

9TH **CCPS**
LATIN AMERICAN
CONFERENCE
ON **PROCESS SAFETY**



OCTOBER 18-20, 2022
RIO DE JANEIRO, BRAZIL

aiche.org/lacps





Conducting Hybrid Security Risk Assessments to Address Physical Cybersecurity Exposures



Alyse Keller

AcuTech Group, Inc.

Vienna, Virginia, USA 22182

www.acutech-consulting.com



Alyse Keller | AcuTech Group, Inc.

- Process Safety Engineer at AcuTech Group, a U.S. risk management consulting firm
- Almost 10 years of experience in EHS in the Oil, Gas, and Chemicals industries
- Bachelor of Science in Petroleum Engineering, Colorado School of Mines
- Focus areas include hazard assessments, audits, regulatory compliance, industry advocacy, and training






INTRODUCTION

- Increased digitization of critical systems and industrial controls creates an increasing risk from cybersecurity events.
- These events can be caused by digital or physical attacks against OT assets.
- If physical or cyber security SRAs are not coordinated there could be unrealized risks.

The Unstoppable
Convergence Between
**Physical and
Cybersecurity**



**Technologies are integrating into our processes faster
than our organizations are adapting**



MISCONCEPTIONS

- There is a misconception that physical security and cybersecurity can be effectively evaluated separately.

• **Current Assessment:**

- Cybersecurity assessments are generally focused on protection from remote manipulation
- Physical Security Assessments may miss interfaces with OT/ AICS access

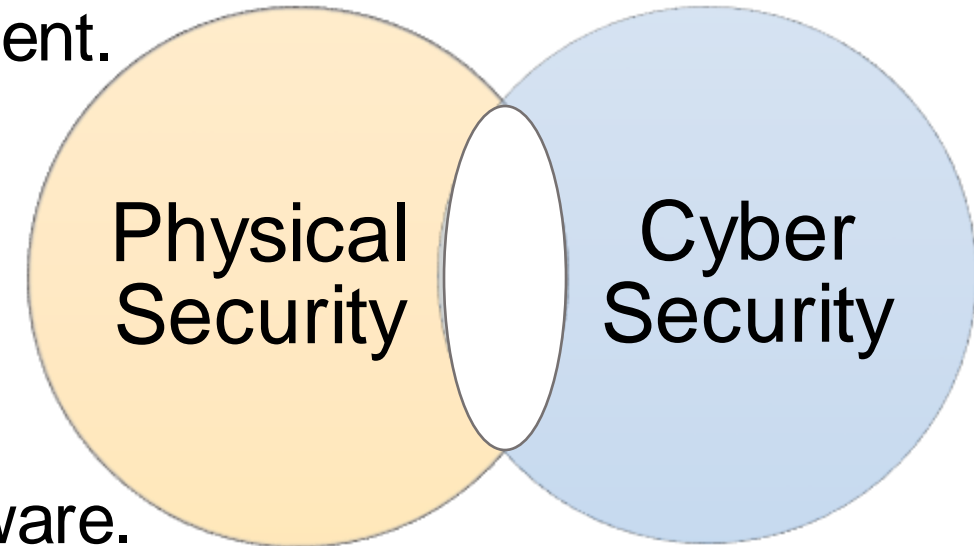
• **Issues:**

- Physical access to networks is often overlooked and may result in loss of AICS function or maloperation of a process.
- May exclude insider threats, colluded threats between insiders and external threats, and external threats



BACKGROUND

- Internationally recognized authorities and standards exist for cybersecurity and cybersecurity risk management.
 - ISA/IEC Standards
 - NIST Publications (800 Series)
 - ETSI Standards
- Best practices recognize the potential risk of physical manipulation of networked hardware.
 - Physical access to controls, or the process may be a more destructive means of attacking the infrastructure.





INSIDER THREAT

Insider threat - [CNSSI 4009, Adapted]

- The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, and the Nation.
- This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of organizational resources or capabilities.

