The Case for Control Systems Cybersecurity Capability

Aleksandra Scalco, Ph.D. (c), M.ENG., M.B.A.
aleksandra.scalco@incose.net

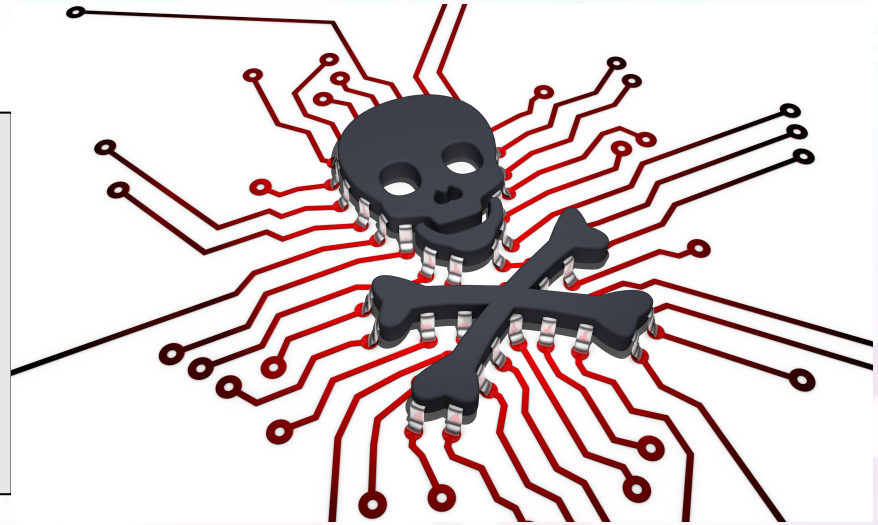
October 20, 2021

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Case for Control System Cybersecurity

- Risks to Control Systems are rapidly expanding
- ***What is the cost of <u>not</u> investing in Cyber Security?***
- Cyber attacks can have significant physical, socio-economic and other consequential impacts

The average cost of a data breach in 2020 is $3.86M -- An attack on critical infrastructure could have far greater significant consequences that far exceed the monetary costs -- negatively impacting operations and ability to carry out mission.

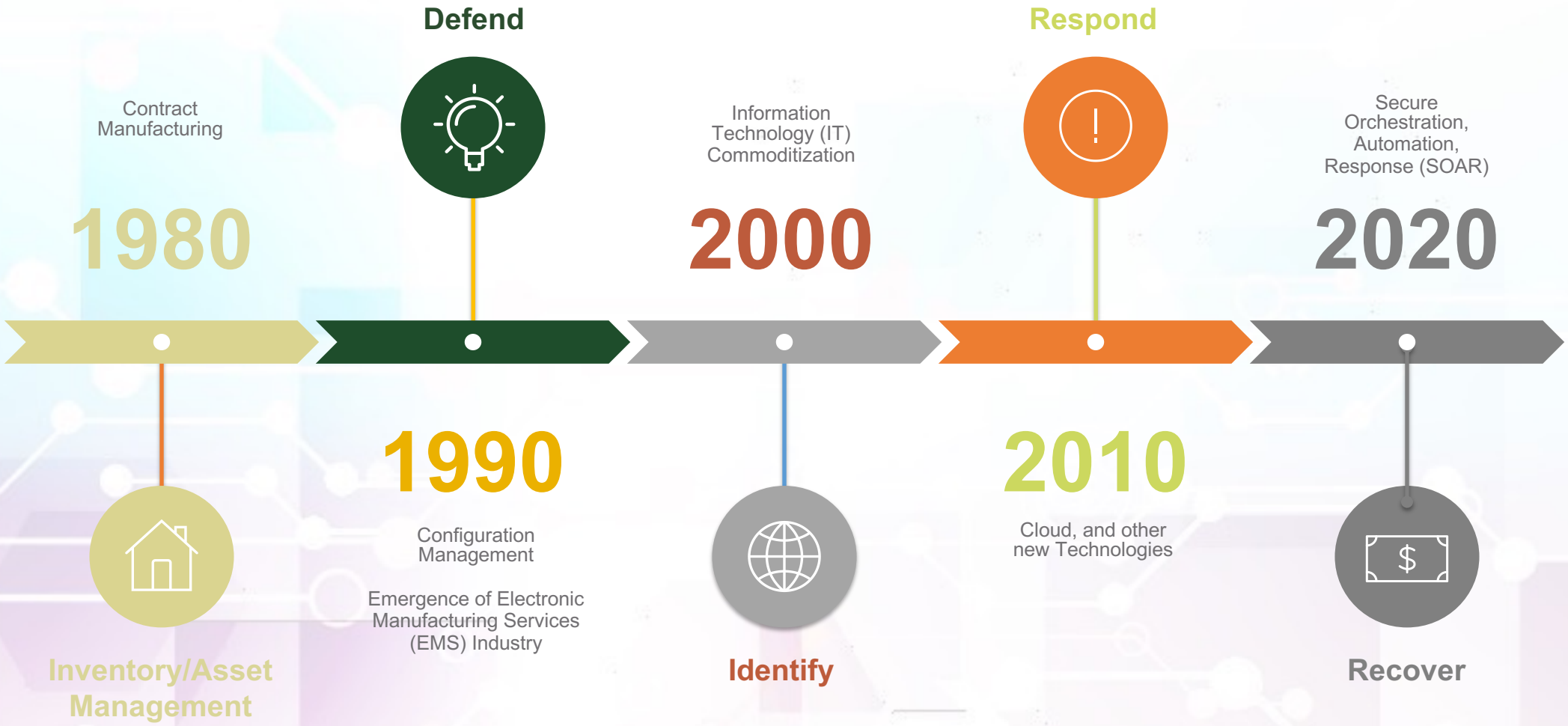


Reference: Ponemon Institute, 2020 Global PKI Trends Study, 2020

Images: Shutterstock, Shutterstock.com, 2021.

