Where Cyber Security and Process Safety Meet

Your host today:

Phanney Kim Brevard
Principal, Portfolio Marketing, Industry Business

Introducing today’s esteemed panel:

Larry O’Brien
Analyst, ARC Advisory Group

Farshad Hendi
Safety Services Practice Leader

Gary Williams
Sr. Director Technology Cyber Security & Communications

John Cusimano
Director, Industrial Cyber Security, aeSolutions

This presentation is available to View OnDemand:

You can also contact the panel here
Agenda

1. Process Safety & Cyber Security: Converging Requirements
2. Process Safety Overview
3. Cyber Security Overview
4. Process Safety & Cyber Security
5. Panel Discussion
Cyber Security and Process Safety: Converging Requirements

- Larry O’Brien  Analyst, ARC Advisory Group
Technology is changing the Industrial Control System (ICS) landscape

Technology Developments
- Mobility and ubiquitous connectivity
- Industrial Internet of Things (IIoT)
- Cloud computing

New Control System Architectures
- More dynamic, distributed architectures
- More integration with external systems
- More reliance on external services

New ICS Cyber Security Challenges
- Exponential increase in attack surface
- Increased likelihood of attacks
- Loss of direct control of security risk
Cyber Security implications of ICS changes

> Exponential increase in vulnerabilities and threat levels
  > More plant devices with software and communications capabilities
  > More custom, embedded operating systems and applications
  > More users and user devices accessing ICS components
  > Cloud and IIoT devices are higher value targets

> Exponential decrease in ability to control intrusions
  > More porous plant perimeters and more use of public internets
  > Sharing of cloud services and applications with other companies
  > More direct access to ICS and IIoT devices
  > More unmanaged, device to device communications

> Core challenging environment for cyber risk management
  > Limited control over cloud, IIoT, and public networks
  > Multiple risk perspectives of supporting systems and organizations
A future view of industrial systems – O&G

Suppliers & Service Providers

Enterprise Systems

Smart Consumer Devices

Cloud Services

Mobile Devices

Remote Intelligent Assets

Remote Operations

Plants, Factories

In-Plant Intelligent Assets

Ubiquitous Connectivity
The safety challenge

> There is a disturbing trend in the severity of plant incidents.

> Developing a safety culture.

> The need to modernize safety system infrastructure will result in sweeping changes across the process industries.
The IEC 61511/ISA 84 lifecycle

1. **Analysis**
   - Perform Hazard & Risk Analysis
   - Allocate Safety Functions to Protection Layers
   - Specify Requirements for Safety System
   - Design & Engineer Safety System
   - Design & Develop Other Means of Risk Reduction
   - Install Commission & Validate the Safety Protections

2. **Realization**
   - Operate and Maintain
   - Modify & Update
   - Perform Decommissioning of Safety System

3. **Maintenance**
   - Ongoing Functions

4. **Manage Functional Safety, Safety Assessment and Safety Audit**
   - Plan & Structure Safety Life-Cycle

5. **Verify Safety System**
Converging requirements of Process Safety and Cyber Security

Health, Safety, and Environment
“On August 5th, [2008] at the Baku-Tbilisi-Ceyhan pipeline at the Refahiye settlement of the Turkish province of Erzincan, there was a powerful explosion that caused a large fire at the pumping station. Thirty thousand barrels of oil were spilled. As a result of the explosion, the Baku-Tbilisi-Ceyhan pipeline was left inoperative for 20 days and the pumping was resumed only on August 25th. Pipeline shareholders suffered of five million USD losses per day. Azerbaijan lost almost one billion USD.”

Source: Georgian Journal, December 2014
Cyber Security IS a Process Safety issue

Stuxnet is typically introduced to the target environment by an infected USB flash drive. The virus then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC. In the absence of both criteria, Stuxnet becomes dormant inside the computer. If both the conditions are fulfilled, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.\textsuperscript{[7][8]}
Process Safety and Cyber Security are part of cyber physical systems and industry 4.0

> Cyber Physical System is a system featuring a tight combination of, and coordination between, the system’s computational and physical elements.