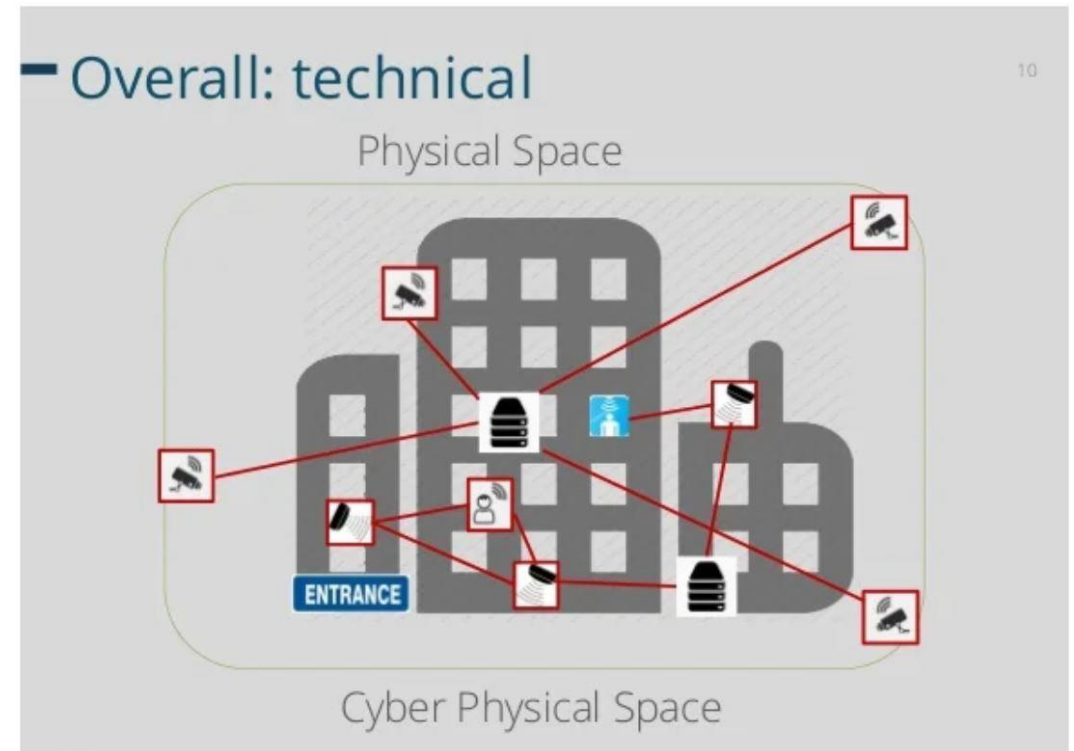
Industrial control system [SP 800-82]

- General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) found in the industrial sectors and critical infrastructures. An industrial control system consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).



MISSING CYBERSECURITY

- In the conduct of Security Risk Assessments (SRA), AcuTech notes that sites frequently do not evaluate physical access to cybersecurity nodes (i.e., physical access points).
- Cybersecurity standards and Cyber SRAs mostly identify means to prevent remote access and manipulation.





OBSERVATIONS

- AcuTech has identified a significant gap throughout industry involving the (mis)identification of physical cybersecurity exposures.
 - Physical cybersecurity attacks bypass digital controls to access systems and cause disruption, damage, or destruction.
 - Adversaries with physical access to a networked device or network node can expose control systems to compromise.
- Conventional physical/technical security personnel often fail to adequately assess or remediate risk exposure to cyber-assets.
 - These teams incorrectly assume that such exposures are fully mitigated by cybersecurity countermeasures.
- With few exceptions organizations tend to be extremely vulnerable to cyberattacks that involve a threat actor gaining direct access to the infrastructure.