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

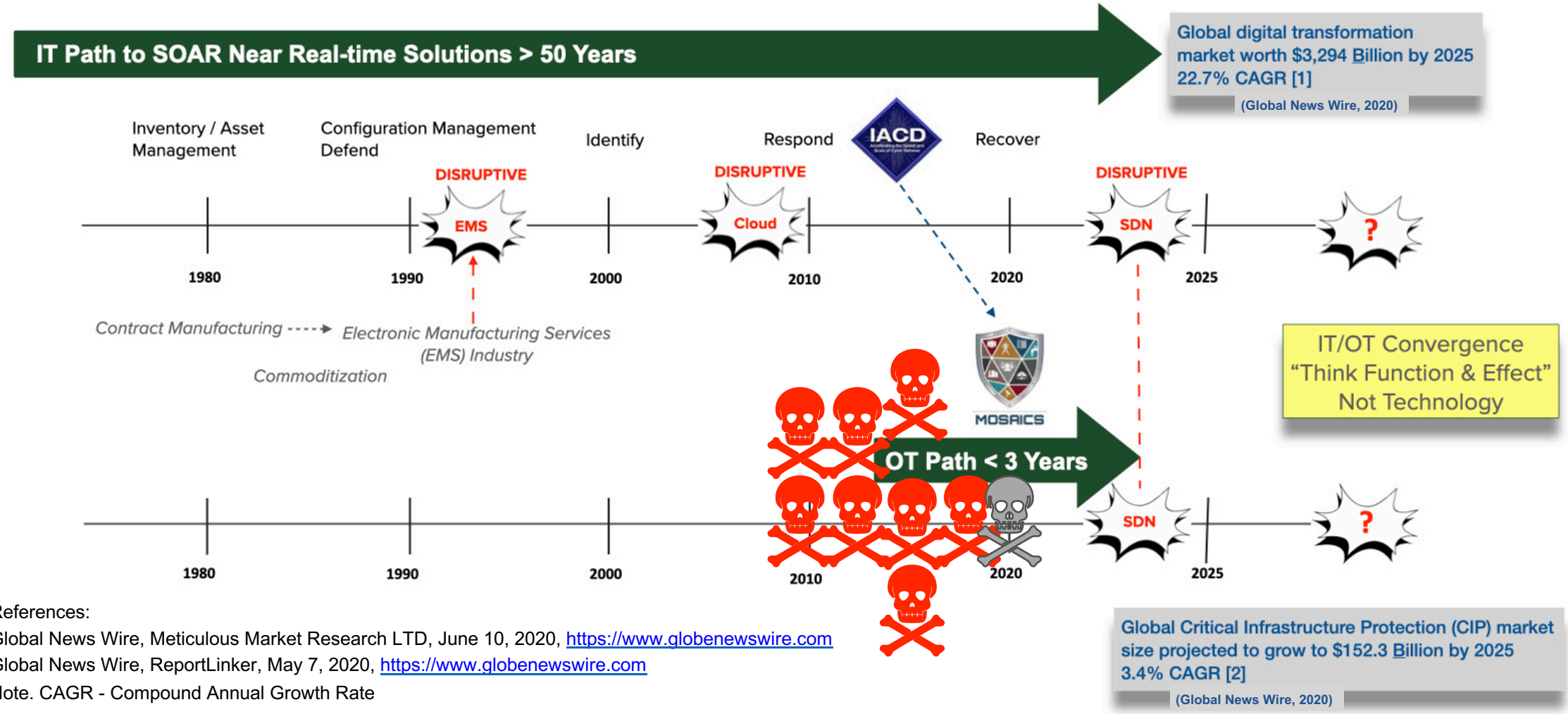
Path to Near Real-time Solutions



Reference: Aleksandra Scalco, "Cyber-physical Systems/Control System (CPS/CS) Workforce," INCOSE International Workshop 2021 (IW2021), January 2021

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Control System Path to Near Real-time



References:

Global News Wire, Meticulous Market Research LTD, June 10, 2020, https://www.globenewswire.com
Global News Wire, ReportLinker, May 7, 2020, https://www.globenewswire.com

Note. CAGR - Compound Annual Growth Rate

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Cyber Attacks on Critical Infrastructure

- Oldsmar water-treatment facility hack attempt in February 2021 (DHS, 2021)
- Attempt to poison town (pop. 15,000) by release of sodium hydroxide (“lye”) chemical by a factor of 100 into water supply
- Remote-access system used as entry point
- Attacked a vulnerable, outdated, end-of-life (EOL) Operating System (OS)
- Facility supervisor saw the hacker’s pointer move across the screen to make unauthorized changes to settings
- Hack averted