> CPS uses computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical system

> Convergence of computation, communication, and control

Security by design approach in process automation systems

“Goal 5: Secure-by-design. ICS products will be secure-by-design within 10 years. Chemical Sector owners and operators will insist, through specifications and orders, that vendors provide systems that are secure-by-design, and will work with vendors to achieve this goal.”

Roadmap to Secure Control Systems in the Chemical Sector
September, 2009
People, processes and technology
Standards exist, and applying them can prevent most failures and attacks.
ISA84 working groups

Working group 8 (WG8) addressing wireless technology for safety applications, which includes a partnership with ISA100 to address joint issues between wireless and functional safety.

Working group 9 (WG9) addressing security issues in SIS applications.

WG7, a joint effort with ISA99 to address overlapping security and functional safety related issues.

See more at: https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2012/june/cover-story-understanding-isa-84/#sthash.8SGeVN82.dpuf
What merged ISA84 and ISA99 lifecycles might look like

Source: Aligning Cyber-Physical System Safety and Security: Giedre Sabaliauskaite and Aditya P. Mathur
2

Process Safety Overview

- Farshad Hendi  Safety Services Practice Leader
On the night of December 2-3, 1984, a sudden release of about 30 metric tons of methyl isocyanate (MIC) occurred at the Union Carbide pesticide plant at Bhopal, India.

The accident led to the death of over 2,800 people (other estimates put the immediate death toll as high as 8000) living in the vicinity and caused respiratory damage and eye damage to over 20,000 others. At least 200,000 people fled Bhopal during the week after the accident. Estimates of the damage vary widely between $350 million to as high as $3 billion.
### Incidents that define Process Safety

<table>
<thead>
<tr>
<th>WHEN</th>
<th>WHERE</th>
<th>WHAT</th>
<th>FATALITIES</th>
<th>REGULATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1966</td>
<td>Feyzin, France</td>
<td>LPG Bleve</td>
<td>18</td>
<td>First LPG prescriptive regulations</td>
</tr>
<tr>
<td>1974</td>
<td>Flixborough, UK</td>
<td>Cyclohexane</td>
<td>28</td>
<td>EU Seveso I Directive 1982</td>
</tr>
<tr>
<td>1976</td>
<td>Seveso, Italy</td>
<td>Dioxin</td>
<td>1</td>
<td>US Chemical Emergency Preparedness Program 1985</td>
</tr>
<tr>
<td>1979</td>
<td>Bantry Bay, Ireland</td>
<td>Crude ship</td>
<td>50</td>
<td>US Emergency Planning and Community Right-to-Know Act 1986</td>
</tr>
<tr>
<td>1982</td>
<td>Ocean Ranger, Canada</td>
<td>Platform</td>
<td>84</td>
<td>US Chemical Accident Prevention Program 1986</td>
</tr>
<tr>
<td>1984</td>
<td>Mexico</td>
<td>LPG Bleve</td>
<td>600+</td>
<td>EU Seveso I Directive update 1987</td>
</tr>
<tr>
<td>1984</td>
<td>Bhopal, India</td>
<td>Methyl isocyanate</td>
<td>20000+</td>
<td>US Chemical Safety Audit Program 1986</td>
</tr>
<tr>
<td>1986</td>
<td>Challenger</td>
<td>Space shuttle</td>
<td>7</td>
<td>EU Seveso I Directive update 1987</td>
</tr>
<tr>
<td>1986</td>
<td>Chernobyl, USSR</td>
<td>Nuclear powerplant</td>
<td>100+</td>
<td>US Chemical Safety Audit Program 1986</td>
</tr>
<tr>
<td>1986</td>
<td>Sandoz, Bale, Switzerland</td>
<td>Warehouse</td>
<td>0</td>
<td>EU Seveso I Directive update 1987</td>
</tr>
<tr>
<td>1987</td>
<td>Texas City, USA</td>
<td>HF</td>
<td>0</td>
<td>US Clean Air Act Amendments 1990</td>
</tr>
<tr>
<td>1987</td>
<td>Grangemouth, UK</td>
<td>HCK HP/LP interface</td>
<td>1</td>
<td>UK HSE Offshore Installations (Safety Case) Regulations 1992</td>
</tr>
<tr>
<td>1989</td>
<td>Pasadena TX, USA</td>
<td>Ethylene/isobutane</td>
<td>23</td>
<td>EU Seveso II Directive 1996</td>
</tr>
<tr>
<td>1992</td>
<td>La Mède, France</td>
<td>Gasoline/LPG FCCU</td>
<td>6</td>
<td>UK Control of Major Accident Hazard Regulations 1999</td>
</tr>
<tr>
<td>1994</td>
<td>Milford Haven, UK</td>
<td>FCCU feedstock</td>
<td>0</td>
<td>EU Seveso II update 2002</td>
</tr>
<tr>
<td>1998</td>
<td>Longford, Australia</td>
<td>LPG, brittle fracture</td>
<td>2</td>
<td>UK HSE Offshore Installations (Safety Case) Regulations 2005</td>
</tr>
<tr>
<td>2001</td>
<td>Toulouse, France</td>
<td>Ammonium Nitrate</td>
<td>30</td>
<td>API RPs on occupied buildings and vents</td>
</tr>
<tr>
<td>2001</td>
<td>Petrobras</td>
<td>Platform</td>
<td>11</td>
<td>OSHA Refinery National Emphasis Program</td>
</tr>
<tr>
<td>2003</td>
<td>Columbia</td>
<td>Space shuttle</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>Skikda, Algeria</td>
<td>LNG</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>Texas City, US</td>
<td>Gasoline ISOM</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>Buncefield, UK</td>
<td>Gasoline</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>Bombay High, India</td>
<td>Platform</td>
<td>13</td>
<td></td>
</tr>
</tbody>
</table>