REMOTE THREATS CONSIDERATION VS ONSITE THREATS

- Extensive resources are allocated for addressing remote threats.
 - Physical security addressing technical and administrative elements is often overlooked because organizations are focused on technology-oriented security countermeasures.
 - Insider access to this equipment, such as for maintenance of servers and networked equipment, is often conducted by contractors.
 - Potential threats and public incidents involving “trusted” insiders, contractors, vendors, and criminal are still overlooked.
 - This paradigm leads to inadequate security of systems and interfaces from exploitation.





RISK ASSESSMENT AND TREATMENT

- There is a strong business case to be made to go beyond physical and cyber SRAs and employ a hybrid SRA approach that incorporates the knowledge and expertise of both cyber and physical security experts.
- Providing cybersecurity input into the ANSI/API Standard 780 SRA methodology has proven to be effective in identifying and mitigating physical cybersecurity blind spots.



ANSI/API Standard 780

Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

FIRST EDITION | MAY 2013 | 113 PAGES | \$190.00 | PRODUCT NO. K78001

API Standard 780 methodology was developed for the petroleum and petrochemical industries, for a broad variety of both fixed and mobile applications. The standard describes the recommended approach for assessing security risk widely applicable to the types of facilities operated by the industry and the security issues the industry faces. The standard is intended for those responsible for conducting security risk assessments (SRAs) and managing security at these facilities. The method described in this standard is widely applicable to a full spectrum of security issues from theft to insider sabotage to terrorism.

The objective of conducting a SRA is to assess security risks as a means to assist management in understanding the risks facing the organization and in making better informed decisions on the adequacy of or need for additional countermeasures to address the threats, vulnerabilities, and potential consequences.

The API SRA methodology is a team-based, standardized approach that combines the multiple skills and knowledge of the various participants to provide a more complete SRA of the facility or operation. Depending on the type and size of the facility or scope of the study, the SRA team may include individuals with knowledge of physical and cyber security, facility and process design and operations, safety, logistics, emergency response, management, and other disciplines as necessary.

Ultimately, it is the responsibility of the user to choose the SRA methodology and depth of analysis that best meet the needs of the specific operation. Differences in geographic location, type of operations, experience and preferences of assessors, and on-site quantities of hazardous substances are but a few of the many factors to consider in determining the level of SRA that is required to undertake. This standard should also be considered in light of applicable laws and regulations.

For ordering information:

Online: www.api.org/pubs

Phone: 1-800-854-7179
(Toll-free in the U.S. and Canada)
(+1) 303-397-7056
(Local and International)

Fax: (+1) 303-397-2740

API members receive a 30% discount where applicable.



THREAT OVERVIEW / ASSESSMENT

- Threats can include:
 - Insider threats (Deliberate or Inadvertent)
 - External threats
 - Collusion: An act involving two or more employees, or an employee and an outsider that work together to bypass cybersecurity measures.



THREAT OVERVIEW / MODES OF ATTACK

Example modes of attack may include:

- Planting infected USB drives in public areas and waiting for employees to view them on company equipment.
- Using force, coercion, or subterfuge to install a rogue device.
- Physically accessing internet or data drop lines outside the facility that connect to the network.
- Person with only general access entering a restricted area to access cyber nodes.
- Directly attacking a CCTV, process control system, electrical or data highway.
- Using a drone (UAS) to access a network from a discreet location.
- Abusing the notion that if someone is accessing a cyber asset, they “*must* know what they are doing and be authorized”.



THREATS – INADVERTENT INSIDERS

- Insider threats are not limited to malicious or coerced individuals.
 - Well-meaning but untrained personnel can easily introduce unintended threats.
- The most famous incident that exploited inadvertent insiders is Stuxnet.
 - Infected USBs were distributed in areas that employees of the Natanz nuclear facility were considered likely to contact.
 - No single USB contained the entire virus.
 - Components bypassed security measures, allowing the virus to innocuously spread.
 - Once the components were all present in the target environment, a process logic controller, the virus assembled itself.
 - Once in place the virus allowed for remote manipulation/damage of sensitive equipment.



