Industrial Cybersecurity: A Culture Change

Reliable operational technology (OT) or industrial control systems (ICS) underpin every facet of American lives. Without them, our defenses, our economy, and our national security engine would grind to a halt — especially when so many of these systems are becoming "smart" and integrated. Securing infrastructure requires a culture change that prioritizes cybersecurity at the employee and organizational levels. OT is associated with information systems, devices, sensors, and equipment that are connected across a network (similar to information technology, or IT) but include the unique ability to interact with the physical world. Examples can include systems that support power generation and distribution, manufacturing, water treatment, chemical processing, oil and gas, weapons platforms, transportation and logistics, and building automation.

OT systems are often associated with critical infrastructure, and securing them requires a different approach than traditional IT systems. Today's industry is built upon yesterday's infrastructure, technology, and networks, and as a result, not all OT systems are identical, nor do they have the same security in design. Often, OT systems represent a mismatch of obsolete and legacy technologies with infrastructure built before the modern internet or even commonly used operating systems. OT systems are commonly integrated with newer systems that are subsequently retrofitted with the latest advancements. In addition, incorporating OT with other operational designs such as conditional alarms, hard-wired configurations, and process interlock strategies creates additional network differences. These operational characteristics will require different security configurations tailored specifically to each facility. Therefore, it's not applicable to develop an "off the shelf" or a business enterprise traditional IT solution as it will not fit the unique architectures for the majority of OT systems. Convergence of IT and OT will be the new reality. Modern control systems and technologies have evolved from simple analog sensors, such as a temperature sensor, to fully automated and integrated manufacturing facilities, safely running multiple simultaneous complex operations.

Typically, OT systems are architecturally designed to monitor their environment and automatically interact based on detected changes. Changes are discovered through remote sensors, reacting to predefined conditions, but also through data analysis and predictive algorithms. When compromised, the results can be personal injury (including loss of life), environmental contamination, or real damage of property. Consequently, there isn't a quick reboot to the common computer glitch. Operations must be sustained, and maintenance needs to be scheduled and coordinated in advance. Furthermore, OT systems cannot tolerate an interruption in dataflow, and some cybersecurity solutions are too intrusive or restrictive and can knock OT systems offline. As a result, the design focus places greater emphasis on availability over system confidentiality or data integrity. Since the potential consequences of conventional IT tools can hinder, cause failure, or even compromise an OT system, the accepted solution is to reduce the priority of cybersecurity or attempt to separate the systems. However, the important strategy is risk mitigation.

Addressing known vulnerabilities and improving the cybersecurity of critical systems or infrastructure — and therefore making these systems more adaptable, resilient and reliable — can help bolster key components of the nation's security in the energy sector. As the need continues for superior security and efficiently connected OT systems that have availability requirements as the priority, company leaders will need to better understand their environments and be able to predict technology interactions. In order to understand one or more technology interactions, security, efficiency and communication networks, while still managing limited resources, organizations are turning to advance risk mitigation strategies to accomplish their understanding.