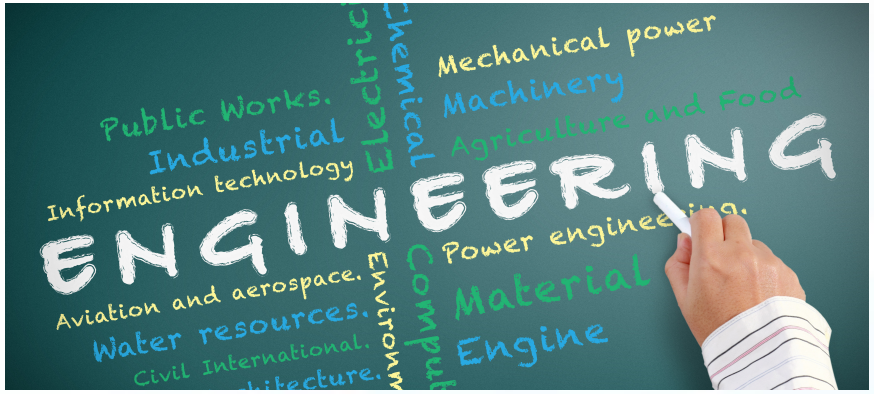


Image 11. https://shutterstock.com

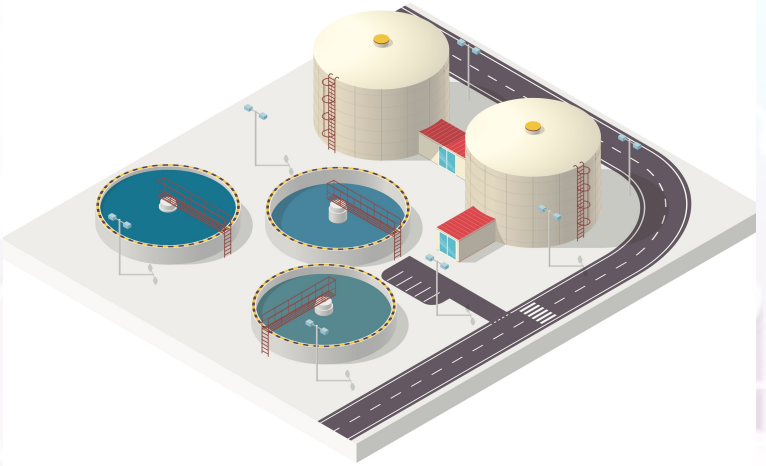


Image 12. https://shutterstock.com

- 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].

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

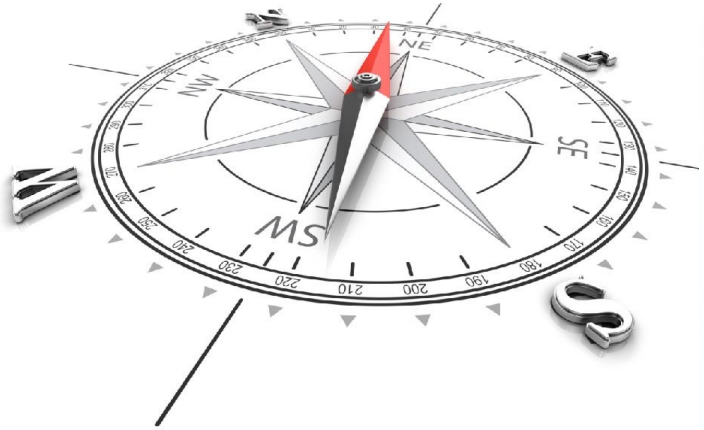
Impacts of ***No*** Control System Cybersecurity

- **Mission.** Loss of command and control of mission functions.
- **Physical.** Personnel injury or loss of life, loss of assets, environmental damage.
- **Economic.** Unavailability of critical infrastructure (i.e., electrical power, fuel, water, etc.) beyond the systems sustaining direct and physical damage.
- **Social.** Potential loss of public confidence.

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Images: Shutterstock, Shutterstock.com, 2021.

System Variables



Context-sensitive, Dynamic Classes

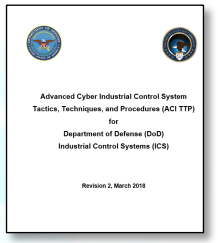
- View of the system designer/operator
- Critical infrastructure sector
- System layer in reference architecture
- System governance
- System mission
- Set of classes dynamically classified at the time of operation rather than as a static set of classes

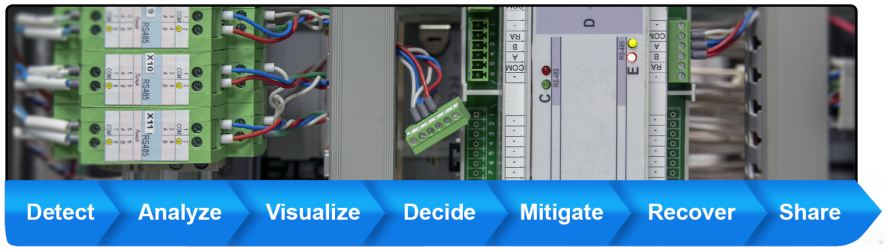
Images: Shutterstock, Shutterstock.com, 2021.