Image licensed under [CC BY](https://creativecommons.org/licenses/by/4.0/)



THREATS – INADVERTENT INSIDERS

- Countering USB Drop Attacks proves surprisingly difficult despite their infamy and prevalence.
 - One study conducted by a Google researcher found that **48%** of flash drives deliberately discarded in public were used (most within hours)
 - <https://elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots/>
- Methods for preventing USB-based threats can be:
 - Behavioral – Policies and ongoing education.
 - Hardware based – Physically sealing USB drives on devices.
 - Software based – Security software is capable of scanning USB devices to determine if they are verified and permitted devices.



Image licensed under [CC BY](https://creativecommons.org/licenses/by/4.0/)



THREATS – INADVERTENT ACCESS OR COLLUSION

- Providing inadvertent or deliberate access to specialized OT assets:
 - Server rooms, control rooms, field cabinets, and other hubs are often secured, but are not always understood.
 - If someone is working the server room, who is responsible for checking their credentials?
 - Who is competent / responsible for checking their work?
 - Exceptions for support staff in critical areas is never allowed but is frequently tolerated.
 - This presents a different threat in server rooms compared with manned control rooms.



Spot the sabotage above



THREATS – INADVERTENT INSIDERS

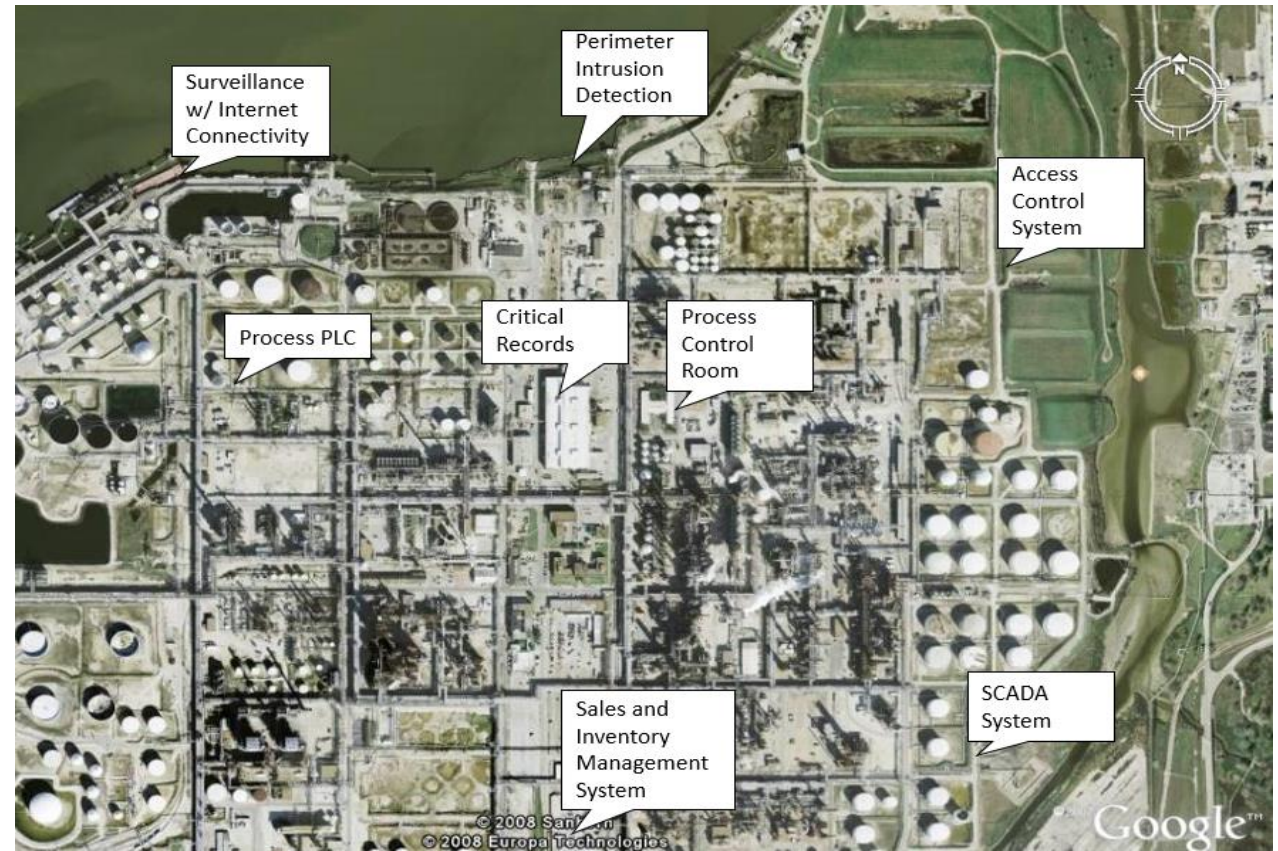
- Providing inadvertent or deliberate access to seemingly innocuous cyber assets:
 - Field cabinets, internet hardware, and ancillary equipment that may only connect to the internet occasionally, present a challenge
 - There is no comprehensive guidance identifying all of these connected devices, and their utility and vulnerability changes over time.
- Despite uncertainty, staff need to be informed that connected devices are critical and need to remain adequately secured.





