Championing Cultural Change & Control Systems Cyber Security

Aleksandra Scalco, M.ENG., M.B.A., C.S.E.P., Ph.D. Student

Colorado State University (CSU)

Wasatch Aerospace & Systems Engineering Conference

Topics

Introduction

Cyber security

Control Systems

Adverse cyber security conditions

Oldsmar water-treatment facility in Florida (“hack”)

Aerospace threat conditions (manufacturing, infrastructure, modernization)

Professional cultural change

Forecasting indicators

Commercial demand signal

Emerging policy

Workforce enhancement

Conclusion

Introduction

- Someone tried to poison the water supply (Ref. [1])
  - Oldsmar water-treatment facility hack attempt in February 2021
  - Attempt to poison town by release of sodium hydroxide by a factor of 100 into water supply
  - Remote-access system
  - Outdated, end-of-life Operating System (OS)
  - Facility supervisor saw the hacker's pointer move across the screen in attempt to make unauthorized changes to settings
  - Hack averted

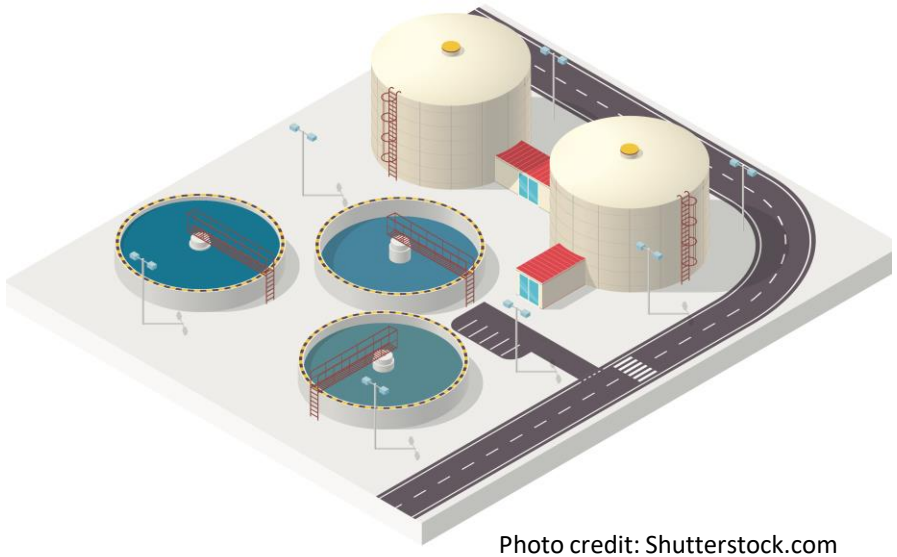


Photo credit: Shutterstock.com

[1] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

Adverse Cyber Security Conditions

- Control physical world processes
- Lifecycle of 30+ years
- Near-real time
- Purpose built
- Zero downtime
- Safety