A. Scalco, S. Simske (Ph.D.), "Engineering and Development of a Critical Infrastructure Cyber Defense Capability for Highly Context-Sensitive Dynamic Classes — Part 1, Engineering and Part 2, Development," Journal of the Homeland Defense & Security Information Analysis Center (HDIAC), Volume 7, Number 1, June 15, 2020. Link: https://www.hdiac.org/journal-article/more-situational-awareness-for-industrial-control-systems-mosaics-engineering-and-development-of-a-critical-infrastructure-cyber-defense-capability-for-highly-context-sensitive-dynamic-class

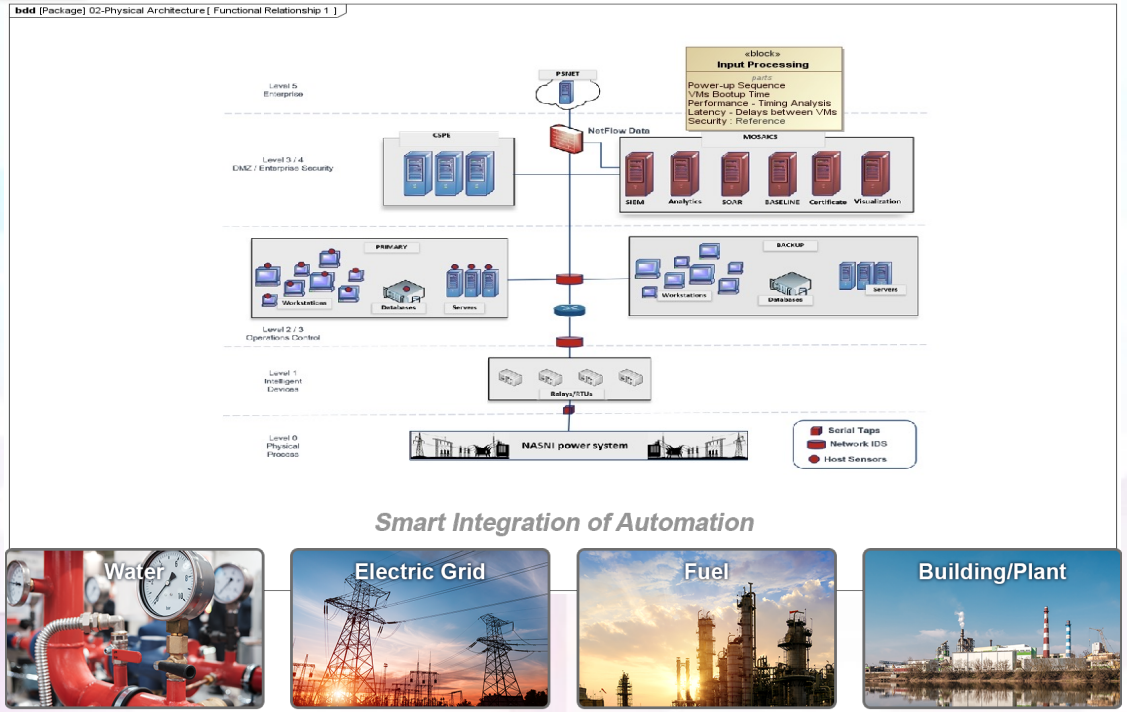
Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Conceptual Design





Joint Warfighter Operations



ICS Protection

ICS Operator

Cyber Defender

Reference: MOSAICS Joint Capability Technology Demonstration, 2021.

