Months to Minutes — Command and Control (C2) of Control Systems

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

January 25, 2022

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

INCOSE

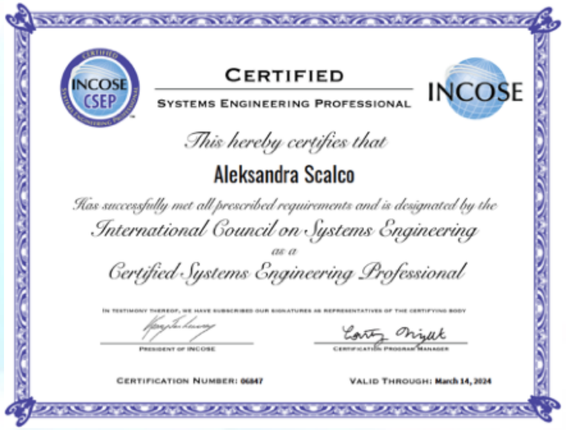
About Me

Mizzou
University of Missouri

Iowa State University
of Science and Technology

Colorado State University

Certified
INCOSE CSEP
Systems Engineering Professional



Certified

Systems Engineering Professional

INCOSE

This hereby certifies that

Aleksandra Scalco

Has successfully met all prescribed requirements and is designated by the

International Council on Systems Engineering

as a

Certified Systems Engineering Professional

In testimony thereof, we have subscribed our signatures as representatives of the certifying body

President of INCOSE

Certification Program Manager

Certification Number: 06847

Valid Through: March 14, 2024

Institute for Technical Leadership
INCOSE

INCOSE
Technical Leadership
Institute (TLI)
Seventh Cohort

IEEE

Senior Member

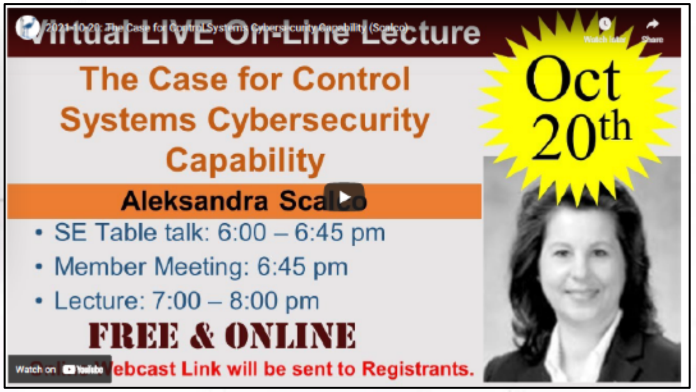
INCOSE Critical Infrastructure Protection (CIPWG) Working Group Co-Chair

INCOSE Resilient Systems Working Group Member

ITIL®

EXPERT

Champions and Practitioners of Systems Engineering
CHESAPEAKE CHAPTER



2021-10-20: The Case for Control Systems Cybersecurity Capability (Scalco)

Virtual LIVE On-Line Lecture

The Case for Control Systems Cybersecurity Capability

Aleksandra Scalco

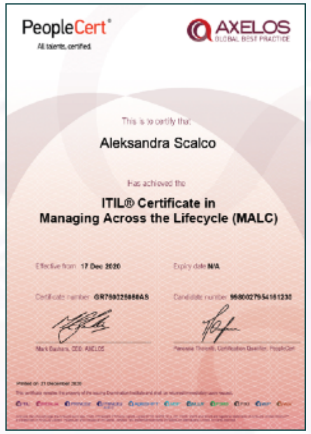
- SE Table talk: 6:00 – 6:45 pm
- Member Meeting: 6:45 pm
- Lecture: 7:00 – 8:00 pm

FREE & ONLINE

Webcast Link will be sent to Registrants.

Oct 20th

Previously briefed the Chesapeake Chapter in 2021…



PeopleCert®
All talents, certified.

AXELOS
GLOBAL BEST PRACTICE

This is to certify that

Aleksandra Scalco

Has achieved the

ITIL® Certificate in Managing Across the Lifecycle (MALC)

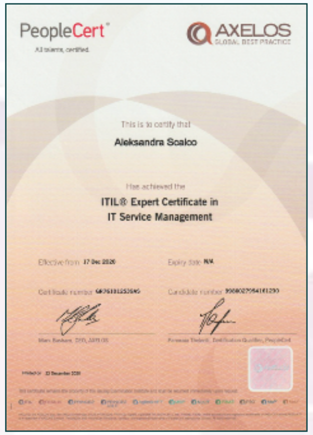
Effective from 17 Dec 2020 | Expiry date N/A

Certificate number GR750025880AS | Candidate number 9980027954181230

Mark Basham, CEO, AXELOS

[illegible], Certification Qualifier, PeopleCert

Printed on: 21 December 2020



PeopleCert®
All talents, certified.

AXELOS
GLOBAL BEST PRACTICE

This is to certify that

Aleksandra Scalco

Has achieved the

ITIL® Expert Certificate in IT Service Management

Effective from 17 Dec 2020 | Expiry date N/A

Certificate number [illegible] | Candidate number 9980027954181230

Mark Basham, CEO, AXELOS

[illegible], Certification Qualifier, PeopleCert

Printed on: 22 December 2020

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

INCOSE

Agenda

COLORADO STATE UNIVERSITY

- Control Systems Cybersecurity — Background
- Research Objectives — Remediation of Vulnerability
- Measuring Disagreement as a Means of Identifying Vulnerabilities
- Case Study — Water Treatment Facility & Use Case Protect
- Future Work

Disagreement ⟶ Misalignment ⟶ Vulnerability

The vulnerability induced by misalignment may be greater than innate system design vulnerability.

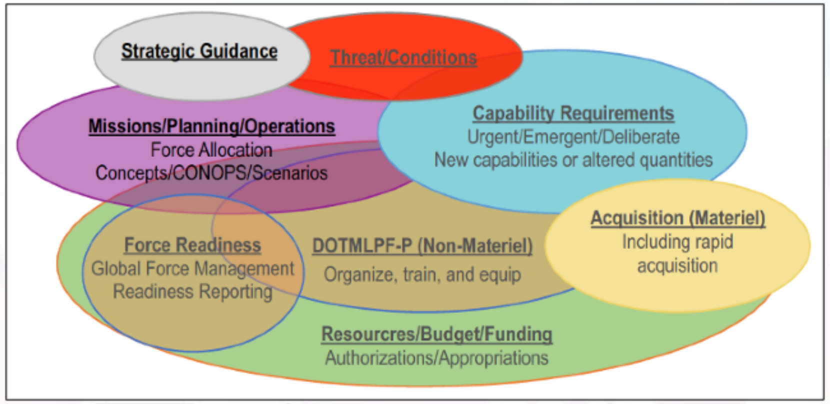
Copyright © 2021 by Aleksandra Scalco and Steve Simske. Permission granted to INCOSE to publish.

Image: Shutterstock, Shutterstock.com, 2021.

Uncertainty and Lack of Agreement

- Eight (8) domains are used to assess and solve warfighting gaps (DOD, 2021)
  - DOTMLPF-P. Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
- Uncertainty and lack of professional agreement about how Control Systems (CS) are defended from cyber events across DOTMLPF-P lead to a misalignment resulting in deficient C2.
- Measurement of uncertainty and agreement can be used to remediate vulnerability.

- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01 establishes policies for the Joint Capabilities Integration and Development System (JCIDS).
- JCIDS supports the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council (JROC) in identifying and assessing joint military capability needs.



[1] Department of Defense (DOD), Acquisition Notes, “JCIDS Process,” 2021. URL: https://acqnotes.com/acqnote/acquisitions/cjcsi-3170 [retrieved March 2021].

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

Image: Shutterstock, Shutterstock.com, 2021.

[3] PEDERSEN, D. 2019. Topgun An American Story, New York, Hachette Books.

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

Top Gun

“On March 3, 1969, the United States Navy established an elite school for the top one percent of its pilots. Its purpose was to teach the lost art of aerial combat and to ensure that the handful of men who graduated were the best fighter pilots in the world. They succeeded. Today, the Navy calls it Fighter Weapons School. The flyers call it: TOP GUN.” (Top Gun, 1986)

Table 1. Enemy Aircraft to US Aircraft Est. Loss Ratio

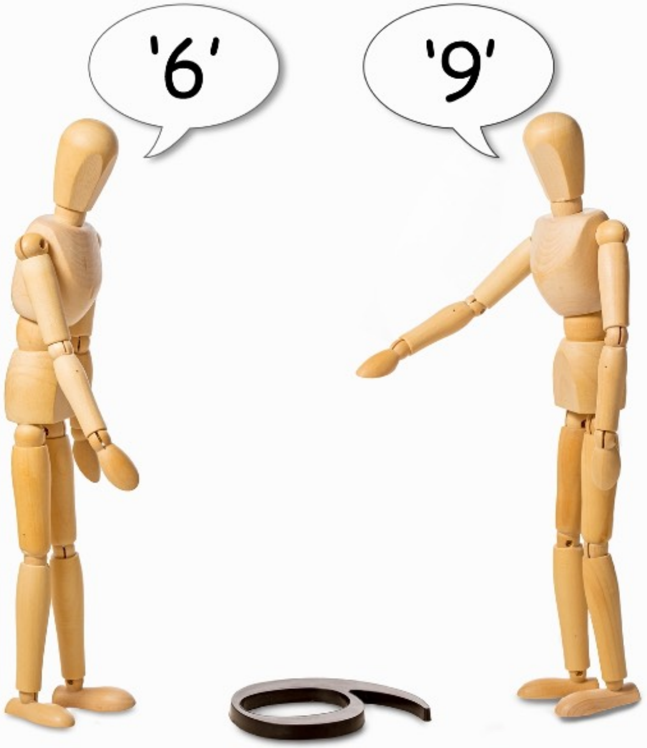
World War II	14:1
Korean Conflict	12:1
Vietnam War (Pre-Top Gun)	2.5:1
Vietnam War with Top Gun Training & Other Measures	13:1

Table 1. [2] BARANEK, D. Origins of Topgun. HistoryNet.

The Best of the Best.

Measuring Disagreement as a Means of Identifying Vulnerabilities

Disagreement ➡ Misalignment ➡ Vulnerability



The vulnerability induced by misalignment may be greater than innate system design vulnerability.

Vulnerability ➡ Alignment ➡ Agreement

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

Image: Shutterstock, Shutterstock.com, 2022.

INCOSE

Control System Cybersecurity and Emerging Policy

COLORADO STATE UNIVERSITY

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

- U.S. House Resolution 1833 (H.R. 1833) “Department of Homeland Security (DHS) Industrial Control Systems Capabilities Enhancement Act” introduced in March 2021 (Ref. [4])
- Presidential Action — Executive Order (E.O.) 14028 on Improving the Nation’s Cybersecurity, May 12, 2021 [5]
- S. 1605 National Defense Authorization Act (NDAA) for Fiscal Year 2022, SEC. 1505. Operational Technology and Mission-Relevant Terrain in Cyberspace, December 21, 2021. [6]
- Presidential Action — National Security Memorandum (NSM) to improve cybersecurity of National Security, Department of Defense (DOD), and Intelligence Community Systems, January 19, 2022. [7]

[4] U.S. House, House Resolution 1833 (H.R. 1833) "DHS Industrial Control Systems Capabilities Enhancement Act of 2021," 2021.

[5[BIDEN, P. J. 2022a. Executive Order on Improving the Nation’s Cybersecurity. *In:* OFFICE, E. (ed.). Washington, D.C.: Executive Office.

[6] 117th Congress, Congressional Bill, National Defense Authorization Act (NDAA) for Fiscal Year 2022

[7] BIDEN, P. J. 2022b. National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. *In:* OFFICE, E. (ed.). Washington, D.C.: Executive Office.

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

Images: Shutterstock, Shutterstock.com, 2022.

2020 Global Pandemic > Remote Workers

COLORADO STATE UNIVERSITY

- Essential critical infrastructure workers increased remote access operations.
- Lack of cybersecurity training, plans, or tools to ensure cybersecurity rules were followed. (Tasheva, 2021).
- Businesses extend remote control access to operations from 9 percent to 60 percent in three months. (Ribeiro, 2021).
- During the same period, cybercrime ransomware attacks were estimated to have increased by 116% between January and May 2020. (Networks, 2021).