### REGULATIONS

- **EU Seveso I Directive 1982**
- **US Chemical Emergency Preparedness Program 1985**
- **US Emergency Planning and Community Right-to-Know Act 1986**
- **US Chemical Accident Prevention Program 1986**
- **US Chemical Safety Audit Program 1986**
- **EU Seveso I Directive update 1987**
- **US Clean Air Act Amendments 1990**
- **UK HSE Offshore Installations (Safety Case) Regulations 1992**
- **US EPA Risk Management Program 1996**
- **EU Seveso II Directive 1996**
- **UK Control of Major Accident Hazard Regulations 1999**
- **EU Seveso II update 2002**
- **UK HSE Offshore Installations (Safety Case) Regulations 2005**
- **API RPs on occupied buildings and vents**
- **OSHA Refinery National Emphasis Program**
Legislative, agency reactions

> EU Seveso I Directive 1982

> Clean Air Act of 1990 required OSHA and EPA to issue regulations

> OSHA 1910.119 is legislated and requires “designated” operations to comply with provisions of 14 element framework. Regulations first published in 1990, effective 1992

> Seveso II Directive 1996


> Seveso III directive 2012
Process Safety

> Freedom from unacceptable risk from:

> Fire

> Explosion

> Suffocation

> Poisoning

Operational Integrity

Process Safety
- People
- Processes
- Equipment/Systems

Functional Safety
- DCS
- SIS (Triconex)
- Alarms

Occupational Safety
- Trips
- Slips
- Falls
Process Safety management focus areas:

- Process Safety Leadership
- Risk Identification and assessment
- Risk Management
- Review and Improvement
Functional safety standard – IEC61511

- Analysis & Assess
  - Risk Analysis & Protection Layer Design
  - Allocation Of Safety Functions To Protection Layers
  - Safety Requirements Specification For The Safety Instrumented System
  - Design, Engineering & FAT Of The Safety Instrumented System
  - Installation, Commissioning & Validation
  - Design & Development of other methods of Risk Reduction

- Design & Implement
  - Management Of Functional Safety & Functional Safety Assessment
  - Safety Lifecycle Structure & Planning

- Operate & Maintain
  - Verification
  - Operations & Maintenance
  - Modification
  - Decommissioning
Layers of protection and risk management

Tolerable Risk Level

SV, etc. → SIS → BPCS

Inherent Process Risk

Mechanical integrity vessels, pipe, etc.