DEVELOPING CORRECTIVE ACTIONS / COUNTERMEASURES

- Identify the location of critical cyber assets in the SRA.
 - Include physical access points to networked devices.
- Assess scenarios wherein an adversary gains physical access.



DEVELOPING CORRECTIVE ACTIONS / COUNTERMEASURES

- Develop countermeasures using a consistent methodology with your security program (e.g., an SRA).
 - Make physical security an integral part of your cybersecurity.
- Cybersecurity Risk Assessments may detail relevant consequences **but** are designed for ‘traditional’ cyber threats that are considered ‘present’ if your asset is online

Security Risk Assessment	Cybersecurity Risk Assessment
Previous SRAs may or may not include detailed information on cybersecurity assets and related consequences.	Contains information on cybersecurity assets, and the consequences of their manipulation.
Evaluates <u>Threats</u> and <u>Likelihood</u> to put the asset in context.	May or may not closely evaluate <u>Likelihood</u> , depending on the method.
Evaluates the security of the <u>Asset</u> itself, and the credible <u>Pathways</u> an adversary would need to use to reach it.	Focuses on the system and its endpoints, not the means of reaching them. Requires a separate survey of <u>Pathways</u> .



DEVELOPING CORRECTIVE ACTIONS / COUNTERMEASURES



- Cybersecurity measures are often technological or behavioral.
- When physically securing cyber assets, align measures with your site security.
 - Employee awareness
 - Access control
 - Monitoring and surveillance
 - Training
 - Policies
 - Barriers, etc.



CONCLUSIONS

Organizations with converged cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats.

The need for
a converged
security solution





CONCLUSIONS



Respective **physical and cyber personnel must coordinate** their efforts to counter potential threats at the physical interfaces, ensuring that measures applied to critical assets are **effectively integrated** with security systems and align with operational requirements.



CONCLUSIONS

Conducting the converged SRA is critical to providing insight into the physical cybersecurity interfaces and identifying and mitigating the vulnerabilities.



You cannot adequately “protect” what you do not understand.



ADDITIONAL RESOURCES

- Security Risk Assessment
 - ANSI/API Standard 780
- ISO Standards
 - 27000/27001 Series of Standards including Information Technology/Security
- ISA/IEC 62443 Series Standards
 - Cybersecurity of industrial automation and control systems
- NIST Special Publications (800 Series)
 - Special publications on Computer Security
- ETSI Standards
 - TR 103 Series and others on cybersecurity and hardware



Questions?

AcuTech Group, Inc.

Vienna, Virginia, USA 22182

www.acutech-consulting.com

akeller@acutech-consulting.com