[8] TASHEVA, I. 2021. Cybersecurity post-COVID-19: Lessons learned and policy recommendations. *European View*.

[9] RIBEIRO, A. 2021. Ransomware strikes rise sharply, fueled by profit potential. *Industrial Cyber*.

[10] NETWORKS, N. 2021. What You Need to Know to Fight Ransomware and IoT Vulnerabilities Including Recommendations for Enhancing Cyber Resilience. *OT/IoT Security Report*. nozominetworks.com: Nozomi Networks, Inc.

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

Images: Shutterstock, Shutterstock.com, 2022.

Misalignment Impacts of ***Command & Control (C2) Loss*** of Control System Cybersecurity

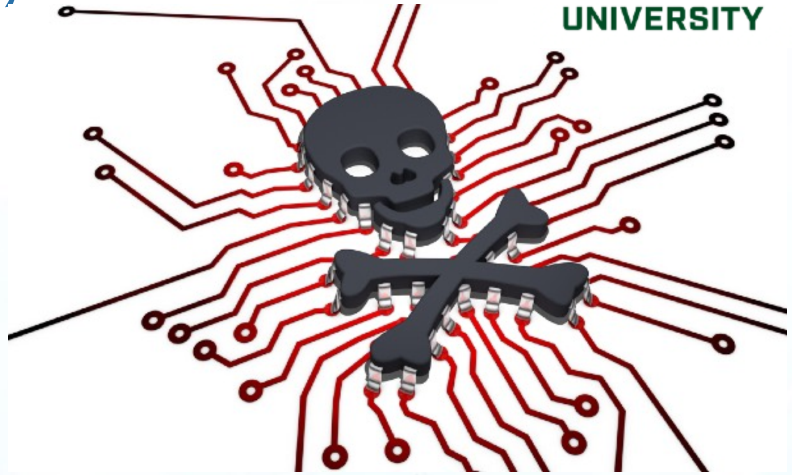
- **Mission.** Loss of command and control of mission functions.
- **Physical.** Personnel injury or loss of life, loss of assets, environmental damage.
- **Economic.** Unavailability of critical infrastructure (i.e., electrical power, fuel, water, etc.) beyond the systems sustaining direct and physical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

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

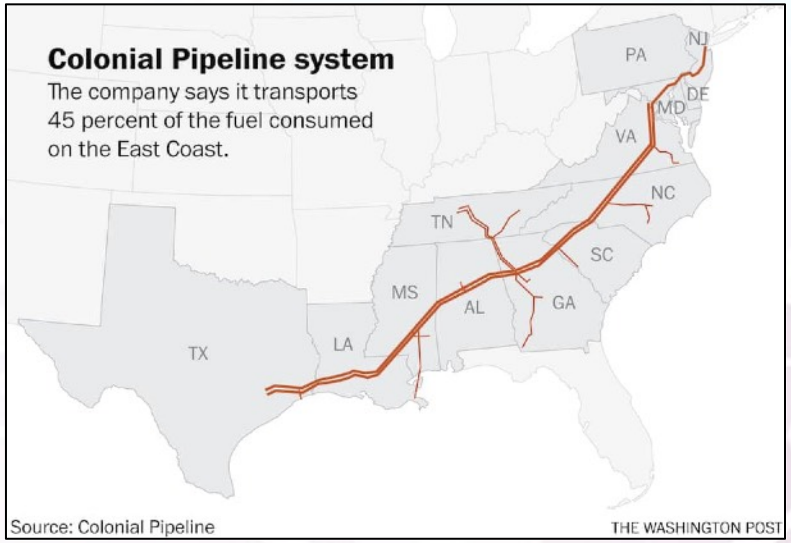
Images: Shutterstock, Shutterstock.com, 2021.

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



Images: Shutterstock, Shutterstock.com, 2021.



Colonial Pipeline system

The company says it transports 45 percent of the fuel consumed on the East Coast.

Source: Colonial Pipeline

THE WASHINGTON POST

[11] TURTON, W. & MEHROTRA, K. 2021. Hackers Breached Colonial Pipeline Using Compromised Password. *Bloomberg*.

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

Image Source: The Washington Post, 2021.

System Variables

Context-sensitive Dynamic Classes

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

[12] 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 and Steve Simske. Permission granted to INCOSE to publish.

Images: Shutterstock, Shutterstock.com, 2021.

INCOSE

Nature Review
Vulnerability — Alignment — Agreement

COLORADO STATE UNIVERSITY

- ***In Nature, schooling behavior, fish appear to synchronize swimming in coordination as a single organism***

- ***Coordinated Movement Alignment at Impressive Speed***

- ***Vulnerability***

- ***Protection***

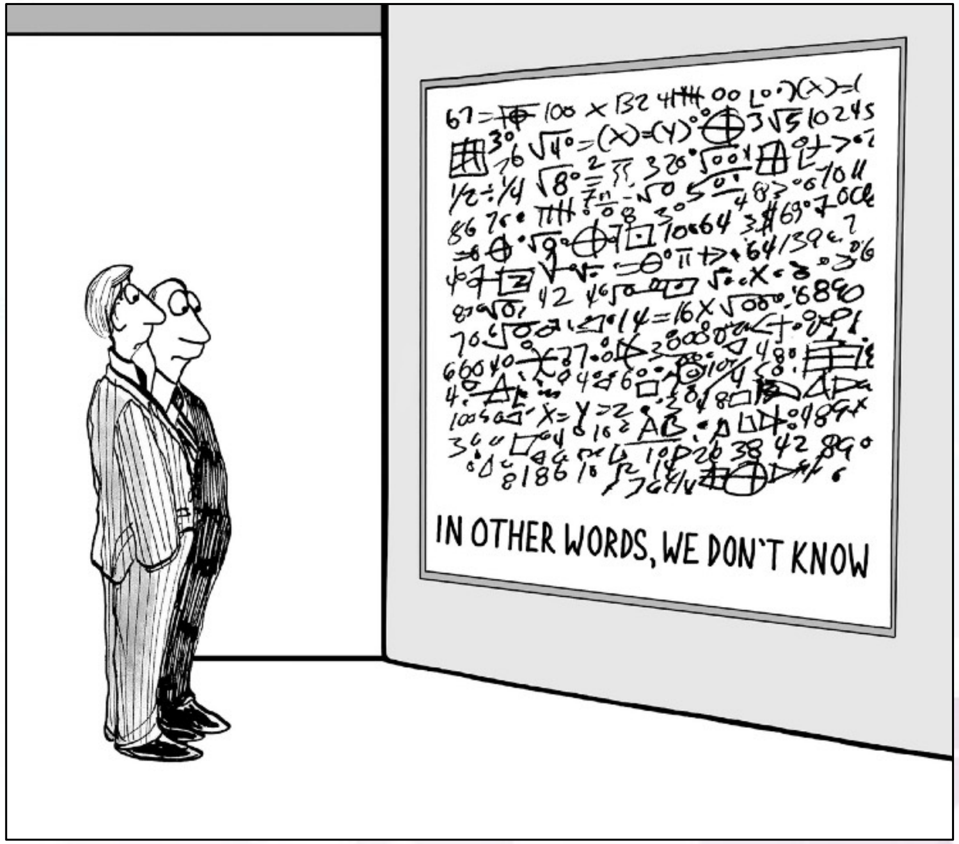
- ***Shared Situational Awareness***

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

Images: Shutterstock, Shutterstock.com, 2022.

Literature Review

- Most companies state cybersecurity for OT/ICS as a significant priority (Schwab and Poujol, 2018).
- IT and OT professionals possess varying goals, processes, tools, and language. (Schwab and Poujol, 2018).
- The term "cybersecurity" is one of the least understood within the DoD. (Span et al., 2018).
- No reinforcement of complementary safety and cybersecurity measures (i.e., activity logging for attack detection and accident anticipation); friction where safety and cybersecurity requirements are conflicting. (Kavallieratos et al.).
- Confusion as new terms emerge to describe new technologies and capabilities without clearly distinguishing the relationships of terms (e.g., IIoT, SCADA, ICS). (Kayan et al., 2021).



[13] SCALCO, A. & SIMSKE, S. 2022. Modeling Uncertainty of Agreement to Achieve Stakeholder Alignment and Overcome Control System Cyber Vulnerability. *In:* INCOSE (ed.) *FuSE.*

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

Images: Shutterstock, Shutterstock.com, 2021.

Research Hypothesis

- Hypothesis — Test whether there is agreement by professionals on how to achieve cybersecurity for control systems
- Null hypothesis (H_0) — There is consistent agreement on how to achieve cybersecurity for control systems is by all professionals
- Alternate hypothesis (H_a)— The degree of agreement by professionals on how to achieve cyber security for control systems varies (examples)
  - By occupation (e.g., engineer, computer scientist, technician),
  - By topic (e.g., network system, incident response, cyber security),
  - By the amount of experience (i.e., number of years of experience in the field),
  - By type of experience (i.e., roles performed and at what level in the architecture),
  - By governance of the asset-owning organization they support (e.g., tools, methods, policies, processes, and procedures).

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

Images: Shutterstock, Shutterstock.com, 2022.

Methodology

COLORADO STATE UNIVERSITY

- Empirical, Quantitative Research Data
- 203 multiple-choice questions + 1 open response
- Data Collection Method
  - Website
  - Word-of-mouth recruiting
  - SurveyMonkey platform
- No Incentives
- No time limit to responding
- Confidentiality and Risks
- Timeline and Limitations
  - August 2020 — February 2021

- Sampling Bias and Size
  - – Total estimated CPS/CS population 5,000
  - – Objective +(-) 10% margin of error
  - – Objective response of 100 participants
  - – Expected 25% informed or invited would respond
  - – # of respondents needed/expected % of response rate
  - – 400 people needed to learn about the survey opportunity based on the expected response rate

Colorado State University (CSU) Institutional Review Board (IRB) Protocol Number: 20-10209H.
Research Director Steve Simske, steve.simske@colostate.edu, Aleksandra Scalco, ascalo@colostate.edu, or RICRO_IRB@mail.colostate.edu.

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

Analysis Plan and Hypothesis Test

- Analysis Plan
  - Data collection to test the hypothesis (August 2020 — February 2021)
  - Performed statistical test
  - Analyzed results
  - Present findings and future work
- Hypothesis Test
  - Measure responses by professionals to questions about cyber security
  - Likert Scale — Examine how strongly participants are in agreement or disagreement with statements along with a neutral option on a 3 - 5 point scale with anchors
  - Measure R^2 values to show sensitivity in the workforce

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

Nine (9) Sections of Questions

1. **Participant Demographics** — Participant data (e.g., Occupational Field, role, employment sector, education, age, gender)
2. **Network Systems** — Knowledge of network systems in the organization
3. **Infrastructure** — Knowledge of facilities and infrastructure used in operations
4. **Incident Response** — How the participant's organization handles a data breach or cyberattack, including the way consequences of the attack or breach (the "incident") are managed
5. **Resources** — Process by which materials, energy, services, staff, knowledge, or other assets are made available
6. **Training** — Representative training and certification courses related to cyber-physical systems/control systems
7. **Knowledge, Skills, and Abilities (KSA)** — attributes that represent is a body of information applied directly to the performance of a function
8. **Red Team** — Ability to evaluate Computer Network Defense Service Providers (CNDSPs) before live play on networks
9. **Security Considerations** — Knowledge of cyber security practices (e.g., penetration testing, encryption)

[14] Simske, S. and Scalco, A., "Cyber-physical Systems/Control System (CPS/CS) Workforce Questionnaire," 2019. Colorado State University (CSU) Institutional Review Board (IRB), Protocol Number 20-102009H.

