if it isn’t
SECURE

it isn’t
SAFE™

Presented at SANS Oil & Gas Summit
Monday, Sept 16, 2019
Houston, TX
John Cusimano
Vice President of ICS Cybersecurity Solutions

20+ years Experience in Industrial Automation & SIS
(Kodak, Moore Products, Siemens)
10+ years Experience in ICS cybersecurity
(exida, ISA, aeSolutions)

Specialization in:
- Process Safety
- Safety Instrumented Systems (BMS, F&G)
- High-availability systems
- Industrial Networking
- ICS Cybersecurity
Agenda

1. Importance of Integrating Cybersecurity & Process Safety Management

2. Functional Safety and Industrial Cybersecurity Standards

3. Introduction to the Cyber PHA method to assess ICS/SIS Cyber Risk

4. Summary
Importance of Integrating Cybersecurity & Process Safety Management Efforts
So many BREACHES!
It’s not just about **IT** anymore … **Operations** is a target

More than half of major malware attack’s victims are industrial targets
Norsk Hydro ransomware incident losses reach $40 million after one week

Norsk Hydro up and running with the exception of one business unit where ‘operations remain almost at a standstill.’


$300M per quarter

The massive ransomware bill faced by Merck echoes the financial hits taken by other enterprises like Maersk and FedEx.
Triton (aka TriSIS) Malware

- Sophisticated malware targeting Triconex SIS
- Detected in Nov 2017 in the Middle East
- First reported cyber attack on a safety instrumented system (SIS)
- Two-stage attack
  - Compromise TriStation engineering workstation
  - Remote Access Trojan (RAT) on the SIS controller
- Discovered due to bug in the malware that caused the SIS to trip (failsafe)

Just because a SIS is SIL rated does not mean it is immune to cyber threats
On the surface it looks the same, but …

…underneath a lot has changed!

The evolution of automation technologies and the convergence of IT and OT
Process Safety & Industrial Cybersecurity

- **Disaster protection**
- **Passive protection**
- **Active protection**

**Prevent**
- Basic automation
- Plant personnel intervenes

**Mitigate**
- Collection basin
- Overpressure valve, rupture disc
- Safety system (automatic)

- **Safety shutdown**
  - Safety Instrumented System (SIS)

- **Process alarm**
  - Basic Process Control System (BPCS)

**Normal activity**

PREVENT MITIGATE
The Challenge

- Modern control systems and safety systems are complex
- It is very common for them to be integrated
- A single threat or vulnerability could disable multiple layers of protection
- Identifying the cyber threats and vulnerabilities that can lead to high risk consequences can be challenging
- Process safety studies (e.g. PHAs, HAZOPs, LOPAs) typically do not take into account cyber impacts on initiating event frequency or effectiveness of safeguards
Functional Safety and Industrial Cybersecurity Standards
Process Safety & Cybersecurity Standards

**Process Safety and Functional Safety Standards:**
- OSHA 29CFR1910.119
- EPA 40CFR68
- IEC 61508
- ISA 84 / IEC 61511

**Bridging Documents:**
- ISA TR 84.00.09
- IEC TR 63069
- NAMUR NA 163

**IT Cybersecurity Standards:**
- ISO/IEC 27000
- NIST 800 Series
- CIS Controls
- PCI DSS

**OT Cybersecurity Standards:**
- ISA/IEC 62443
- NERC CIP
- API 1164
- NIST 800-82

IEC 61511 added two clauses in 2016 edition regarding security of SIS
8.2.4: A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS

11.2.12: The design of the SIS shall be such that it provides the necessary resilience against the identified security risks

NOTE: Guidance related to SIS security is provided in ISA TR84.00.09 and ISA/IEC 62443-3-2.
Integrating Functional Safety with Cybersecurity

- Traditionally, different disciplines
- Yet process safety is dependent upon both
- Integration is critical
- Leverage maturity of safety risk analysis
- Integration at “Analyze” phase is key
ICS Cybersecurity Risk Assessments
Risk and Security Risk

Risk - “(exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility” – Oxford English Dictionary, 3rd ed.

Risk = Impact x Likelihood

“[Security] Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.” – NIST SP800-30

Security Risk = Impact x (Threats x Vulnerabilities)
THREATS

- Malware
- Infected USBs
- Contractors
- Infected Laptops
- Rogue Wireless
- Ransomware
- Human Error
- Disgruntled Employees
- Vendors
- Targeted Malware

IMPACTS

- Health & Safety
- Environment
- Equipment Damage
- Lost Production
- Offspec Product

VULNERABILITIES

- Outdated OSs
- Weak access controls
- Flat networks
- Software bugs
- Outdated antivirus
- No patching
- Poor backups
- Shared credentials
- Physical access
- Unsecured wireless
- SIS integration
- Fileshares (SMB v1)
- Unsecure protocols
- Embedded web servers
- AMS integration
- Serial / Ethernet
Introduction to the Cyber PHA method of assessing ICS/SIS cybersecurity risk
Cyber Process Hazard Analysis (PHA)

A safety-oriented methodology to conduct a security risk assessment for an ICS / SIS

- Systematic, consequence-driven approach
- Aligned with ISA/IEC 62443-3-2 and ISA TR84.00.09 standards
- Leverages established process safety information and techniques (e.g. PHA/HAZOP/LOPA)
- Integrates multiple engineering disciplines
- Delivers a risk-ranked mitigation plan (cyber or non-cyber)
The Cyber PHA Process

**Document System**
- Arch Diagram
- Inventory
- Dataflows

**Vulnerability Assessment**
- Networks
- Endpoints
- Physical
- Policies / Procedures
- Vulnerability register

**Partition System**
- Process Areas / Cells
- Zones & Conduits
- Catalog vulnerabilities by zone

**Risk Assessment Workshop**
- ID consequences (from PHA, etc.)
- ID threat scenarios (kill chain)
- Document safeguards / countermeasures
- Determine risk (risk matrix)

**Mitigation Planning**
- Develop mitigations (technical, procedural or mechanical)
- Risk Ranked and Prioritized

**Cyber Consequence Assessment**
- i.e. PHA/LOPA Review
Cyber PHA Toolset

Cyber PHA Worksheet

Risk Register

Risk Profile

Vulnerability Register

Threat Intelligence (e.g. Dragos WorldView)

Cyber Consequence Assessment (from PHA/HAZOP)

SME (IT, OT, Operations, HSE) Input

Cyber PHA database

© 2018 aeSolutions Inc.; version 1.0
Benefits of Cyber PHA Risk Assessment

- Provides management with risk-ranked mitigation plan
- Encourages collaboration, practical solutions and buy-in
- Satisfies new IEC 61511 SIS security requirements
- Uncovers “hidden” risks
- Establishes a baseline to measure progress and justify decisions
- Raises cybersecurity awareness
- Successfully applied to hundreds of ICS since 2013
Effective OT Cybersecurity Requires a Team

The Cyber PHA process is very effective at bringing these teams together.

CyberPHA
A proven method to assess industrial control system (ICS) cybersecurity risk

- Process Safety
- Industrial Automation
- Industrial IT
- Cybersecurity
John Cusimano, CFSE, GICSP, CISSP  
John.Cusimano@aesolns.com  
linkedin.com/in/john-cusimano-cfse-cissp-gicsp-2b78955  

For more information download our whitepaper:  
http://www.aesolns.com/download/2087/  

if it isn’t **SECURE** it isn’t **SAFE**™