Unraveling the Jargon Between Functional Safety & Cyber Security Related to Industrial Control Systems (ICS)

Safety & security alignment benefits for higher operational integrity

RAHUL GUPTA
TECHNICAL AUTHORITY- AUTOMATION CONTROL, ASIA-PACIFIC
 Topics

➢ ICS and relation to IT/OT
  • ICS
  • IT/OT
  • ICS combination of IT/OT
➢ Safety and Security related to ICS
➢ Risk assessments – Process hazard and IT
➢ Organization challenges
➢ Functional safety and Cyber security integration
➢ Summary-Benefits
What is an Industrial Control System (ICS)?

• A set of devices that directly control the manufacturing processes or operate technical installations
  • Sensors
  • Actuators
  • Logic solvers

• The term ICS covers:
  • DCS
  • IACS
  • PCS
  • SCADA
  • IED
  • RTU
  • PLC
  • ESD
  • PCD
  • SIS
Why does an ICS require security?

• Use of commercially available off-the-shelf (COTS) products

Ethernet / IP
TCP / IP
ICS & Operational Technology (OT)

• OT is an umbrella term used for various technologies that support “operations”

• For safe & reliable operations, OT consist of:
  - Hardware
  - ICS
  - SCADA
  - PLC
  - DCS

• OT is operation critical to sustain safe and stable production/manufacturing operation-REAL TIME CRITICAL

OT often found in Industries that manage Critical infrastructure:
- Water
- Oil & Gas
- Energy
- Utilities

Additionally found in:
- Automated manufacturing
- Pharmaceutical processing
- Defense networks etc.
IT vs. OT

Support
People

Storage systems
Computing technology
Business Applications
Data Analysis

Uses physics to manipulate data

Output

IT

Machinery
Equipment and assets
Monitoring systems
Control systems

Uses data to manipulate physics

OT

Refining (Oil & Gas)
Power (Electricity)
Telecom (Bandwidth)
Logistics (Packages)
Municipality (Water)

Support
People

Input

Typical Applications
Order management, Procurement, Payroll Interfaces
Graphic User Interface, Web Browser, Terminal and keyboard
Focus
Cost, Productivity, Compliance, Efficiencies
Characteristics
Workflow, Analysis, Long term data retention

Typical Applications
Process control, Maintenance, Outage management Interfaces
Sensor and actuators
Focus
Location, Condition, Events, Fault Detection, Alarms
Characteristics
Mission Critical (24*7), Reactive, Volume

Control
Machine
ICS: A Combination of IT & OT?

<table>
<thead>
<tr>
<th>Zone</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Zone</td>
<td>Level 5: Enterprise system</td>
</tr>
<tr>
<td>Business Zone</td>
<td>Level 4: Business Planning &amp; Logistics</td>
</tr>
<tr>
<td>DMZ</td>
<td>Level 3: Site Manufacturing Operations &amp; Control</td>
</tr>
<tr>
<td></td>
<td>Level 2: Area and Supervisory Control</td>
</tr>
<tr>
<td></td>
<td>Level 1: Safety Instrumented systems, Basic Control Devices</td>
</tr>
<tr>
<td></td>
<td>Level 0: Process I/O Devices</td>
</tr>
</tbody>
</table>

**Availibility**
- OT (%): 0
- IT (%): 100

**Standard Reference**
- Safety: IEC-61508/61511
- Security: IEC-62443
- Security: ISO-2700x

**Timeframe**
- Months, weeks, days
- Shifts, hours, minutes, seconds
- Hours, Minutes, Seconds, ms
- Milliseconds
- Milliseconds

© 2016 Singapore ICSS Cyber Security Summit | www.singaporeicsscybersec.sg
Security of ICS: Organization challenge IT or OT

• Historically no overlap between IT and OT
• IT and OT were developed to accomplish:

Processes and technology running on distinct infrastructure → Following separate standards → Managed by isolated organizational departments

- Distinct different missions
- With contrasting agendas
- Using dissimilar tools and priorities
Bridging the gap between IT and OT

Security

Challenge for embedded IT in ICS

Cyber Threat: Malicious digital attack

Availability

Reliability

Security – Missing?