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

Questionnaire Mean *

Mean
126

Mean
145

Mean
170

- Total Number of Participants: 187
- Total Who Completed All 203 Questions: 100
- For all responses, the Mean = 126
- * Remove responses of those who stopped by question 2 (i.e., consent and occupational field), then the Mean = 145
- * Remove responses of those who stopped by question 24 (i.e., profile questions), then the Mean = 170

Question	Responses	Total
203	100	20300
180	1	180
166	2	332
110	6	660
88	2	176
76	3	228
68	2	136
47	18	846
32	1	32
24	27	648
2	25	50
		23588
23588 / 187	**126.139037**	

Table 13: All Responses Mean = 126

Question	Responses	Total
203	100	20300
180	1	180
166	2	332
110	6	660
88	2	176
76	3	228
68	2	136
47	18	846
32	1	32
24	27	648
		23538
23538/162	**145.296296**	

Table 14: Responses without those who stopped at 2 (only opened questionnaire) Mean = 145

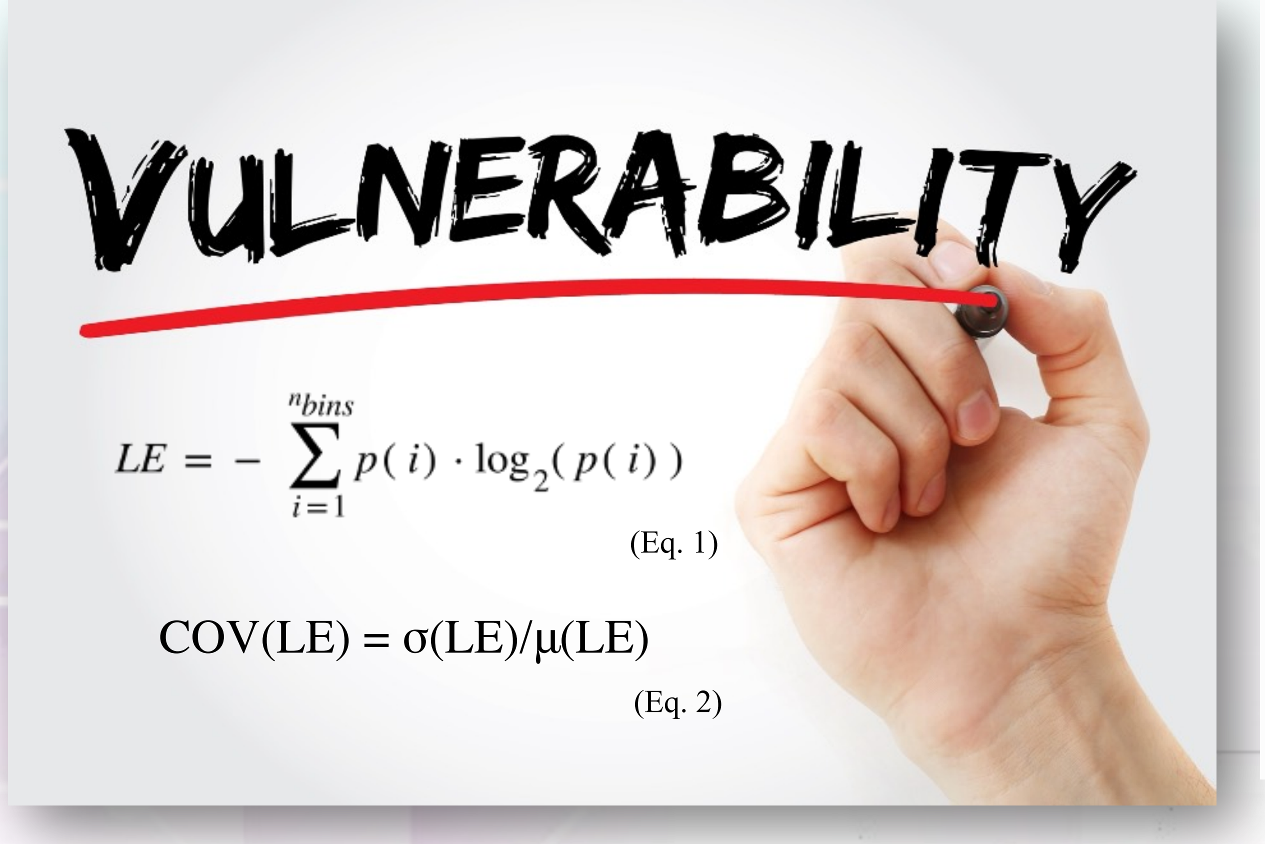
Question	Responses	Total
203	100	20300
180	1	180
166	2	332
110	6	660
88	2	176
76	3	228
68	2	136
47	18	846
32	1	32
		22890
22890/135	**169.555556**	

Table 15: Responses without those who stopped at 2 and those who stopped at 24 (only responded to profile questions) Mean = 170

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

The Analytic Process

Disagreement ➡ Misalignment ➡ Vulnerability

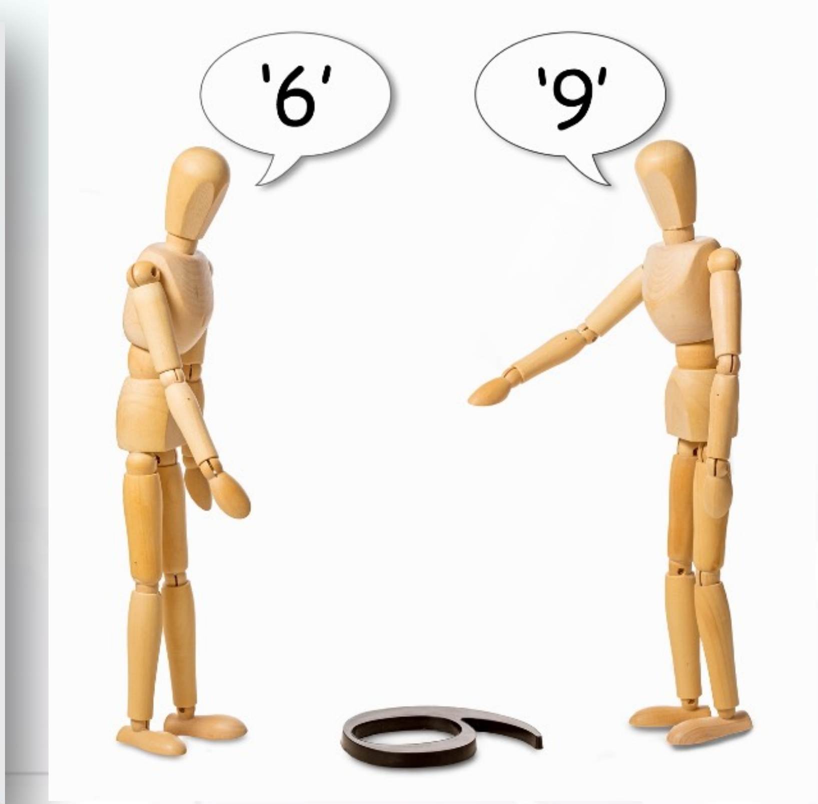


$$LE = -\sum_{i=1}^{n_{bins}} p(i) \cdot \log_2(p(i))$$

(Eq. 1)

$$COV(LE) = \sigma(LE)/\mu(LE)$$

(Eq. 2)



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

Images: Shutterstock, Shutterstock.com, 2022.

R^2 values to show sensitivity in the workforce

- If R^2 value is < 0.3, this is considered as non or very weak effect size
- If R^2 value is 0.3 < r < 0.5, this value is considered as moderate effect size
- If R^2 value is r < 0.7, this value is considered as strong effect size

R^2 value <0.3
Weak

R^2 value 0.3 < r < 0.5
Moderate

R^2 value r <0.7
Strong

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

Vulnerability Induced by Misalignment

Where correlation is poor, these professionals <u>will be at odds</u>.

R^2 value r <0.7
Strong

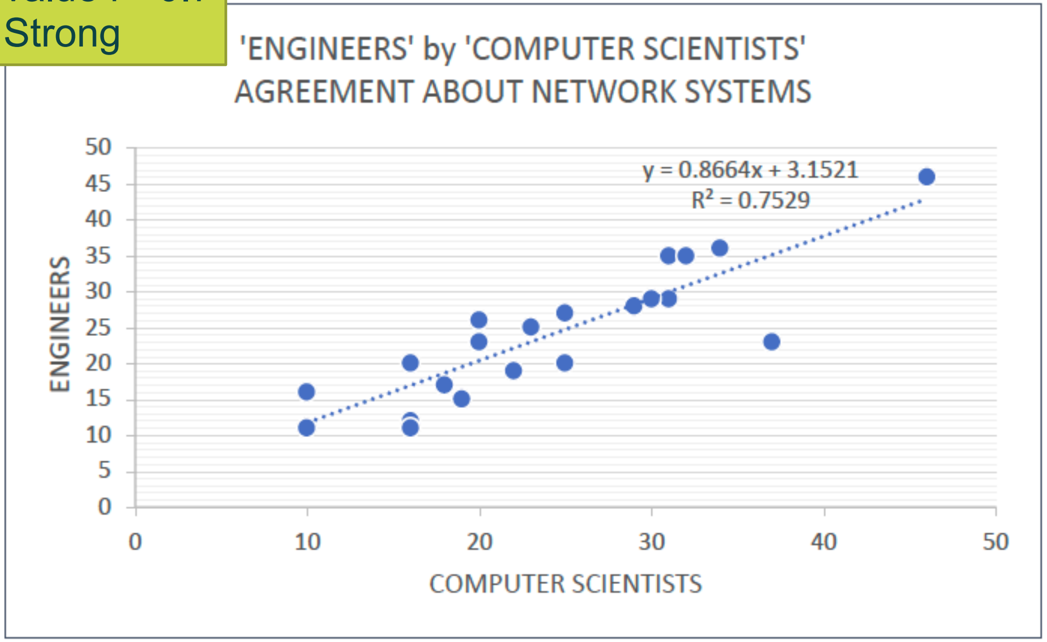


Figure 1 Correlation between Engineers and Computer Scientists for Network Systems Questions