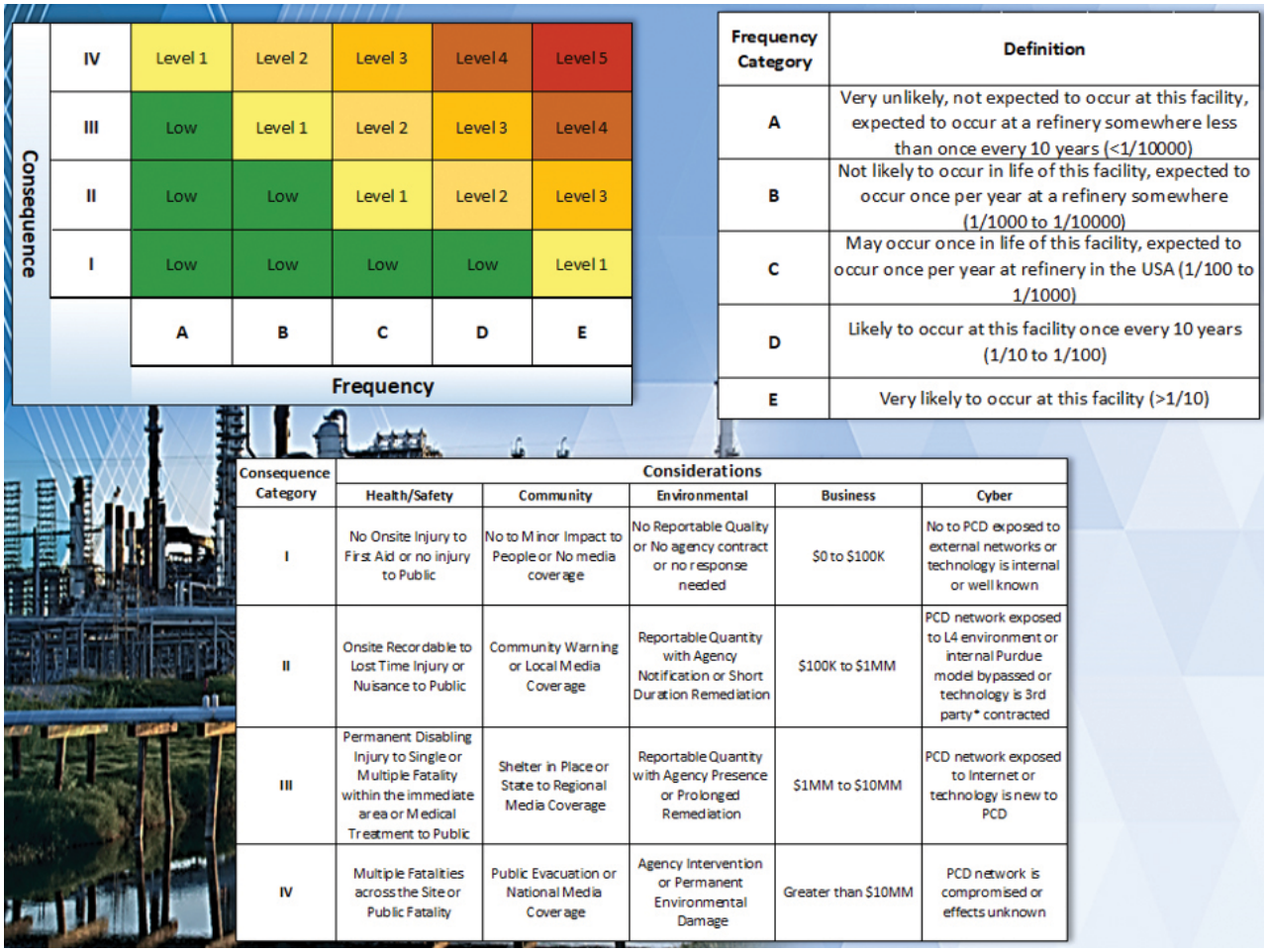
To be successful with cybersecurity implementations, corporate leadership must own and prioritize cybersecurity initiatives for the organization. Top level support is a must for all levels of management to implement the needed culture changes across all team members and staff. This necessary change is analogous to the safety culture changes and efficiency changes with Six Sigma that accelerated during the 90s through the turn of the century.

To achieve site wide adoption, organizations must adopt cybersecurity risk evaluations as a part of process hazard assessments (PHA/PSM) which will quantify the potential risk. By understanding and documenting the risk, organizations are better suited to set priorities, resources, and decisions for cybersecurity initiatives.

Traditionally, energy and process manufacturing industries leverage risk assessments that evaluate consequence versus frequency measured across key impact areas to include health/safety, community or social media, environment and business. However, moving forward in today's information and data age, cybersecurity needs to be included as part of the process control domain (PCD). An example of a risk matrix is captured in Figure 1.

After an organization can measure the risk, leadership will be better positioned to implement the necessary cybersecurity controls to either mitigate or transfer the associated risk. Key areas to consider during the development of the cybersecurity program should include:

- Cybersecurity policies and procedures
- Enhanced employee cybersecurity training
- Vendor relations and 3rd party risk management to include supply chains
- Internal cyber assessments
- Cyber and network security as a part of plant maintenance and plant shutdown schedules
- External media use
- Access management, both physical and virtual, to sensitive areas (Logic control cabinets and control rooms)
- Cyber implications with safety systems and process interlocks
- Company data (PII, HR, financial, legal, trade secrets)



Consequence	A	B	C	D	E
IV	Level 1	Level 2	Level 3	Level 4	Level 5
III	Low	Level 1	Level 2	Level 3	Level 4
II	Low	Low	Level 1	Level 2	Level 3
I	Low	Low	Low	Low	Level 1