Cyber Threat: Anything that negatively affects the system
Importance of safety and security integration when dealing with risk in an ICS

**ABNORMAL TEMPERATURE**
- Sensor failure
- Sensor calibration problem
- Intentional change – negligence
- Intentional change - unauthorized (hacker / virus)

**ABNORMAL HMI OPERATION**
Intentional change – Unauthorized (hacker / virus)
- Blank or frozen HMI
- Erroneous information display
- Command sent to intentionally cause malfunction

**ABNORMAL VALVE OPERATION**
- Valve failure
- Actuator failure
- Remote – Auto, Intentional change –negligence
- Remote – Auto Intentional change – unauthorized (hacker / virus)

SUMMARY of attacks:
- DATA Integrity
- Malware injection

- Malicious act at site
- Remotely
- Or via compromised workstation
Integration of IT & OT security for an ICS in oil & gas - status

• Cyber security is now a boardroom decision

• It’s a business strategy and not just an IT issue

No awareness or Interest in the issue

Aware but unsure how to proceed

Addressing security but limited

Misplaced confidence in IT perimeter defenses

Established robust and on-going security program
Safety and security integration

**SECURITY**
Protection against attack

**SAFETY**
Freedom from risk and harm

**SYSTEMS**
SIS / BPCS

**Attacks**
(Threats)

**Environment**
(Hazards)
What is “security”?

- Illegal or unwanted penetration
- Interference with normal operation
- Inappropriate access to confidential information regardless of consequence (result) or motivation – intentional or unintentional
What is “safety”?

• Focuses on the potential result of an occurrence that has been defined as a risk.
Safety and security

• Two key properties of an ICS

• Share identical goal: protecting the ICS from failures

• Safety aimed at protecting systems from accidental failures to avoid hazards

• Security focused on protecting systems from failures through intentional malicious attacks

ICS is only as Safe as it is Secure......
Interdependencies between safety and security

- When we assess security, indirectly we will be assessing safety
- Can’t be addressed like a project having a start and end date
- Ongoing process

<table>
<thead>
<tr>
<th>Conditional dependencies</th>
<th>Security is a condition for safety and vice versa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reinforcement</td>
<td>Safety and security countermeasures can strengthen each other</td>
</tr>
<tr>
<td>Rivalry</td>
<td>Safety and security countermeasures can weaken each other e.g. passwords</td>
</tr>
<tr>
<td>Independence</td>
<td>No interaction between safety and security</td>
</tr>
</tbody>
</table>
Safety and security integration:
Can we relate functional safety and cyber security?

• The ICS is a combination of IT and OT; however, both IT and OT are different, as is their related security.
Functional Safety

- Part of overall Safety
- Freedom from unacceptable risk
- Achieved through Safety Instrumented Systems (SIS)
  - Electric / Electronic / Programmable Electronic Safety Systems in accordance with IEC – 61508 / 61511
  - Examples:
    - Emergency shutdown system
    - Burner management system
    - Includes field devices not just the logic solver
Functional Safety Management

- ISA 84 5.2.1.2 “A safety management system shall be in place so as to ensure that where Safety Instrumented Systems are used, they have the ability to place and / or maintain the process in a safe state.”
Security-aware Safety / Secured Safety

• Per IEC - 61508: Where Hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, is reasonably foreseeable, a security threat analysis should be carried out.

• Per IEC – 61511-1:2015 – Refer security requirements

Integration of IT and OT

SAFETY
ISA 84 / IEC-61511/61508

SECURITY
ISA99/IEC-62443
Integration of practices and procedures for safety and security
Functional Safety and Cyber Security procedures

- **Functional Safety** assessments typically focus on the failure of a piece of equipment, addressing the probability of failure, the potential consequences, the impact on safety, the environment and the business / asset

- **IT Cyber Security** assessments are similar, but consequences of a system being compromised are more likely to be the economic impact of a production interruption, with a lesser focus on HSE
Functional Safety and Cyber Security procedures - continued

• IT practices and tools have now been created specifically targeted at the process control engineering network

• Beneficial, but provides potential hackers with intelligence that was previously not accessible

• Now more important than ever that the skill-sets of different departments should be applied across all aspects of ICS security – both IT and Engineering
Firewalls

• Combining IT and engineering skills and practices, allows common myths to be fully addressed
• Commonly proposed security solution is to isolate the ICS from corporate and internet systems using a FIREWALL
Firewalls