R^2 value <0.3
Weak

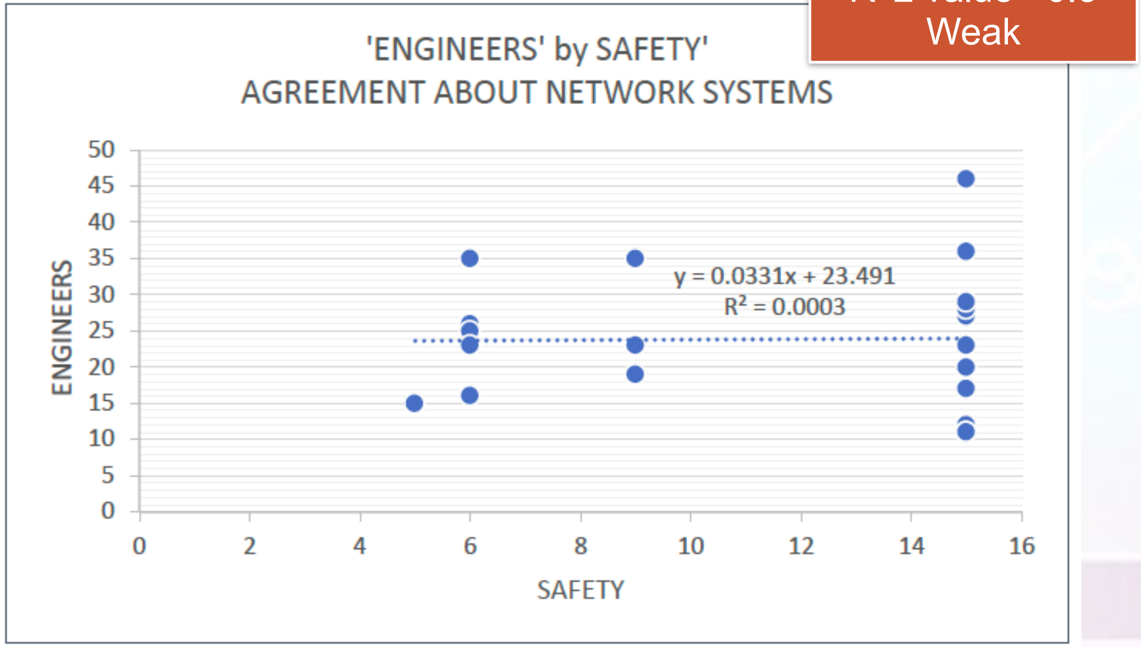
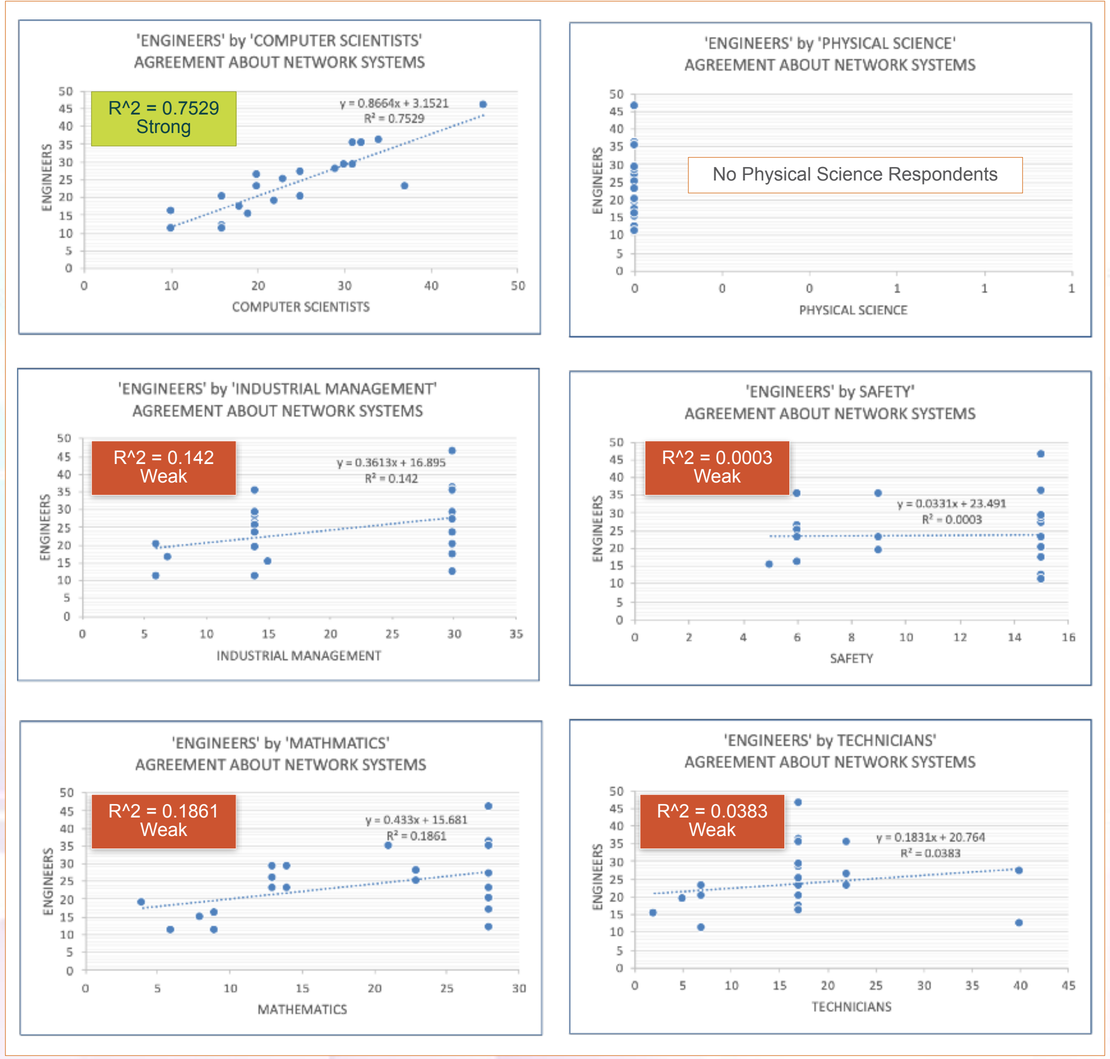


Figure 2 Correlation between Engineers and Safety Personnel for Network Systems Questions

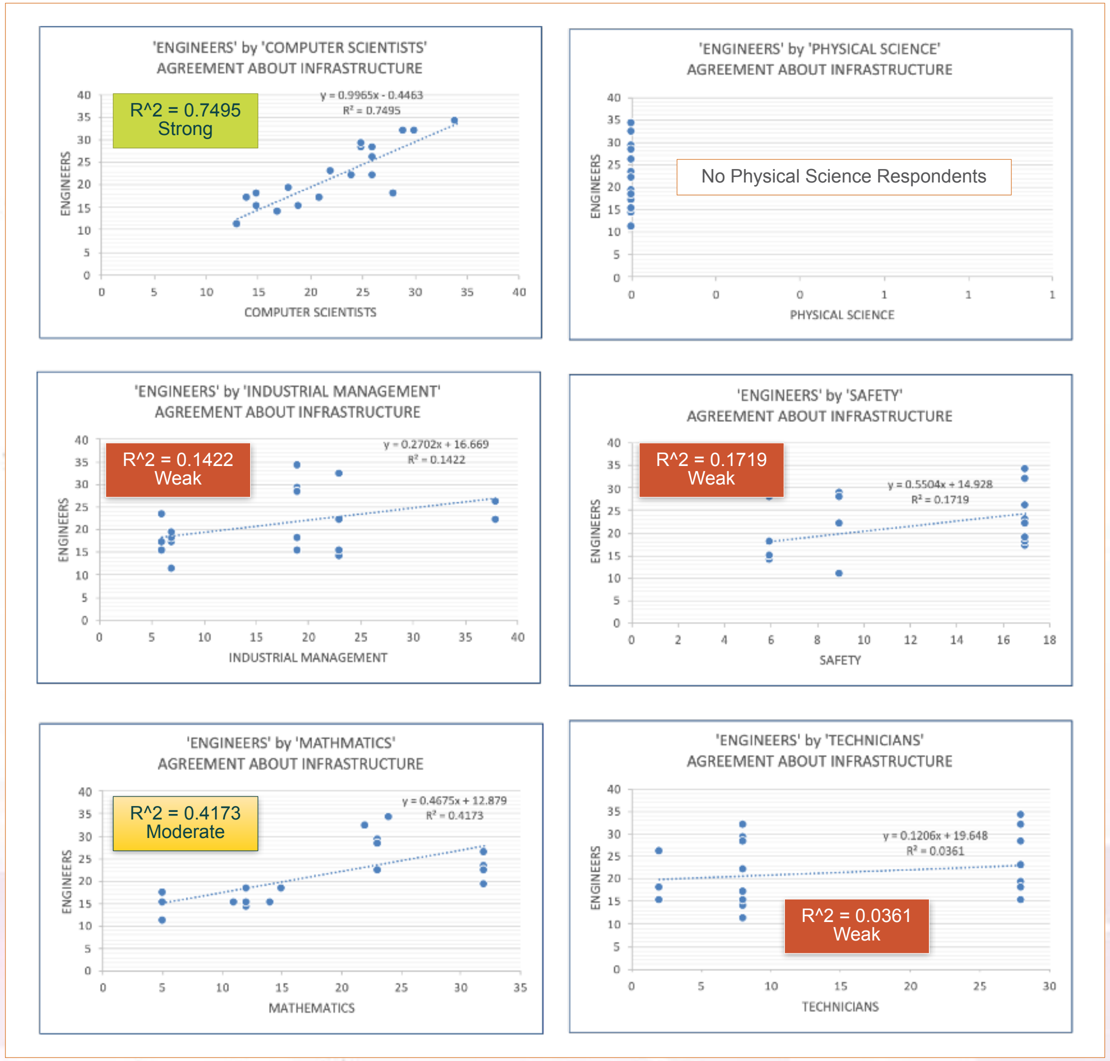
Copyright © 2021 by Aleksandra Scalco and Steve Simske. Permission granted to INCOSE to publish.

Engineers Agreement About Network Systems



- Figure 4: Engineers by Other Occupation Agreement About Network Systems, Questions 25 — 47 (Scalco, 2021)

Engineers Agreement About Infrastructure

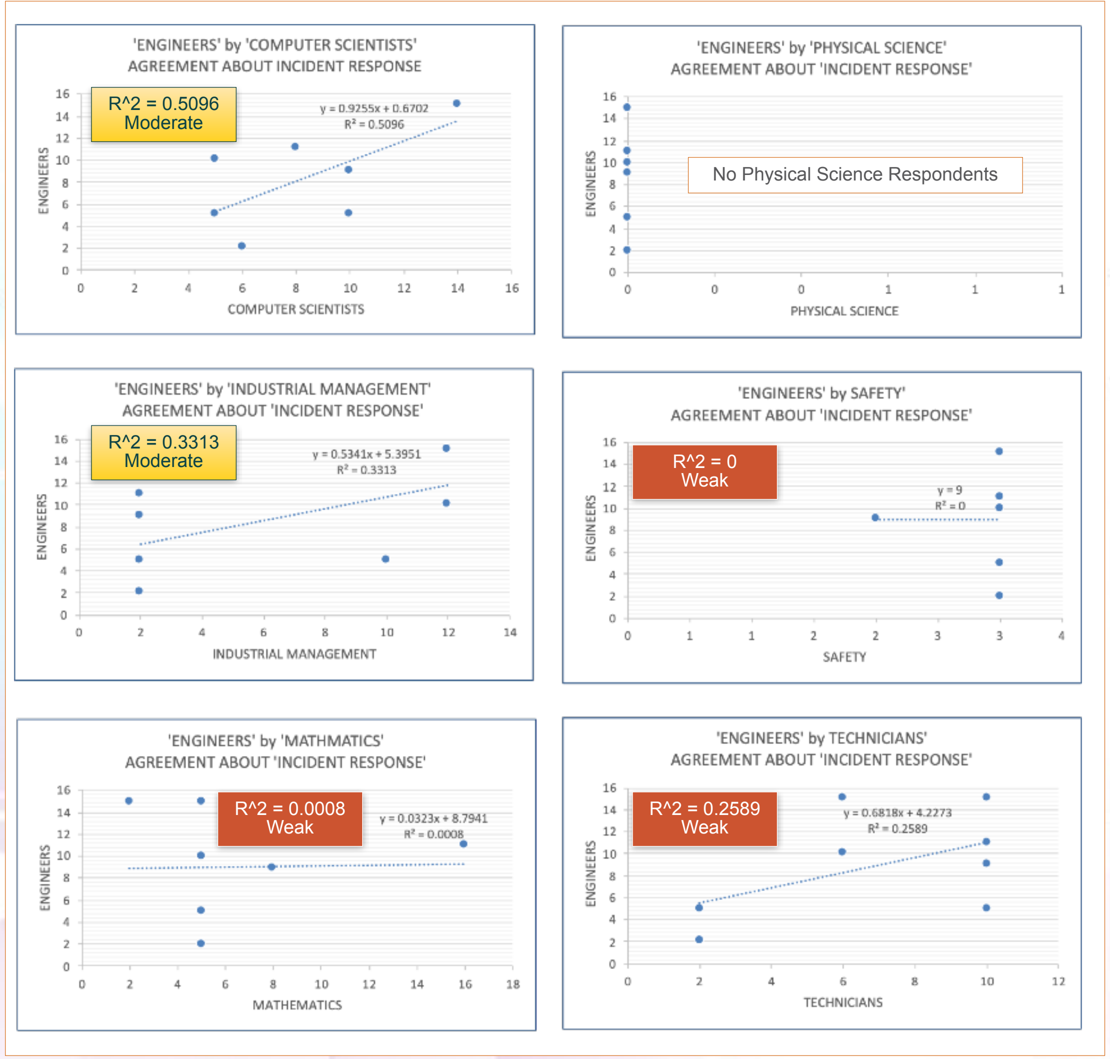


- Figure 5: Engineers by Other Occupation Agreement About Infrastructure, Questions 48 — 68 (Scalco, 2021)