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Case Study MOSAICS JCTD

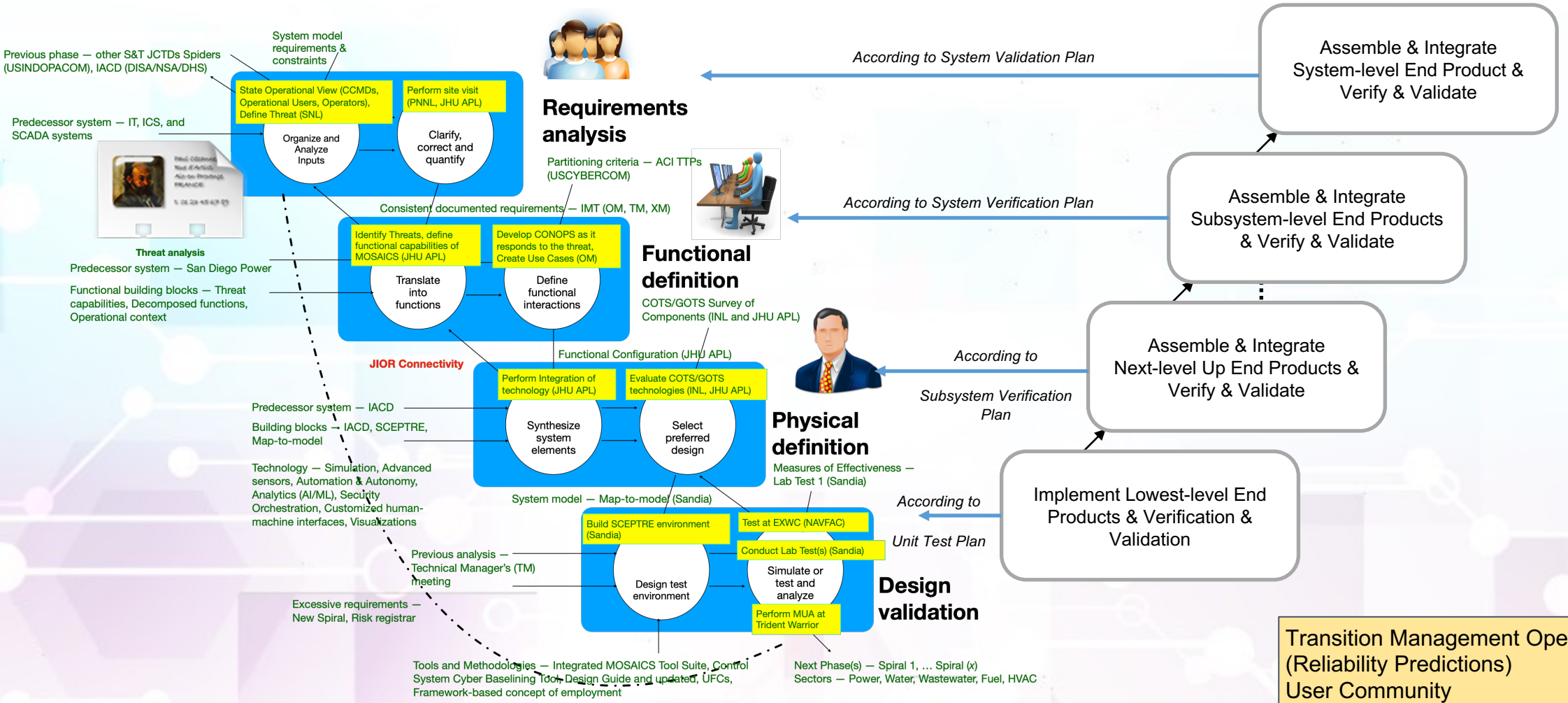


Figure 2. A. Scalco, "Case Study MOSAICS Systems Engineering 'Vee'," Colorado State University, 2019

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Transition Management Operations
(Reliability Predictions)
User Community
Commercial Industry Partnership
"Productization" of Capability