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Brings false sense of security, it is not a “SET &amp; FORGET” device</td>
<td>1. Combine IT and engineering skills and practices in the assessment of today’s plant risk</td>
</tr>
<tr>
<td>2. Effectiveness of IT firewalls in the ICS environment and protocols</td>
<td></td>
</tr>
<tr>
<td>3. Lack of documentation on firewall design, configuration and rules</td>
<td></td>
</tr>
<tr>
<td>4. May introduce latency into time critical systems creating operational constraints</td>
<td></td>
</tr>
</tbody>
</table>
IT and Engineering group communication

- Simple communication between IT and engineering groups is not sufficient
- Effective collaboration required to provide a close analysis of practices and procedures in each department to identify duplication, conflicts, etc.
- Interdepartmental synergy is good, but discrepancies could be a potential weakness in the system
New technology

• If its believed technology can solve all security problems, then its likely the problems, and the technology, are not fully understood.
Is the ‘Human Factor’ a common issue in safety and security?

• New technology must still be managed by people
• People must understand the technology, both in terms of its capabilities and its limitations, in order to be correctly applied
• To ensure the correct implementation - guidelines, procedures, and training of the people must be in place
• The misconception that additional technology is the main protector and guarantees safety, is misguided, ineffective, and potentially dangerous
## Human factor impact in security and safety

### SECURITY

1. **Stuxnet Virus**
   - Threat created outside the plant utilizing specific knowledge of protocols used in the ICS to cause disruption to the running process.
   - Infected USB flash drive was one of the attack vector.
   - It wasn’t just about technology, it also involved human weakness and error.

2. **Shamoon Virus**
   - Threat was created by a disgruntled insider who had full access to the system.

### SAFETY

- Control of human factors is key to achieving high reliability of processes.
- There are numerous human interactions with the SIS that are considered when performing SIL verification calculations.
- But there is a limit to the beneficial effect that can be credited with human involvement.
- Investigation of several industrial accidents identified HUMAN ERRORS as one of the cause.
Measurement of risks and risk assessments: process hazards

HAZOP
- **Identify causes, consequences, safeguards** and generate recommendations based on risk level.

Safety Integrity Level (SIL) Analysis
- **Risk Assessment**: SIL is determined by ranking the **probability of the cause** and the **severity of the consequence**
- **Credits for Layers of Protection**: identifies the safeguards that are not related to a safety system
- **Implementation**: SIL rating is used to determine the design and maintenance requirements of safety system elements
Measurement of risks and risk assessments: security / IT hazard

- Correct management of risks can often make the difference between suffering millions of dollars in damages and keeping assets safe.

- Preparation and understanding of the actual elements of security, and the associated risks, is key.

- People, culture, and location all play a big part.
Why and how to measure security risk and carry out risk assessments

• Typical Risks Analysis
  • TCP/IP device being updated from level-3 due to operational & functional requirements, this is not supported in IEC62443, this is an exception in the network and requires - Risk Analysis.

• Typical Risk equation:
  Risk = Threat (x) Vulnerability (x) Target attractiveness (x) Consequences

• Several factors should be considered in carrying out security risk assessments:
  • Knowledge and awareness of users
  • Appropriate organization structure
  • Security strategy aligned to organization structure
  • Effective policies / procedure in place
  • Audit and measurement programs
  • Security technology appropriate to the installation and the above
Combining IT and Functional Safety for operation integrity

ISA has life-cycle models for security and safety — defined in ISA99/IEC-62443 and ISA84

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 (BPCS) and protective equipment (SIS).
Common integrity issues to both Functional Safety & Cyber Security Assessments

CHAZOP-Control Systems HAZOP is a method to perform systemic Hazard Analysis on the system design, including consideration of cyber risks, human factors and potential systemic failures and weaknesses

<table>
<thead>
<tr>
<th>Description</th>
<th>Functional safety</th>
<th>Cyber Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment issues – moisture, sulfur, chlorides etc. leading to corrosion of control &amp; safety system components</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Incorrect power distribution to redundant devices</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Cooling or HVAC inadequate for heat load</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Preventing unauthorized items, use Access Security: Enabling and disabling read-write</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Most commonly known attack vectors for ICS

- Defense In Depth (DID) strategy is the most effective control if applied systematically
- All the attacks can’t be prevented by one type / level of security
- The weakest points in the system are the most likely targets
- Reliable method of securing an ICS –
  From bottom-up NOT top-down

- Backdoors and holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices
- Database attacks
- Communications hijacking and ‘Man-in-the-Middle’ attacks
## Security Level (SL) and Safety Integrity Level (SIL) relationship