Frequency

Frequency Category	Definition
A	Very unlikely, not expected to occur at this facility, expected to occur at a refinery somewhere less than once every 10 years (<1/10000)
B	Not likely to occur in life of this facility, expected to occur once per year at a refinery somewhere (1/1000 to 1/10000)
C	May occur once in life of this facility, expected to occur once per year at refinery in the USA (1/100 to 1/1000)
D	Likely to occur at this facility once every 10 years (1/10 to 1/100)
E	Very likely to occur at this facility (>1/10)

Consequence Category	Considerations				
	Health/Safety	Community	Environmental	Business	Cyber
I	No Onsite Injury to First Aid or no injury to Public	No to Minor Impact to People or No media coverage	No Reportable Quality or No agency contract or no response needed	$0 to $100K	No to PCD exposed to external networks or technology is internal or well known
II	Onsite Recordable to Lost Time Injury or Nuisance to Public	Community Warning or Local Media Coverage	Reportable Quantity with Agency Notification or Short Duration Remediation	$100K to $1MM	PCD network exposed to L4 environment or internal Purdue model bypassed or technology is 3rd party * contracted
III	Permanent Disabling Injury to Single or Multiple Fatality within the immediate area or Medical Treatment to Public	Shelter in Place or State to Regional Media Coverage	Reportable Quantity with Agency Presence or Prolonged Remediation	$1MM to $10MM	PCD network exposed to Internet or technology is new to PCD
IV	Multiple Fatalities across the Site or Public Fatality	Public Evacuation or National Media Coverage	Agency Intervention or Permanent Environmental Damage	Greater than $10MM	PCD network is compromised or effects unknown

Figure 1: Example risk assessment matrix

- Asset inventory
- Patch management and baseline configurations
- Personal devices
- Software, firmware, and hardware configurations,
- Response plans

To highlight a few areas of key importance, organizations must set the cybersecurity standards they will follow. For example, government agencies closely follow the standards of the National Institute of Standards and Technology (NIST); for OT, that standard would be NIST SP-800-82. Not all the recommendations may be required, as each organization's infrastructure is different, hence why risk assessments are extremely important. In addition to NIST, other standards include International Organization for Standardization (ISO/IEC), North American Electric Reliability Corporation (NERC-CIP), American National Standards institute or International Society for Automations (ANSI/ISA), and/or Center for Internet Security (CIS). These standards, along with the associated risk characteristics of an organization's infrastructure, will create the initial draft of policies and procedures. These initial, steps coupled with employee training, are key in creating a strong base for cybersecurity initiatives.

The threats of cybersecurity to OT/ICS environments have expanded drastically across all sectors of industry. Malicious actors have leveraged insider threats, ransomware, networking pivoting, policy violations, and compromising third party relations to gain a foot hold into OT and critical infrastructure networks. Examples include Stuxnet, TRISIS, Shamoon (1-3), and WannaCry. Specifically, in the oil and gas industry, several entities are gaining sophistication in their targeted attacks, including Xenotime, Magnallium, Dymalloy, Chrysene, Hexane, and nation-state or quasi-government actors.

The first step towards securing infrastructure is a culture change that all organizations and their employees need to adopt; that is, making cybersecurity a new priority. Cybersecurity threats are growing, and organizations must respond to protect its people, imagine, community, and the security of our nation.

Terry Horn, Director of Operation Technology, Associated Universities Inc. | Woodstar Labs Cybersecurity

Terry Horn joined AUI as a leader in cybersecurity operational technology. He focuses on business development, strategic technologies in industrial control systems (ICS), cybersecurity initiatives, and conducting hands-on assessments for clients and partners within the ICS and operational technology cybersecurity domain.

Related Publications/Contributions:

Author: There is More to Simulation Data, White Paper, Booz Allen, FEB-2016. | Fishing Through SCADA, White Paper, Booz Allen, MAR-2016. | Obtaining SCADA Simulation Data, White Paper, Booz Allen, MAR-2016. | Going Wireless within SCADA, White Paper, Booz Allen, APR-2016. | Manufacturing Control Systems, White Paper, Booz Allen, SEP-2016

Contributor: Cybersecurity Risk Steering Committee; Northeast Big Data Innovation Hub, NYU, Columbia University Control System Cybersecurity Association International