Operational View

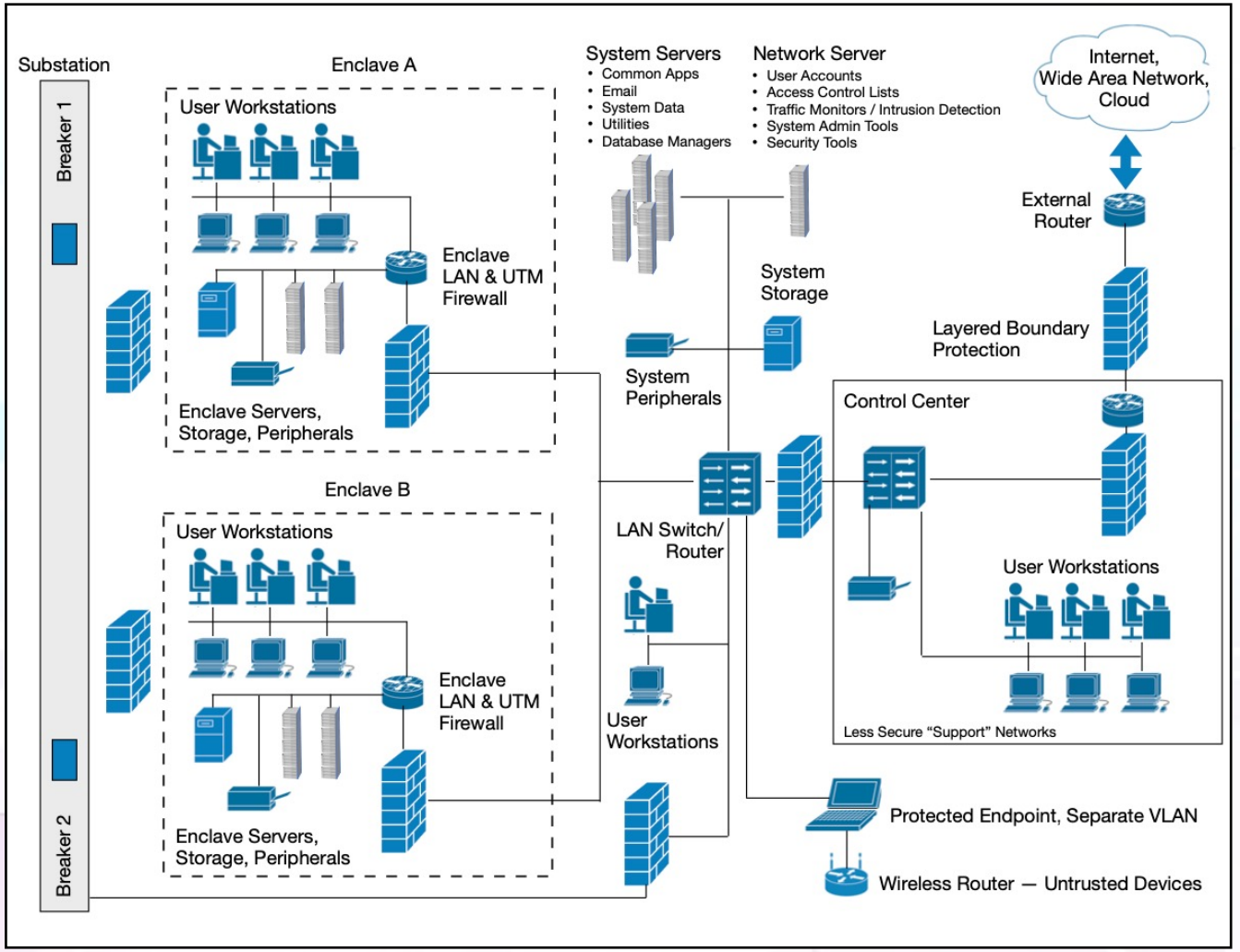


Figure 3. Cybersecurity for a Power Utility Substation Automation System (Scalco, 2021)

A. Scalco, S. Simske (Ph.D.), "Cybersecurity Principles and Technology for a Power Utility Substation Automation System," Journal of the Homeland Defense & Security Information Analysis Center (HDSIAC), March 8, 2021, pp. 36-41. Link: https://www.hdiac.org/hdiac-report/critical-infrastructure-protection/

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Detail Design

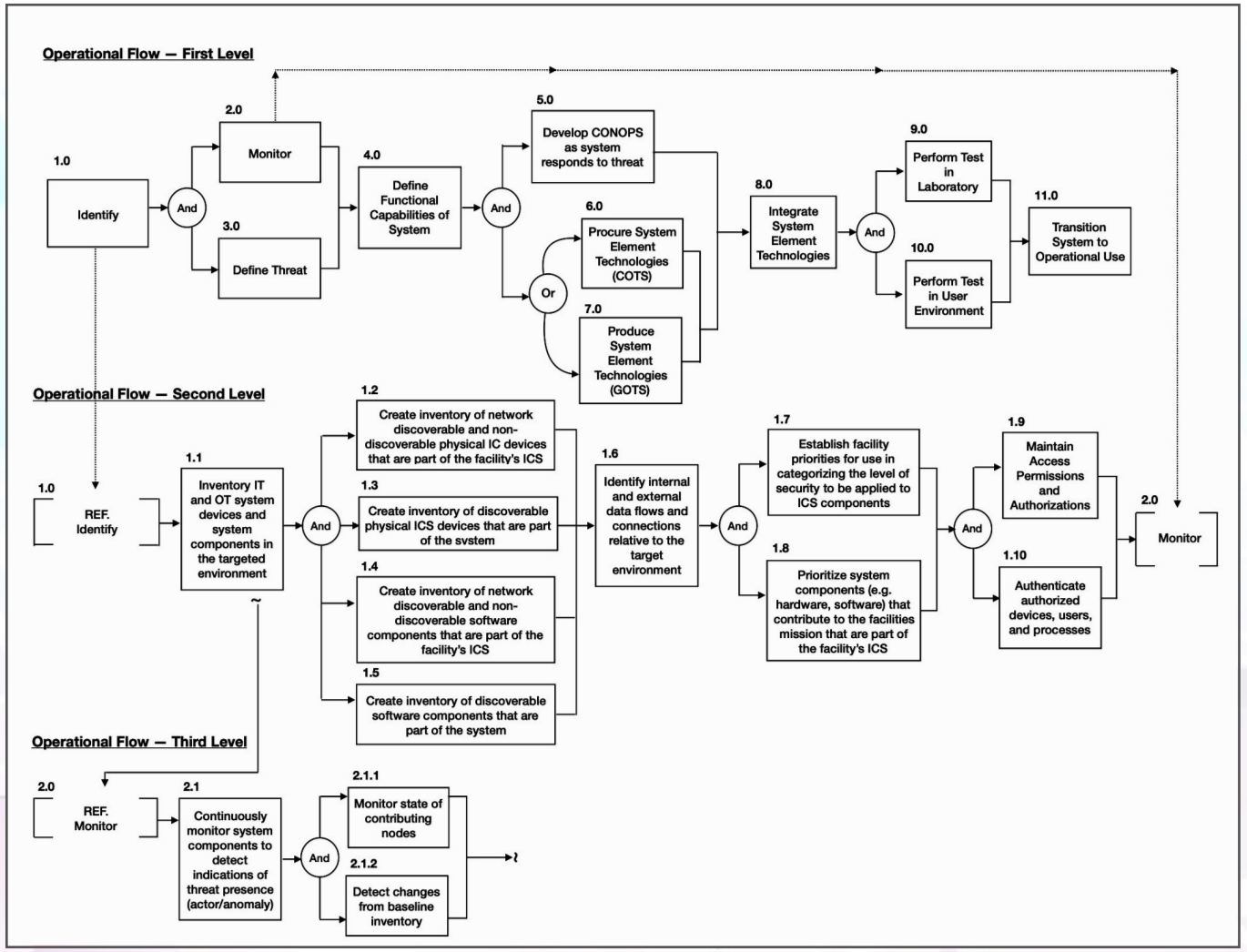


Figure 4. A. Scalco, "Detail Design," Colorado State University, 2020

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Allowable Downtime/Unavailability