<table>
<thead>
<tr>
<th>Safety</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIL - As per IEC - 61511</strong>: Discrete level, (one out of four), specifying the <strong>Safety Integrity requirements of Safety Instrumented Functions</strong></td>
<td><strong>SL - As per IEC 62443</strong>: Level corresponding to the required <strong>effectiveness of countermeasures and inherent security properties</strong> of devices and systems, for a zone or conduit, based on an assessment of risk for the zone or conduit</td>
</tr>
</tbody>
</table>

Safety examines whether the SIS meets the SIL requirement, based on four factors:

- Management of Functional Safety
- Calculated Probability of Failure on Demand (PFD)
- Hardware redundancy
- Software requirements.

Security examines by failure analysis the vulnerability of components to interference that will disrupt their operation.

---

### Diagram

- ISO/IEC 15408
  - Criteria for IT security
  - 7-level Evaluation Assurance Level (EAL)

- IEC 62443
  - Criteria for control and safety systems
  - 4-stage IT security requirement level is defined known as SL
Zone and conduits

TARGET OF EVALUATION:

SL requirement for zones and conduits in IEC 62443-3:

• Risk levels must be determined by the owner-operator organization to align with their tolerable risk criteria.

<table>
<thead>
<tr>
<th>FUNCTIONAL SAFETY</th>
<th>CYBER SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>EQUIPMENT UNDER CONTROL (EUC)</td>
<td>ZONES AND CONDUITS</td>
</tr>
</tbody>
</table>
SIL vs. SL: complementary relationship

- **Similarity of possible consequences**, but with completely different root causes
- **Failure of a safety system could be severe** (damage to equipment or the environment)
- Cyber-induced attack could do the same by either altering the database or disabling the safety system
- Safety functions defined according to the application – security foundational requirements are common
- Security levels are valid for a certain zone
- Safety function with the assigned SIL extends through the conduit
- Some requirements for SLs are already covered in IEC-61508/61511.
Review

There is no safety without security. If a security risk exists via interfaces or integration, the integrity of Functional Safety is in jeopardy.

Security is a key underpinning element of the system’s availability and integrity, which is related to PFD, if the system is not protected against unauthorized changes, malicious or otherwise, then the logic solver PFD is degraded to values above vendor-published Logic Solver PFD data.

Safety and Security deserve similar consideration as key drivers to manage and reduce adverse events. Avoiding impacts on Health, Safety, and the Environment while maintaining production and in compliance with local and global regulations.

Safety and Security focus on different problems, causes and consequences. It is no longer possible to be truly Safe without also being Secure.
Summary

Why integration?
• Functional Safety IEC-61508/61511
• Cyber Security IEC-62443
Summary

• As today’s cyber threats become increasingly malicious with the focus now firmly on automation systems, suggest that we battle them with the combined force of both the IT cyber security approach and an OT engineering Functional Safety approach.
Safety, Security and Productivity

Challenge:

• Not only address safety and security issues, but derive the most benefit from the interconnected systems by sharing information conducive to effective and efficient decision-making

• Fine line between safety, security and productivity
WGM Approach

• Industry knowledge and experience in **Functional Safety** in accordance with IEC - 61508 / IEC – 61511.

• **Design and configuration of Integrated ICS networks**, including primary ICS vendors and third party systems and networks.

• Industry knowledge and experience in **Cyber Security** in accordance with ISA99 / IEC - 62443.

• Extensive knowledge in **Automation and Control / Safety system engineering** allied to **Process hazard and risk assessment**.

• Utilizing **all aspects of Cyber Security International & National standards**, Laws and Regulations
  • ISO 2700X, ISO-3100X, ISO-17799, ISO-15408, NIST framework,

• Full-service capabilities, from **Front End Engineering Design to implementation** and commissioning.

• **Vendor independent approach**.

• Depth of **multi-discipline resources** available within the WGM organization.

• Structured approach to project management utilizing proven tools and systems for improved efficiencies and communication.
Where To Get More Information

• IEC-61511, ANSI/S84.00.01-2004 - Functional Safety: Safety Instrumented Systems for Process Industry
• IEC-61508, IEC-62443, ISO 15408, ISO-2700X
• NIST Framework
• DHS
• Wikipedia
• Presenter Contact Information: Rahul.Gupta@woodgroup.com
THANK YOU FOR YOUR ATTENTION
QUESTIONS TIME