COLORADO STATE UNIVERSITY

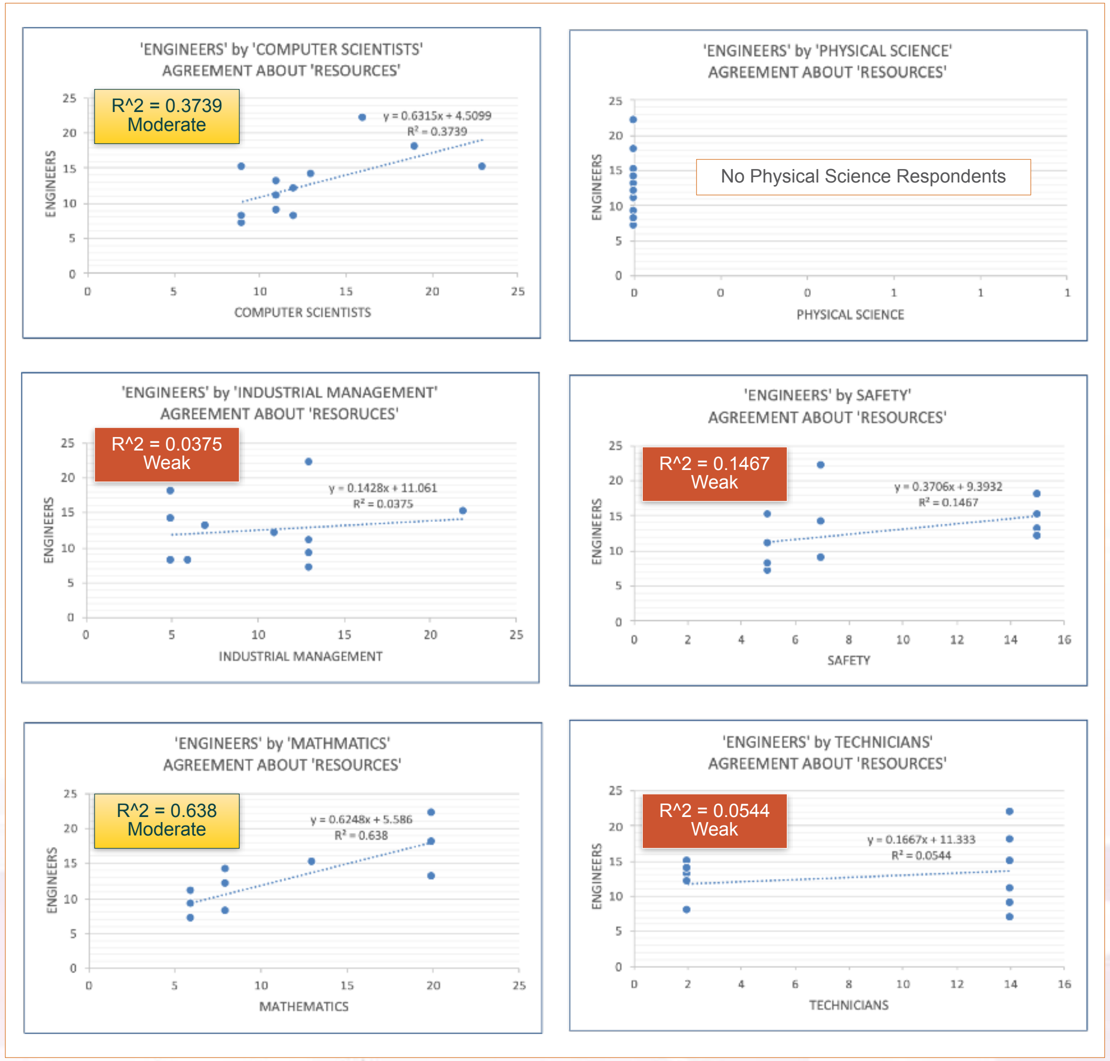
Copyright © 2021 by Aleksandra Scalco and Steve Simske. Permission granted to INCOSE to publish.

Engineers Agreement About Incident Response



- Figure 6: Engineers by Other Occupation Agreement About Incident Response, Questions 69 — 76 (Scalco, 2021)

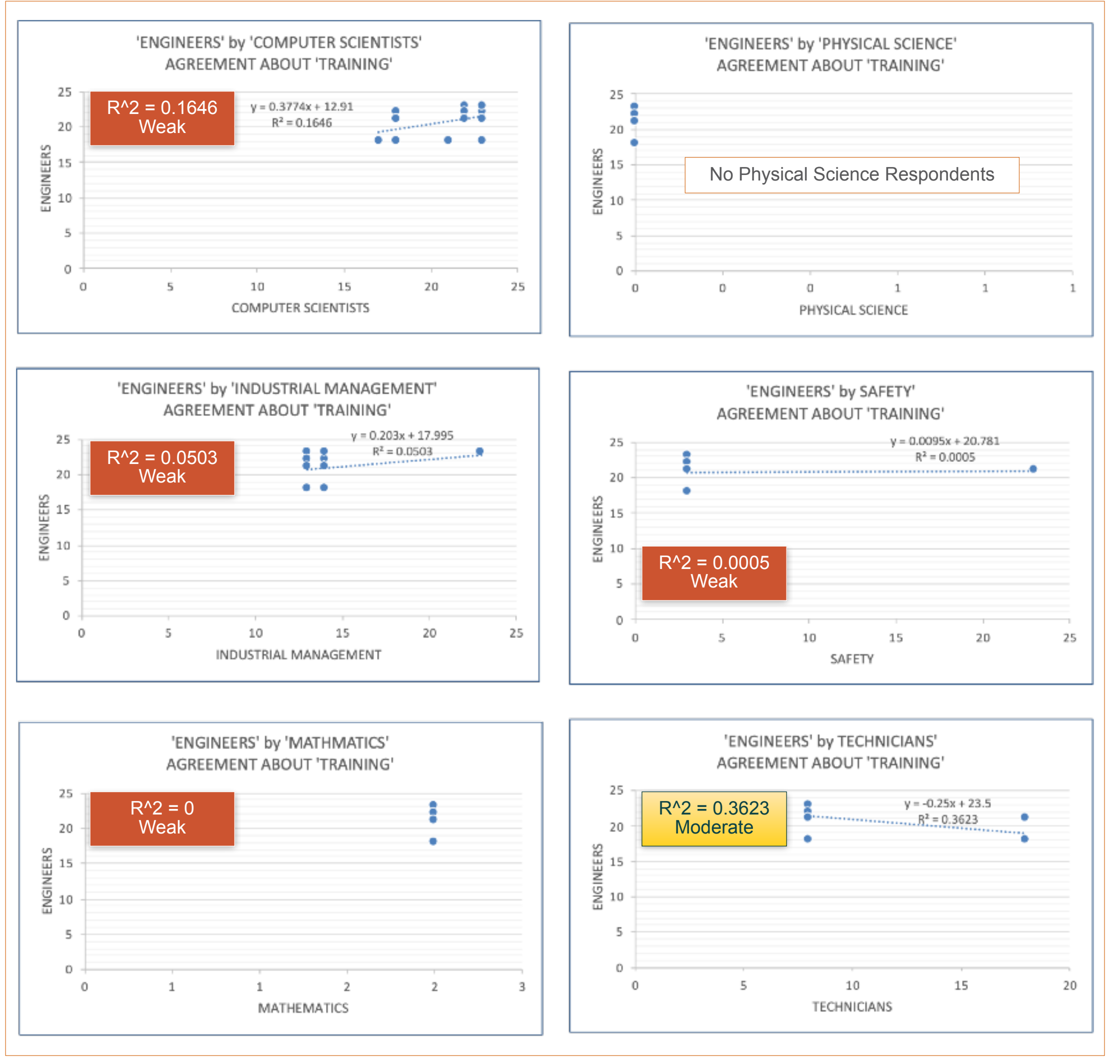
Engineers Agreement About Resources



- Figure 7: Engineers by Other Occupation Agreement About Resources, Questions 77 — 88 (Scalco, 2021)

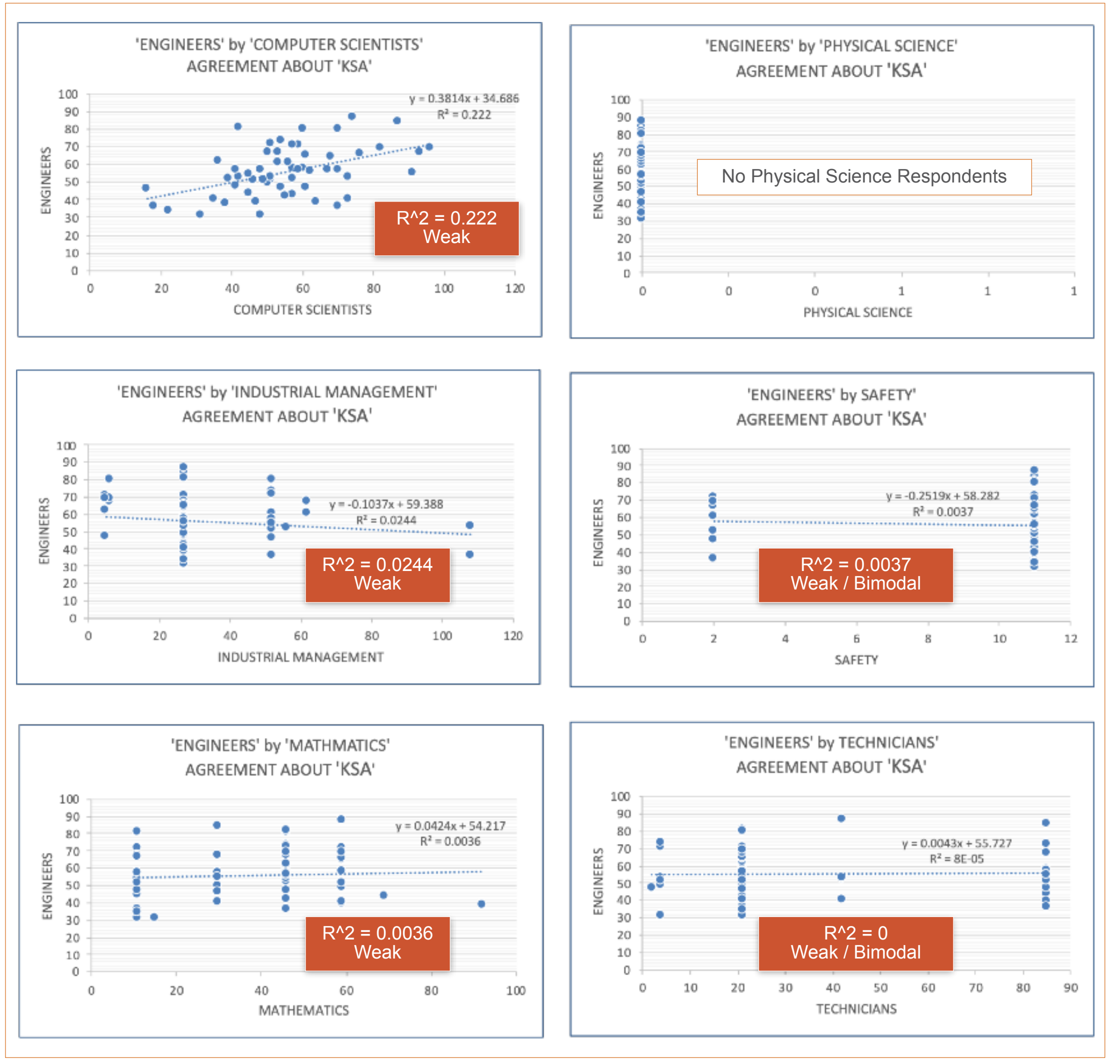
Copyright © 2021 by Aleksandra Scalco and Steve Simske. Permission granted to INCOSE to publish.