PROCESS

RISK
Cyber Security Overview

Gary Williams
Sr. Director Technology, Cyber Security & Communications
Cyber Security is now as important as safety

Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar Era

STUXNET designed to target Iran nuclear centrifuge

Dragonfly/Energetic Bear
Over 1000 European and US energy firms hit by Russian ‘Energetic Bear’ virus that let hackers take control of power plants
Cyber Security is now as important as safety

New Havex malware variants target industrial control system and SCADA variants

Spear fishing brings down German Steel Mill

A spear phishing attack led to a German steel mill to perform an unscheduled shut down and a blast furnace could not be shut down as normal. Attackers were very skilled and used both targeted emails and social engineering techniques to infiltrate the plant. The attackers showed familiarity with both IT security systems but also the specialized software used to oversee and administer the plant.
Industry response
Standards – Controls – Best Practices, Policies & Procedures

1. ISO27001/27002
2. ISA 99
3. ISASecure
4. ANSSI
5. WIB
6. IEC 62443

Gap Analysis; Risk & Threat Assessment; Vulnerability Assessment; Cause & Consequence; Due diligence; Audit
APPENDIX 2  ARCHITECTURE LEVELS IN ISA-99.00.01, PART 1


Figure 5 – DCS Example using the General Reference Model
Defense in depth - Security architecture

> Typical security architecture for Industrial Automation and Control Systems

> ISA99/WIB levels with Foxboro Evo specific level 1, 2 & level 3 layout
Enhanced solution architecture
4

Process Safety & Cyber Security

John Cusimano
Director, Industrial Cyber Security, aeSolutions
The challenge with modern Industry Control System (ICS)

- Modern control systems and safety systems are intelligent, programmable systems using digital communications.
- They are vulnerable to intentional or unintentional cyber attacks.
- It is common for control systems and safety systems to be integrated.
- A single vulnerability could disable multiple layers of protection!

PHA’s / HAZOP’s aren’t designed to analyze network and control system failures and typically treat the BPCS, alarms and SIS as independent layers of protection.
Layers of protection

- Disaster protection
- Collection basin
- Overpressure valve, rupture disc
- Safety system (automatic)
- Plant personnel intervenes
- Basic automation

Disaster protection
Passive protection
Active protection
Safety Instrumented System (SIS)
Process control system
Process alarm
Normal activity
Process value
Safety shutdown
Understanding risk is fundamental to determining how to best protect our systems

- We must first understand the risk
  - Identify the critical assets
  - Determine the realistic threats
  - Identify existing vulnerabilities
  - Understand the consequence of compromise
  - Assess effectiveness of current safeguards

- Develop a plan to address unacceptable risk
  - Recommend existing countermeasures
  - Recommend additional countermeasures
  - Recommend changes to current policies and procedures
  - Prioritize recommendations (based upon relative risk)
  - Evaluate cost / complexity versus effectiveness
Cyber Security regulations and standards require ICS/SCADA cyber risk assessments

- NIST Cybersecurity Framework
- NIST SP800-82 Guide to Industrial Control Systems (ICS) Security
- DHS Chemical Facility Anti-Terrorism Standards (CFATS)
- TSA Pipeline Security Guidelines
- NERC CIP Rev. 5
- ISA/IEC 62443, Industrial Automation and Control System (IACS) Security
- API Standard 1164 - SCADA Security
Cyber Security risk assessment deliverables

- Updated ICS/SCADA “security” architecture drawings
- Cyber security requirement specification
- Cyber vulnerability assessment
- Gap analysis with peer comparison
- Formal, documented analysis of cyber risk
- Zone and Conduit models
- Deployment strategy
- Updated ICS/SCADA cybersecurity policy and standards
How have you seen people address security over the past few years and what are some of the frustrations?
How do you even begin this path of cross collaboration between cybersecurity and process safety?
Final thoughts – what’s the one thing you want the audience to walk away with after hearing today’s discussion about security and safety?
Q & A
2015 Process Automation Global Client Conference

April 27 – May 1                   Dallas, TX

We see the promise of a bright industrial future. So will you.

Watch for more information coming soon
Thank you!
Where Cyber Security and Process Safety Meet

Your host today:

Phanney Kim Brevard
Principal, Portfolio Marketing, Industry Business

Introducing today’s esteemed panel:

Larry O’Brien
Analyst, ARC Advisory Group

Farshad Hendi
Safety Services Practice Leader

Gary Williams
Sr. Director Technology Cyber Security & Communications

John Cusimano
Director Industrial Cyber Security, aeSolutions

This presentation is available to View OnDemand:

You can also contact the panel here