Service Level Agreement (SLA) calculations assume a requirement of continuous uptime (i.e., 24/7/365)

Agreed Service Level Agreement (SLA) Uptime/Availability	SLA Uptime/Availability 99.9%	Uptime/Availability 99%	Uptime/Availability 98%
	Allowed Downtime/ Unavailability ***0.1%***	Allowed Downtime/ Unavailability ***1%***	Allowed Downtime/ Unavailability ***2%***
Daily	1m 26s	14m 24s	28m 48s
Weekly	10m 4s	1h 40m 48s	3h 21m 36s
Monthly	43m 49s	7h 18m 17s	14h 36m 34s
Quarterly	2hr 11m 29s	21h 54m 52s	1d 19h 49m 44s
Yearly	8h 45m 56s	3d 15h 39m 29s ***<5 days>***	7d 7h 18m 59s
What is acceptable Mission downtime/unavailability of critical infrastructure?			

Table 1. Agreed Service Level Agreement (SLA) Uptime/Availability (Uptime.is, 2021).

If infrastructure is worth $100 Billion a year, and if estimated downtime is just 1% that is a $1B threat.

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

High Value Assets

- New Substation Automation System (SAS) cost range $9M to $36M depending on voltage level (i.e., 69kV, 115kV, 138kV, 161kV, 230kV, 345kV, or 500kV) (PEguru, 2021)
- Sensitive information and processes (which is different from the sensitive assets of value or cost) also require protection (i.e., Network Analysis, Arc Flash, Load Modeling, Ground Grid Systems, Network Optimization, Power Transformers, GIS Map, Data Exchange, Cable Systems, Transmission Line, DC & Control Systems, Panel Systems, Protection Coordination, and Core Business Operations) (Scalco, 2021)
- High value items in terms of price of a power utility SAS (PEguru, 2021). However, with regard to cyber security, sensitive assets are at the lower levels of the Purdue Model (Scalco, 2021)

Type 1	Lower End Per Unit Cost	Higher End Per Unit Cost
Transformer	10MVA or less small power transformer, $500,000	Specialty phase shifter 100MVA, +(-) $4M
Circuit Breaker	12kV 1200AMP 16KAIC Vacuum Circuit Breaker, $26,000	765kV 3000Amp 40KAIC Gas Circuit Breaker Live Tank, $800,000
Circuit Switcher	34.5kV 600amp 25KAIC Capacitor Switcher, $45,000	230kV 3000amp 40KAIC switcher, $85,000
Disconnect Switches	12kV 600amp/1200amp switch manual operator, $7,000	765kV 3000amp switch motor operator, $150,000
Capacitors	12kV 4MVAR metal enclosure with breaker and reactor, $70,000	500KV 230MVAR fuseless with neutral reactors & stand, $700,000
Voltage Transformer	4kV wound voltage transformer, $1,500/phase	765kV capacitor voltage transformer relaying grade, $25,000/phase
Current Transformer	138kV current transformer, $15,000/phase	345kV current transformer, $30,000/phase
Surge Arrester	12.47kV 10.2kV MCOV porcelain station class arrester, $300/phase	765kV 467kV MCOV porcelain arrester, $28,000/phase
Station Service Transformer	12kV 150KVA SS pad mounted power transformer, $7,000 3ph unit	230KV 100KVA SSVT, $120,000/phase
Carrier Equipment	69kV 1200Amp wave trap & tuner, $12,000	345kV 3000Amp wave trap & tuner, $30,000
Insulators	138kV nominal 650kV BIL insulator, $500	500kV nominal rated insulator, $1,800
Control Building	60’ x 25’ building space for 20 panels, $1.5M	Switchgear building space for 13 breakers and HV relay panel and SCADA, $4M
Structural Steel	34.5kV H-frame deadens, $20,000	138kV double circuit monopole, $180,000
Conductors/Connectors	4/C #12, $1/foot	1/C 350kCMIL CU 600V, $14/foot

Table 2. Substation Cost Estimates High Value Items in Terms of Price of a Power Utility SAS (PEguru, 2021)

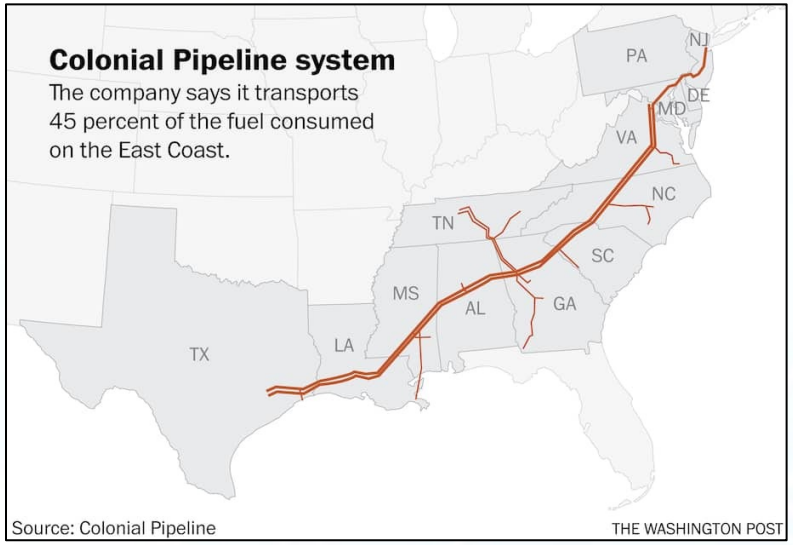
Reference: PEguru, “Substation Cost Estimator,” 2021. Substation Design — Power System Analysis. URL: https://peguru.com/substation-cost-estimator/