Engineers Agreement About Training



- Figure 8: Engineers by Other Occupation Agreement About Training, Questions 89 — 110 (Scalco, 2021)

Engineers Agreement About KSAs

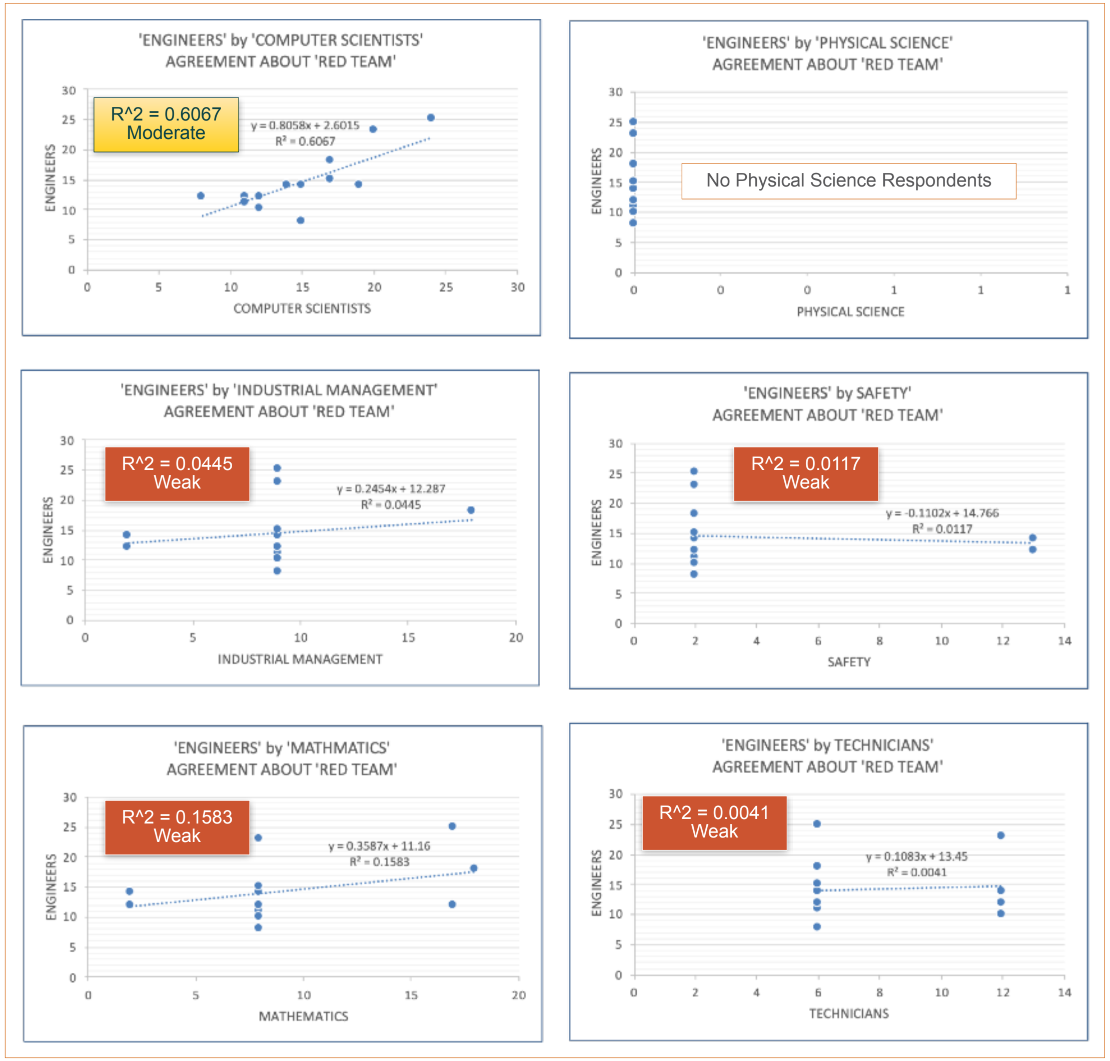


- Figure 9: Engineers by Other Occupation Agreement About KSA, Questions 111 — 166 (Scalco, 2021)

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

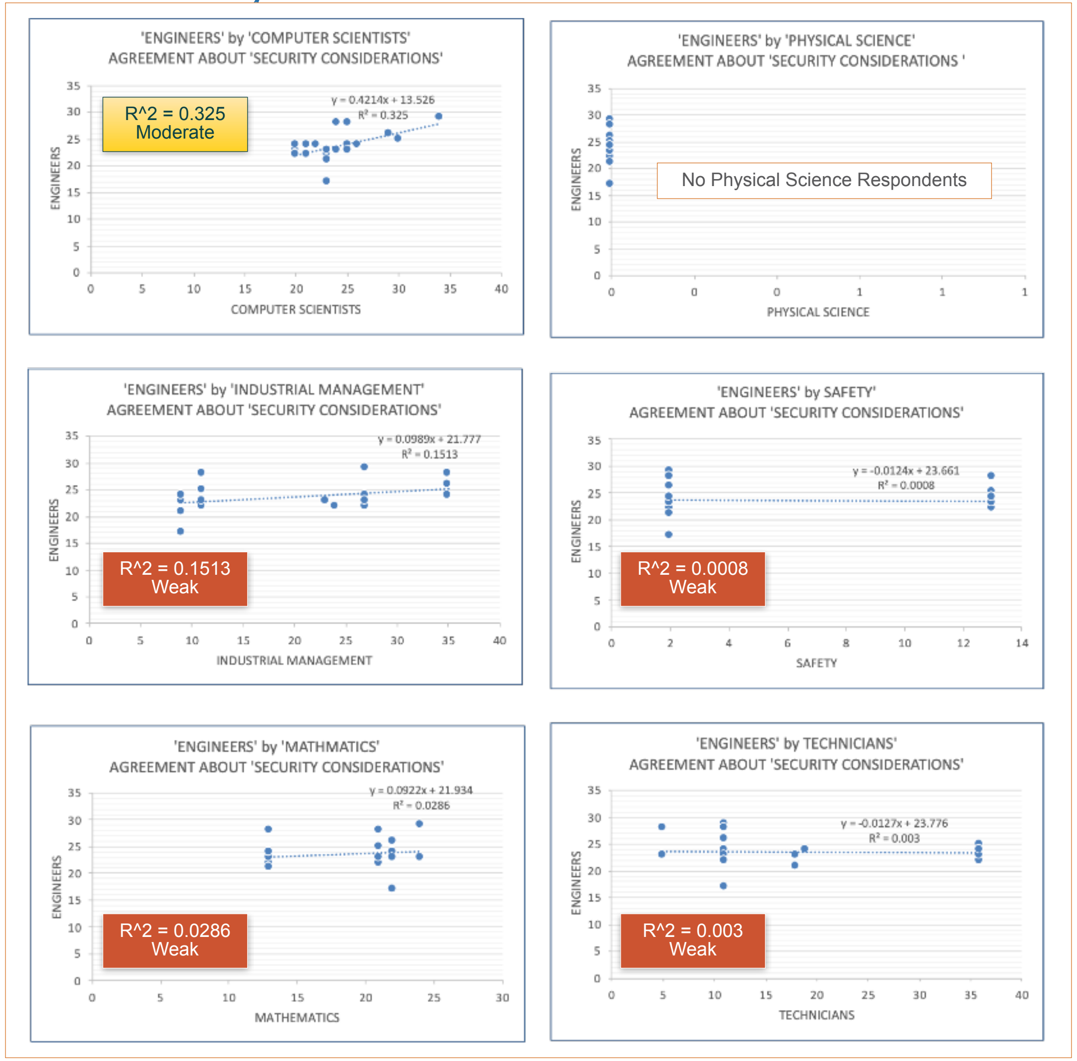
COLORADO STATE UNIVERSITY

Engineers Agreement About Red Team



- Figure 10: Engineers by Other Occupation Agreement About Red Team, Questions 167 — 180 (Scalco, 2021)

Engineers Agreement About Security Considerations

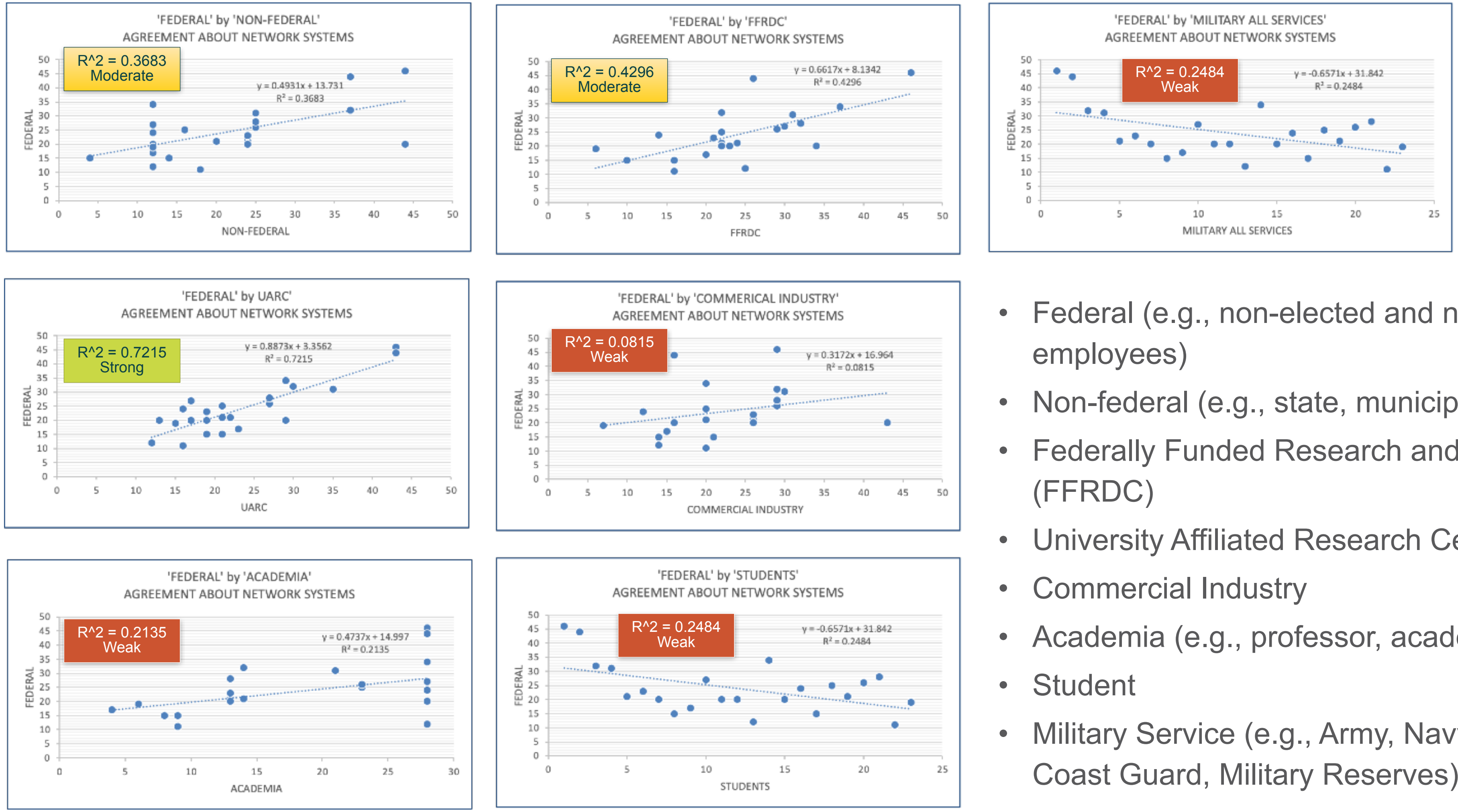


- Figure 11: Engineers by Other Occupation Agreement About Security Considerations, Questions 181 — 203 (Scalco, 2021)