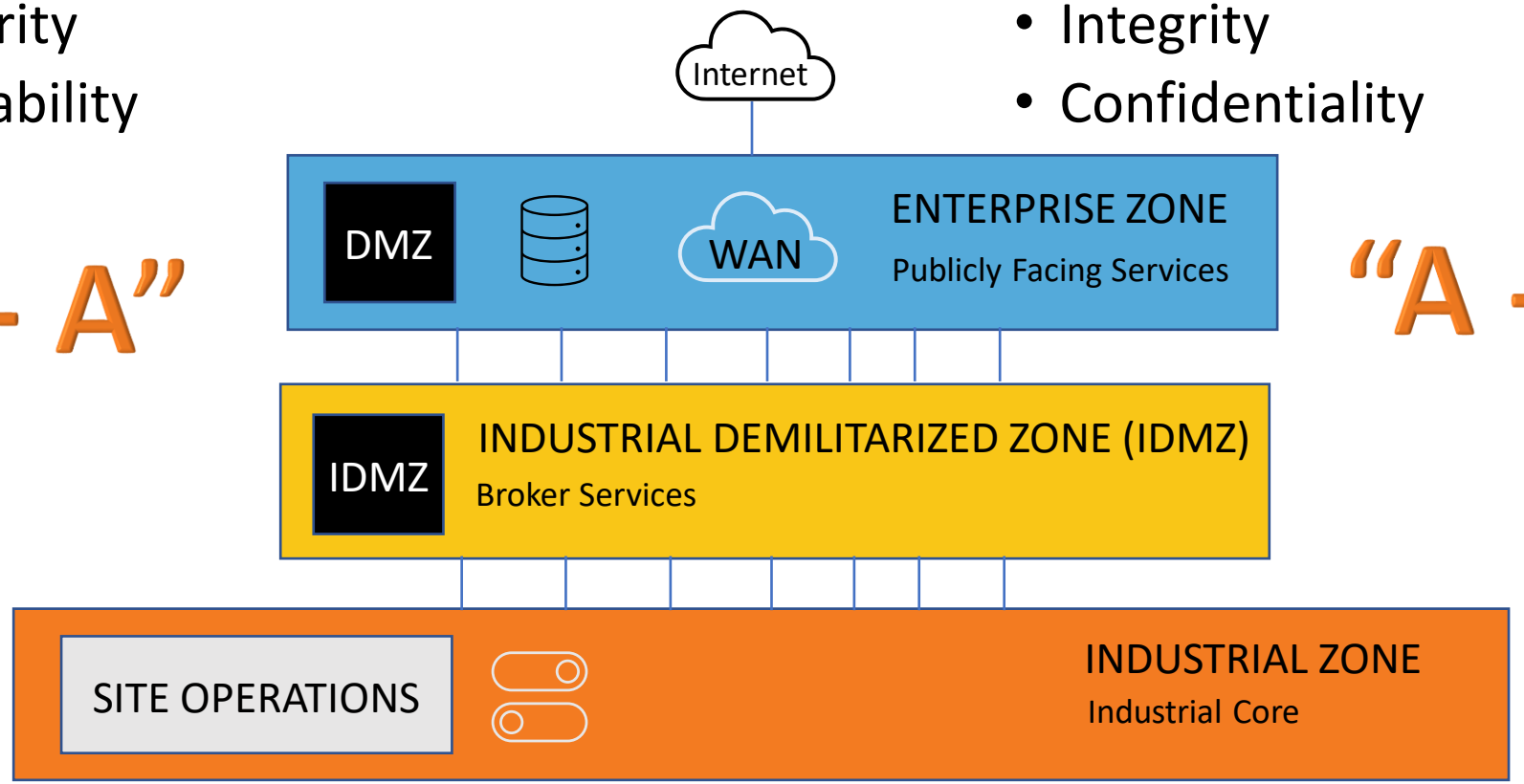
Photo credit: Shutterstock.com

Professional Cultural Change

- Information Technology (IT)
  - Confidentiality
  - Integrity
  - Availability

- Operational Technology (OT)
  - Availability
  - Integrity
  - Confidentiality

"C - I - A"



"A - I - C"

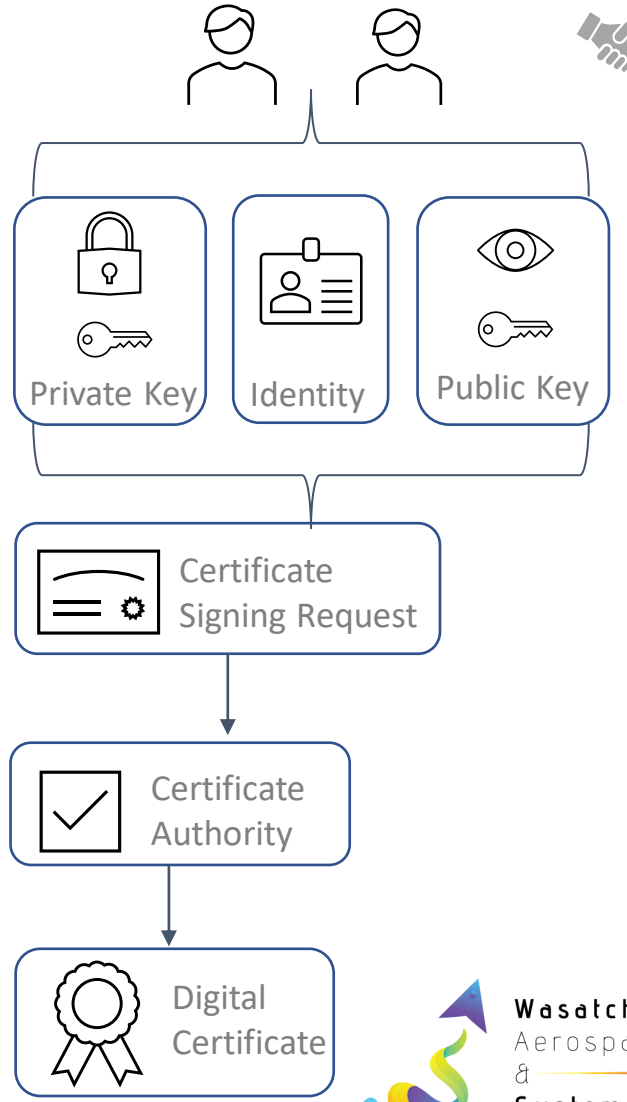
Adverse Cyber Security Condition Mitigations (Ref. [2])

- Use multiple-factor authentication.
- Use strong passwords to protect Remote Desktop Protocol (RDP) credentials.
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured and secure.
- Audit network configurations and isolate computer systems that cannot be updated.
- Audit networks for systems using RDP, closing unused RDP ports, applying multiple-factor authentication wherever possible, and logging RDP login attempts.
- Audit logs for all remote connection protocols.
- Train users to identify and report attempts at social engineering.
- Identify and suspend access of users exhibiting unusual activity.

