at least delay) hackers trying to break into a system. The number and sophistication of these deterrents will decrease the likelihood of an attack succeeding. The principle of DID 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. DID is a term used to describe the full complimentary suite of controls for consideration in protecting systems and networks, such as [Refer Table-3 for DID]:

Policies & Procedures	Security policies, procedures, standards, training, business continuity and recovery plan
Physical Security	Locks, access control, guards
Perimeter Security	Firewalls, intrusion prevention system (IPS), internet access filtering, remote access controls, email filtering, denial of service mitigation, data loss prevention tools, Intrusion / leakage detection system(IDS), multi-factor authentication and authorization, access control lists (ACL)
Internal Network Security	Network segregation-zone and conduits, port management, ACL, device authentication, wireless network encryption, asset inventory management, vulnerability scanning tools, Internal firewalls, Network-based IDS

Host security	Authentication & privilege management, patch management, anti-virus and host intrusion prevention system, blacklisting, white listing, removable media restrictions, host based firewall, server hardening, access controls, continuous monitoring
Application defenses	Unique user and password required, secure coding practices, training, testing tools, penetration tests, code analysis tools, software inventory management, access control, authentication, secure software
Data Defenses	Access controls, encryption, crown jewel protection, data leakage protection(DLP),secure communication, access control, authentication

Table-3: Defense in Depth

Defense-in-depth strategy focuses on incremental but intelligent controls at each layer of the organization. The following are the most commonly known attack vectors for ICS, DID strategy is most effective in controlling them if applied systematically:

- Backdoors and holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices
- Database attacks
- Communications hijacking and man-in-the-middle attacks

To reduce systematic errors, standards IEC 61511-1 (Safety) and IEC 62443-3-3 (Security) require separate levels of protection and autonomy of the operating equipment and protective equipment. By design, an autonomous process control system and a safety system from different manufacturers require different engineering tools, databases, and operating procedures. Such systems from different manufacturers avoid common cause risks and reduce the security risk through diverse technology. In practice diverse technology also ensures a clear separation of the areas of responsibility and supports the different handling of operating equipment and protective devices.

Conclusion

ISA 99 / IEC 62443 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.

Benefits of Integration of safety and security are

- More safe and secured systems
- Systematic analysis of threats and hazards
- Identification of safety function where security is important
- Define common mitigations and requirements
- Harmonize safety and security contradictions

Although safety and security focus on different problems, causes and consequences, it is no longer possible to be truly safe without also being secure. The challenge however, 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.

References:

1. IEC, “Functional safety – safety instrumented systems for the process industry sector IEC 61511,
2. IEC ,”Functional Safety of electrical/ electronic/ programmable electronic safety-related systems IEC 61508,
3. DHS Cyber security Self Evaluation Tool (CSET)
4. National Institute of Science and Technology (NIST) Publication
5. ISA-99/IEC-62443-security for Industrial Automation and control systems
6. Wikipedia

Biography: Rahul Gupta was born in Ajmer (India) in year 1968.He graduated in Electronics & Communications engineering from University engineering college, Kota (Rajasthan).He worked in Instrumentation and Control department in Engineers India Ltd. New-Delhi between 1994 to 2005.At present he is Technical Authority (Automation and Control) at Wood Group Mustang Kuala Lumpur (Malaysia)-covering primarily Asia Pacific region. He is a certified Functional Safety Expert (TÜV Rheinland) and Industrial Automation and Control Systems Cyber Security specialist (ISA) for control and safety system. He has over 25 years of global working experience in the oil and gas industry. He provides consultancy advice in functional and process safety particularly on practical aspects for the implementation of functional safety and its management requirements as per IEC-61508/61511 for the whole safety instrumented system (SIS) life cycle on new projects, as well as for the installed base of SIS, Cyber Security Risk Assessment as per IEC 62443, Alarm Management, Reliability and Availability of Control and Safety Systems. He has participated and presented technical papers in several global conferences/ symposium.