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

Federal Agreement About Network Systems

COLORADO STATE UNIVERSITY



'FEDERAL' by 'NON-FEDERAL' AGREEMENT ABOUT NETWORK SYSTEMS

R^2 = 0.3683 Moderate

'FEDERAL' by 'FFRDC' AGREEMENT ABOUT NETWORK SYSTEMS

R^2 = 0.4296 Moderate

'FEDERAL' by 'MILITARY ALL SERVICES' AGREEMENT ABOUT NETWORK SYSTEMS

R^2 = 0.2484 Weak

'FEDERAL' by UARC' AGREEMENT ABOUT NETWORK SYSTEMS

R^2 = 0.7215 Strong

'FEDERAL' by 'COMMERICAL INDUSTRY' AGREEMENT ABOUT NETWORK SYSTEMS

R^2 = 0.0815 Weak

'FEDERAL' by 'ACADEMIA' AGREEMENT ABOUT NETWORK SYSTEMS

R^2 = 0.2135 Weak

'FEDERAL' by 'STUDENTS' AGREEMENT ABOUT NETWORK SYSTEMS

R^2 = 0.2484 Weak

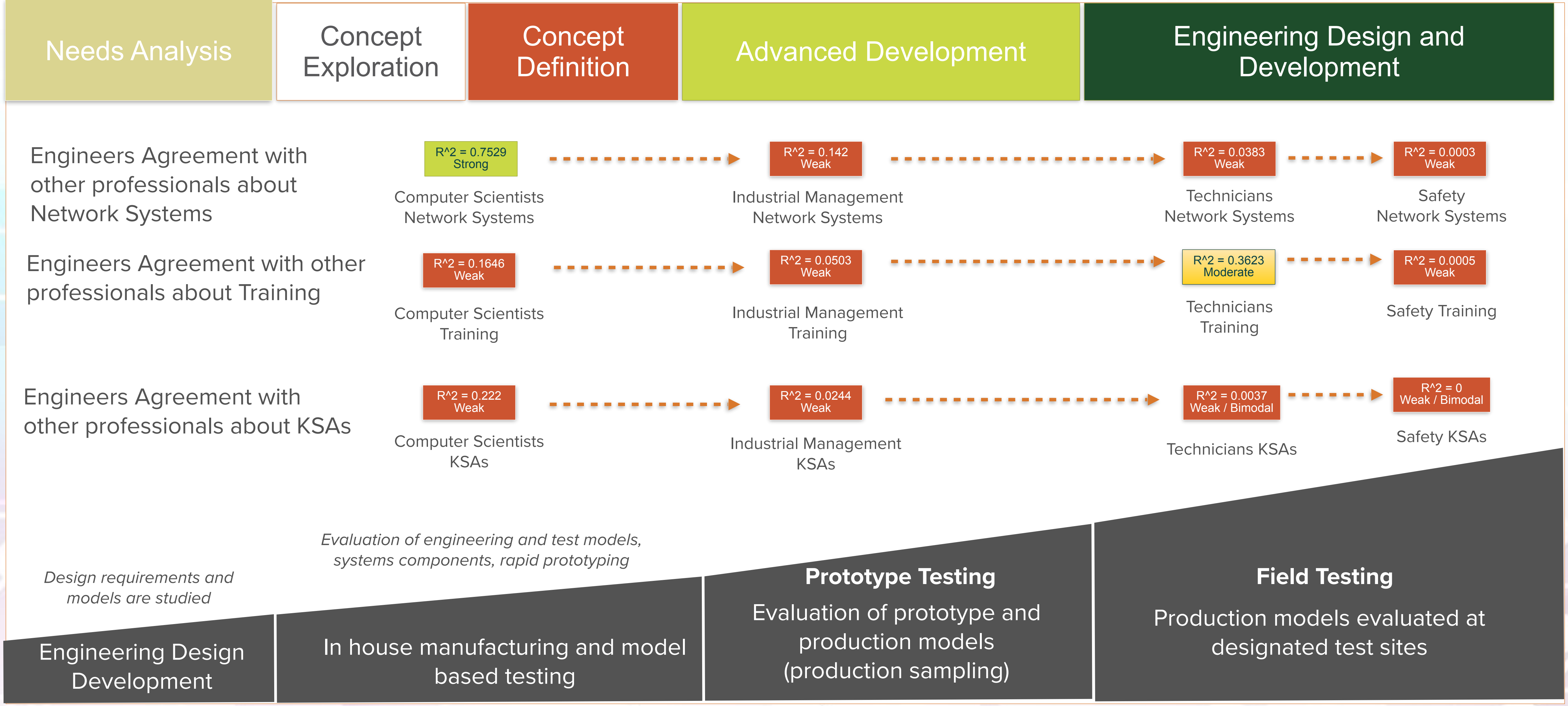
- Federal (e.g., non-elected and non-military public sector employees)
- Non-federal (e.g., state, municipality, local, tribal)
- Federally Funded Research and Development Centers (FFRDC)
- University Affiliated Research Centers (UARC)
- Commercial Industry
- Academia (e.g., professor, academic researcher)
- Student
- Military Service (e.g., Army, Navy, Air Force, Marines, Coast Guard, Military Reserves)

- Figure 12: Federal Agreement About Network Systems, Questions 25 — 47 (Scalco, 2021)

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

Engineers Agreement Through System Lifecycle

COLORADO STATE UNIVERSITY



Needs Analysis | Concept Exploration | Concept Definition | Advanced Development | Engineering Design and Development

	Computer Scientists	Industrial Management	Technicians	Safety
Engineers Agreement with other professionals about Network Systems	R^2 = 0.7529 Strong Computer Scientists Network Systems	R^2 = 0.142 Weak Industrial Management Network Systems	R^2 = 0.0383 Weak Technicians Network Systems	R^2 = 0.0003 Weak Safety Network Systems
Engineers Agreement with other professionals about Training	R^2 = 0.1646 Weak Computer Scientists Training	R^2 = 0.0503 Weak Industrial Management Training	R^2 = 0.3623 Moderate Technicians Training	R^2 = 0.0005 Weak Safety Training
Engineers Agreement with other professionals about KSAs	R^2 = 0.222 Weak Computer Scientists KSAs	R^2 = 0.0244 Weak Industrial Management KSAs	R^2 = 0.0037 Weak / Bimodal Technicians KSAs	R^2 = 0 Weak / Bimodal Safety KSAs

Design requirements and models are studied

Engineering Design Development

Evaluation of engineering and test models, systems components, rapid prototyping

In house manufacturing and model based testing

Prototype Testing

Evaluation of prototype and production models (production sampling)

Field Testing

Production models evaluated at designated test sites

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

OV-1 Operational Concept Network Systems (r2)

Where correlation is poor, these professionals <u>will be at odds</u>.

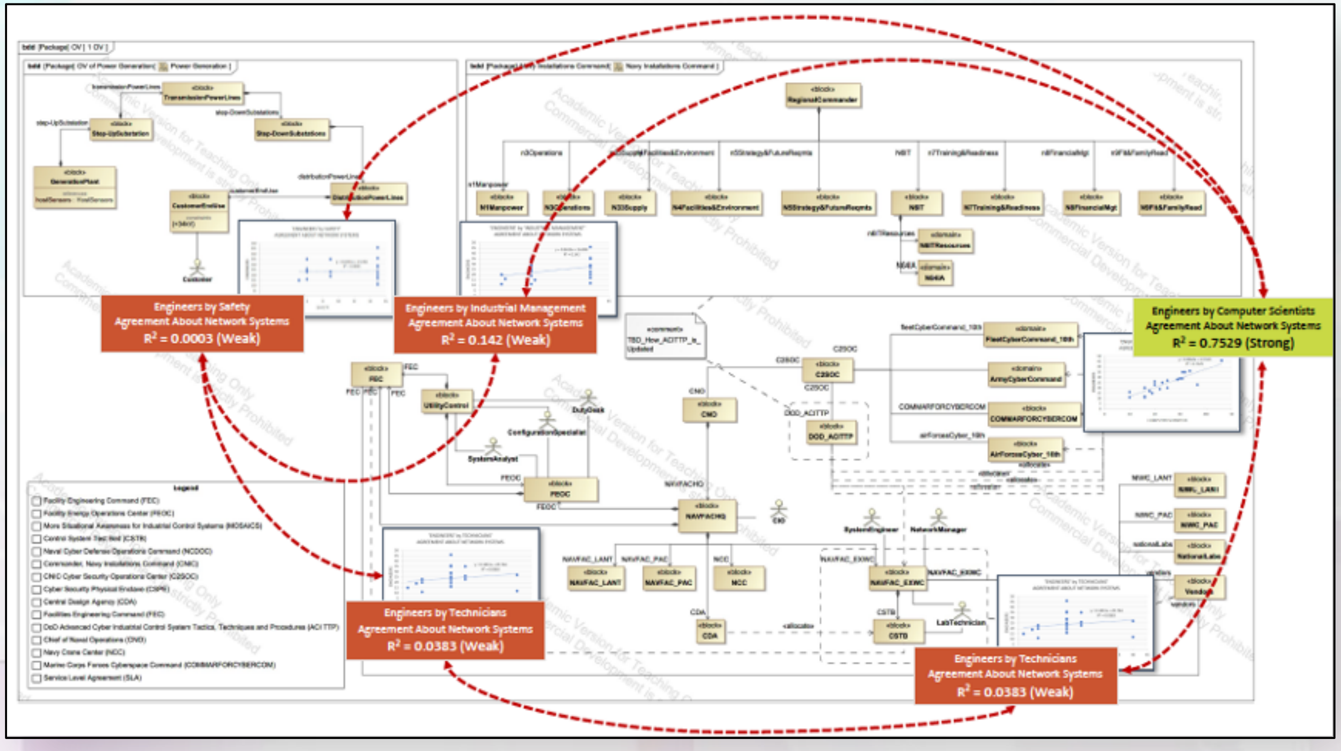

bdd [Package] OV [1 OV]
bdd [Package] OV of Power Generation [Power Generation]
bdd [Package] Navy Installations Command [Navy Installations Command]
RegionalCommander
N1Manpower
N3Operations
N33Supply
N4Facilities&Environment
N5Strategy&FutureReqmts
N6IT
N7Training&Readiness
N8FinancialMgt
N9FA&FamilyReadi
N6ITResources
NSIIA
TransmissionPowerLines
Step-UpSubstation
Step-DownSubstations
GenerationPlant
CustomerEndUse
DistributionPowerLines
Customer
Engineers by Safety
Agreement About Network Systems
$R^2 = 0.0003$ (Weak)
Engineers by Industrial Management
Agreement About Network Systems
$R^2 = 0.142$ (Weak)
Engineers by Computer Scientists
Agreement About Network Systems
$R^2 = 0.7529$ (Strong)
Engineers by Technicians
Agreement About Network Systems
$R^2 = 0.0383$ (Weak)
Engineers by Technicians
Agreement About Network Systems
$R^2 = 0.0383$ (Weak)
TBD_How_ACITTP_is_Updated
FEC
UtilityControl
DutyDesk
ConfigurationSpecialist
SystemsAnalyst
FEOC
CNO
C2SOC
DOD_ACITTP
FleetCyberCommand_10th
ArmyCyberCommand
COMMARFORCYBERCOM
AirForcesCyber_16th
NAVFACHQ
CIO
SystemsEngineer
NetworkManager
NAVFAC_LANT
NAVFAC_PAC
NCC
NAVFAC_EXWC
CDA
CSTB
LabTechnician
NWC_LANT
NWC_PAC
NationalLabs
Vendor
Legend
□ Facility Engineering Command (FEC)
□ Facility Energy Operations Center (FEOC)
□ More Situational Awareness for Industrial Control Systems (MOSAICS)
□ Control System Test Bed (CSTB)
□ Naval Cyber Defense Operations Command (NCDOC)
□ Commander, Navy Installations Command (CNIC)
□ CNIC Cyber Security Operations Center (C2SOC)
□ Cyber Security Physical Enclave (CSPE)
□ Central Design Agency (CDA)
□ Facilities Engineering Command (FEC)
□ DoD Advanced Cyber Industrial Control System Tactics, Techniques and Procedures (ACI TTP)
□ Chief of Naval Operations (CNO)
□ Navy Crane Center (NCC)
□ Marine Corps Forces Cyberspace Command (COMMARFORCYBERCOM)
□ Service Level Agreement (SLA)

Figure 13: BDD Prototype OV-1 High-Level Operational Concept Showing R^2 About Network Systems

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

Water Treatment Facility

- 2018 Legislation, funds never appropriated
- Water Utility “self-assessments.”
- Yet not required to submit any report.
- Systems >3,300 customers exempt

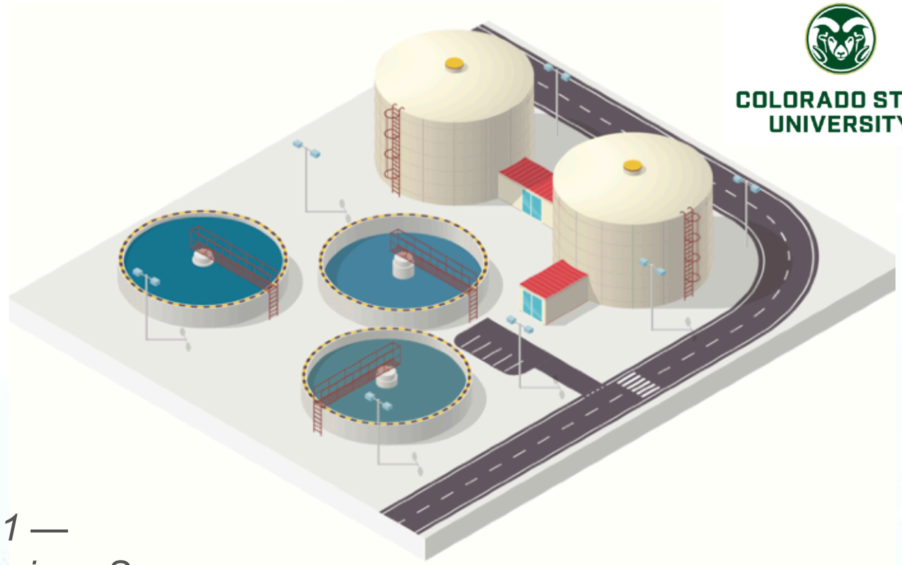
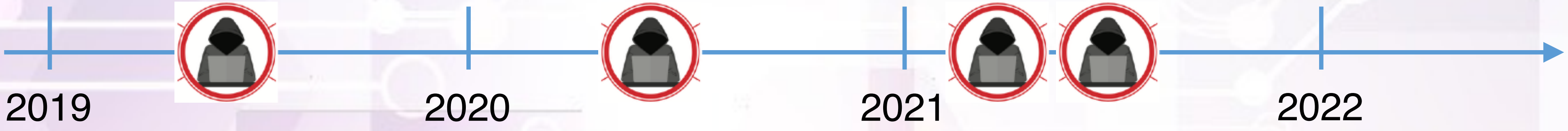


Image: Shutterstock, Shutterstock.com, 2021.