Reference: Aleksandra Scalco, Ph.D. Preliminary Exam, Colorado State University (CSU), 2021

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Potential Consequences of Cyber Event

- Impact on national security—facilitate an act of terrorism
- Reduction or loss of ability to conduct mission (one or multiple sites simultaneously)
- Injury or death of operators and other persons
- Damage to expensive equipment and systems
- Release, diversion, or loss of hazardous materials
- Contamination of product and physical plant
- Loss of proprietary or confidential information
- Loss of organizational image or customer/public confidence
- Long term Environmental damage
- Violation of regulatory requirements
- Criminal or civil legal liabilities



Source: The Washington Post, 2021

RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Source: Defense Acquisition University, 2021

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Substation Quantitative Risk Analysis (RA)

Electrical Distribution Substation
Example Site x

- Asset Valuation
- Threat Analysis
- Vulnerability Assessment

Total Risk = Sum All Identified Risk Assessments and Estimated Reduction Achieved by Applying Security Controls/Countermeasures as Mitigation

Residual Risk = Total Risk - Total Mitigation

ALE = SLE x ARO
SLE = Asset Value x Exposure Facture (EF)

- *Annual revenue $250M (Commercial)*
- *Estimated loss from a specific attack = 0.02% of annual revenue*
- *Estimated Frequency (EF) of attacks = 2/year*
- *Countermeasure target cost $6k/month estimated to reduce the loss to 0.002% of annual revenue*
- Calculate *Annualized Loss Expectance (ALE) from Single Loss Expectancy (SLE) and Annualized Rate of Occurrence (ARO)*
- *ARO = 2, EF = 0.002*
- *EF is the fraction of total asset value potentially lost in a single event with a specific threat*
- *ARO is the estimated number of occurrences of a specific threat in a 12-month period*
  - SLE (no control) = 0.02 x $250M = $5M
  - SLE (with control) = 0.002 x $250M = $500k
  - ALE (no control) = $5M x 2 = $10M
  - ALE (with control) = $6k x 2 = $12k
  - Total Cost of Control = $6k/mo x 12 mos = $72k
  - Control Value = $10M – $12k – $72k = $9,916k, or almost $10M ROI in the control
- Result = A positive return on the investment in the control

Reference: Steve Simske, Colorado State University (CSU) Lectures, 2020

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Colonial Pipeline Example

Malicious Actor(s) claimed financial gain to be objective, not physical damage.

Ransomware 7 - 12 May 2021

<5 days>
Downtime/Unavailability

- Asset Valuation
- Threat Analysis
- Vulnerability Assessment

- Annual Revenue >$500M
- 5,500 miles/>100 million gallons of fuel or 2.5 million barrels a day
- 45% of all fuel consumed on East Coast
- Serves more than 50 million Americans

- Single Ransomware Attack, 7 - 12 May 2021
- 5 days x 2.5M barrels = 12.5M barrels
- Crude Oil ($/barrel) 10 May = $64.92/barrel
- Crude Oil ($/barrel) 12 May = $68.83/barrel
- <12.5M x 10 May $64.95 = $812M>

ALE = SLE x ARO
SLE = Asset Value x Exposure Facture (EF)

- *Annual revenue >$500M (Commercial)*
- *Estimated loss from a specific attack = 0.02% of annual revenue*
- *Mission Criticality - HIGH (45% of all fuel consumed on East Coast)*
- *Estimated Frequency (EF) of attacks = 2/year*
- *Countermeasure target cost $6k/month estimated to reduce the loss to 0.002% of annual revenue*
- Calculate *Annualized Loss Expectance (ALE) from Single Loss Expectancy (SLE) and Annualized Rate of Occurrence (ARO)*
- *ARO = 2, EF = 0.002*
- *EF is the fraction of total asset value potentially lost in a single event with a specific threat*
- *ARO is the estimated number of occurrences of a specific threat in a 12-month period*
  - SLE (no control) = 0.02 x $500M = $10M
  - SLE (with control) = 0.002 x $500M = $1M
  - ALE (no control) = $10M x 2 = $20M
  - ALE (with control) = $6k x 2 = $12k
  - Total Cost of Control = $6k/mo x 12 mos = $72k
  - Control Value = $20M – $12k – $72k = $19,916,000
  - Positive Return on Investment (ROI) = ~ $20M

Colonial Pipeline paid **$4.4M** to obtain decryption tool in crypto currency

Reference: Steve Simske, Colorado State University Lectures, 2020

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.

Thank you!

Questions?

Copyright © 2021 by Aleksandra Scalco. Permission granted to INCOSE to publish.