[2] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

Certificate Management

- Digital certificates identify and control who can access and operate a facility network
- Both people and devices are identified and authenticated
  - Wireless access points (WAP) access restriction to external devices
  - WAP access restriction to who can access devices
- Every person and device has a certificate
- Every connection is identifiable



Where to Find Free Cybersecurity for ICS Training

- CISA offers free training https://ics-training.inl.gov/learn (Ref. [3])
- 1 - 2 hours per course E-Learning 22+ courses & instructor-led available
- Example course: “Differences in Deployments of Industrial Control Systems”
  - Define ICS.
  - Recognize the importance of cybersecurity in ICS.
  - Describe critical infrastructure sectors and their importance.
  - Recognize the types of facilities that support critical infrastructure.
  - Identify different types of industrial processes and dependencies

[3] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

Credentialing of ICS Security Professionals

- Global Information Assurance Certification (GIAC)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Industrial Control System Information Sharing and Analysis Center (ICS-ISAC)
- International Society of Automation (ISA)
- National Institute of Standard and Technology (NIST)
- SANS Institute
- Others

Additional Credentialing

- International Information Systems Security Certification Consortium, Inc. $(ICS)^2$
  - Certified Information Systems Security Professional (CISSP)
  - Information Systems Security Engineering Professional (CISSP-ISSEP)
  - Information Systems Security Architecture Professional (CISSP-ISSAP)
- International Council of Electronic Commerce Consultants (EC-Council)
  - Certified Chief Information Security Officer (CCISO)
- ISACA
  - Certified Information Security Manager (CISM)
- Computing Technology Industry Association (CompTIA)
  - Advanced Security Practitioner (CASP+)

Forecasting Indicators

- Commercial demand signal
- Emerging policy (Ref. [4])
  - HR 1833 “Department of Homeland Security (DHS) Industrial Control Systems Capabilities Enhancement Act” introduced in March 2021
  - Would give greater authority to the Cybersecurity and Infrastructure Security Agency (CISA) to defend critical systems against cyber attack

Photo credit: Shutterstock.com

- Aerospace conditions
  - Aircraft manufacturing
  - Airport Infrastructure modernization
  - Air Traffic modernization

[4] U.S. House, House Resolution 1833 (H.R. 1833) "DHS Industrial Control Systems Capabilities Enhancement Act of 2021," 2021. URL: https://www.congress.gov/bill/115th-congress/house-bill/5733 [retrieved March 2021].

Workforce Enhancement

Photo credit: Shutterstock.com

- Colorado State University (CSU) (Ref. [5])
  - Cyber-physical System (CPS)/Control System (CS) Workforce Study
  - 203 questions to better understand workforce
- AIAA Cyber Security Market Study (Ref. [6])
  - Strong Demand to increase cyber security awareness
  - Cyber security inclusion in supply chain management, development, engineering, and production processes
  - Cyber security curriculum needed for students and professionals

[5] Simske, S., and Scalco, A., “Cyber Physical System (CPS)/Control System (CS) Workforce Questionnaire,” Colorado State University (CSU) Institutional Review Board (IRB), August 2021.
[6] American Institute of Aeronautics and Astronautics (AIAA), "The Connectivity Challenge: Protecting Critical Assets in a Networked World: A Framework for Aviation Cybersecurity," AIAA, Decision Paper, August 2013

Conclusion

- SYSE are useful for forecasting indicators and championing cultural change
- Safe and secure cyber systems require regular updates and improvements
- Technology-based solutions alone will not “fix” challenges
- Cyber threats and cybersecurity solutions will change and challenge organizations
- Workforce cultural changes are required:
  - Credentialing CISA free training is available at https://ics-training.inl.gov/learn (Ref. [7])
  - Designing and engineering systems
  - Handling or processing information, using networks, or interacting with cyber-connected systems by personnel
  - Changing degree, experience, and work-based learning requirements
- Looking for a new generation of systems and cybersecurity thinkers

[7] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021.

Thank you.

References

[1] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[2] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[3] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[4] U.S. House, House Resolution 1833 (H.R. 1833) "DHS Industrial Control Systems Capabilities Enhancement Act of 2021," 2021. URL: https://www.congress.gov/bill/115th-congress/house-bill/5733 [retrieved March 2021].

[5] Simske, S., and Scalco, A., “Cyber Physical System (CPS)/Control System (CS) Workforce Questionnaire,” Colorado State University (CSU) Institutional Review Board (IRB), Protocol Number 20-10209H, August 2021.

[6] American Institute of Aeronautics and Astronautics (AIAA), "The Connectivity Challenge: Protecting Critical Assets in a Networked World: A Framework for Aviation Cybersecurity," AIAA, Decision Paper, August 2013. URL: https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/aiaa-cyber-framework-final.pdf?sfvrsn=7bd09ec9_0 [retrieved March 2021].

[7] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

Thank you.

Wasatch Aerospace & Systems Engineering CONFERENCE