- *2019 — Former employee attempted to shut down water treatment cleaning and disinfecting operations.*
- *2020 — Camrosa Water District, California, infected with ransomware.*
- *January 15, 2021 — Hacker tried to poison San Francisco Bay Area water treatment plant.*
- *February 9, 2021 — Hacker tried to poison the Tampa area water treatment plant in Oldsmar, Florida.*

If there is disagreement among professions, self-assessment might not solve the problem.



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

[16] COLLIER, K. 2021. 50,000 security disasters waiting to happen: The problem of America's water supplies. *NBC News.* NBC News.

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

Use Case — Protect

Table 11 Use Case Protect Capability Mapped to Operational Requirement and Sample Survey Questions

Requirement Number	Operational Requirement Text	Capability	Sample Cybersecurity Survey Question(s) (Response Options)
O2.1	Enable and support access control mechanisms within the environment.	Protect	Q47. User accounts and credentials are managed in our organization by the following authentication approach. (Modern Authentication; Cloud Identity Authentication; Federated Authentication; I do not know.)
O2.2	Authenticate authorized devices, users, and processes.	Protect	Q120. I [can] to identify if an individual device is being tampered with within a complex system. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.3	Implement controls to limit access to physical and logical assets.	Protect	Q136. I [can] identify cyber connections to critical physical systems. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.4	Protect data in transit and data at rest.	Protect	Q58. In our organization, timestamp data is used to reference persistent time-based trends. (Yes; No; I do not know.)
O2.5	Manage maintenance activities for system components.	Protect	Q130. I ensure that maintenance procedures or workarounds do not void anomaly detection in control systems. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.6	Create and manage audit logs.	Protect	Q140. In my current job function, I use data collected from a variety of cyber defense tools (e.g., Intrusion Detection System (IDS) alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.7	Enable facility operations to maintain a mission capable state.	Protect	Q. 186. Traditional statistical forecasting strategies (e.g., dynamic regression) are used in our organization as a baseline for prediction of network performance. (Yes; No; I do not know.)

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

Remote Operations, Assistance, Alarms

Requirement Number	Operational Requirement Text	Capability	Sample Cybersecurity Survey Question(s) (Response Options)
O2.1	Enable and support access control mechanisms within the environment.	Protect	Q47. User accounts and credentials are managed in our organization by the following authentication approach. (Modern Authentication; Cloud Identity Authentication; Federated Authentication; I do not know.)

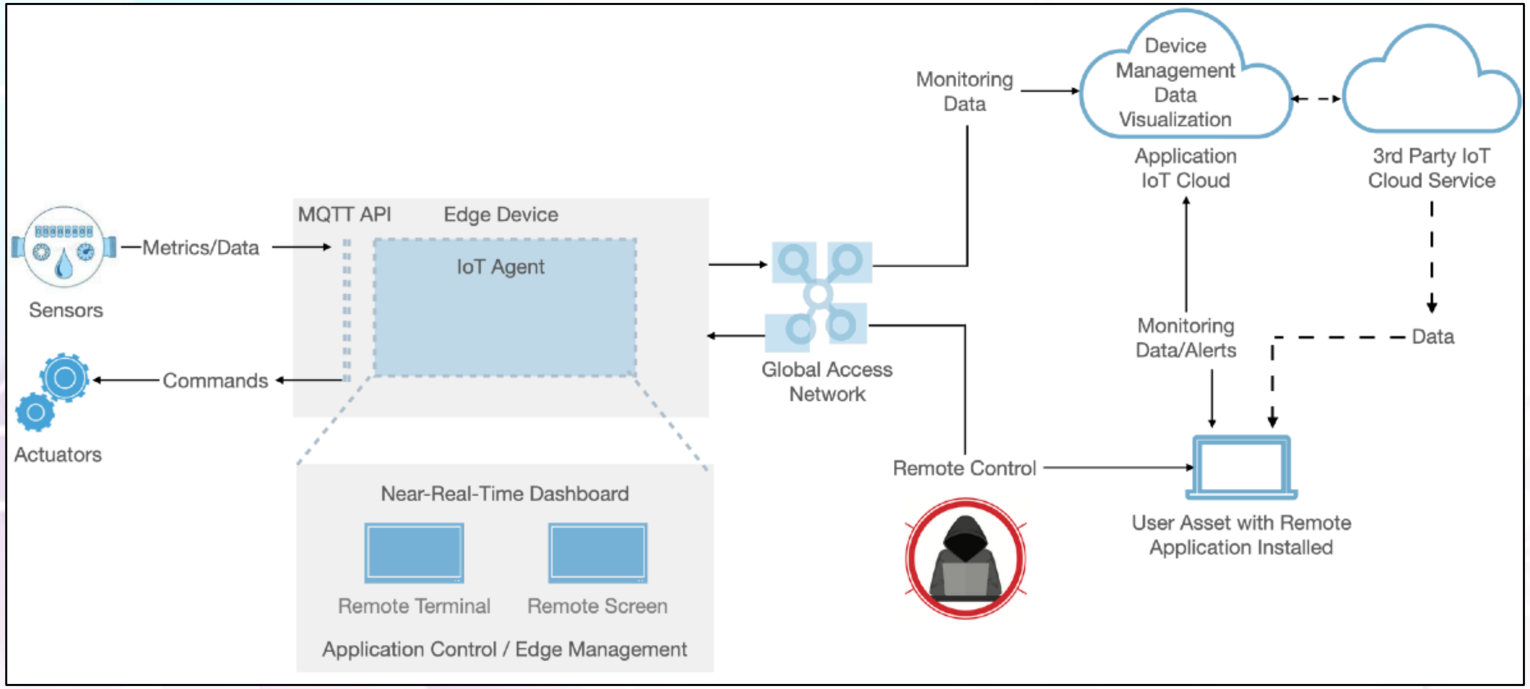
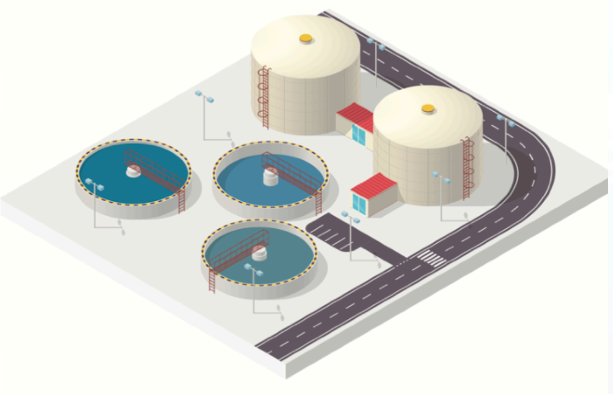


Figure 14: Remote Operations Network Architecture for Water Utility



Water Utility Intrusion Commonality:

Remote Access

Compromised Passwords

Outdated, end-of-life Operating System (OS)

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

Image: Shutterstock, Shutterstock.com, 2021.

INCOSE

Control System Cybersecurity Priorities

COLORADO STATE UNIVERSITY

Disagreement ➡ Misalignment ➡ Vulnerability

Administrative Password Used on Multiple Systems

VPN Account Allows Remote Access / Threat Actor Obtains Credentials

Compromised Credentials Enable Unauthorized Access

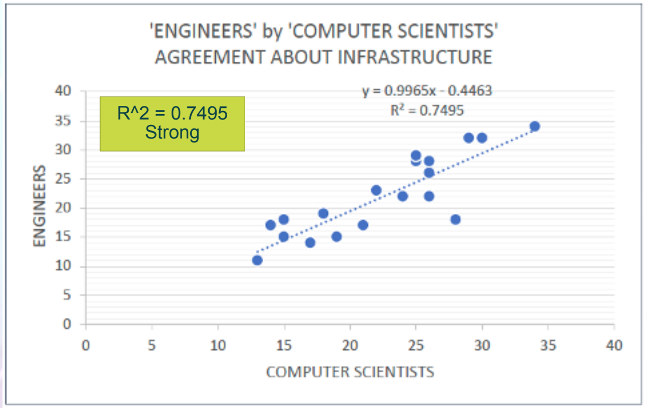


Figure 15: Correlation between Engineers and Computer Scientists about Infrastructure Questions

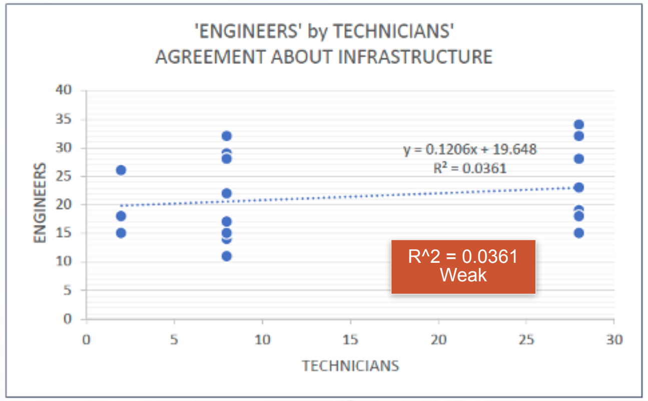


Figure 16: Correlation between Engineers and Technicians about Infrastructure Questions

Software Flaws

Purchase Updated Operating System (OS)

Update Software

Perform Regular Software Updates

Credential Mangement

Vulnerability ➡ Alignment ➡ Agreement

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

Image: Shutterstock, Shutterstock.com, 2022.

COLORADO STATE UNIVERSITY

Red Team (r2) by Infrastructure Sector

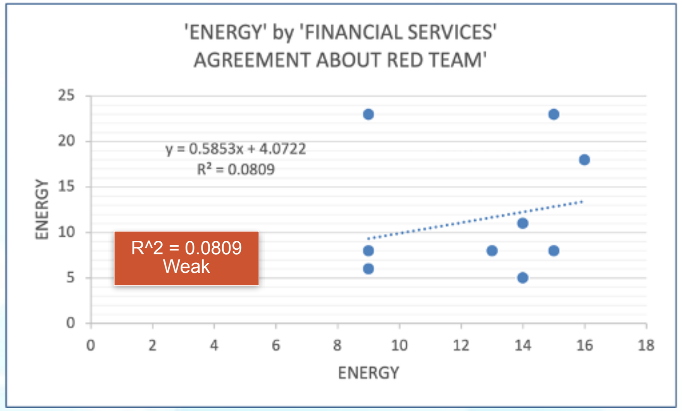


Figure 17: Correlation between Energy and Financial Services for Red Team Questions

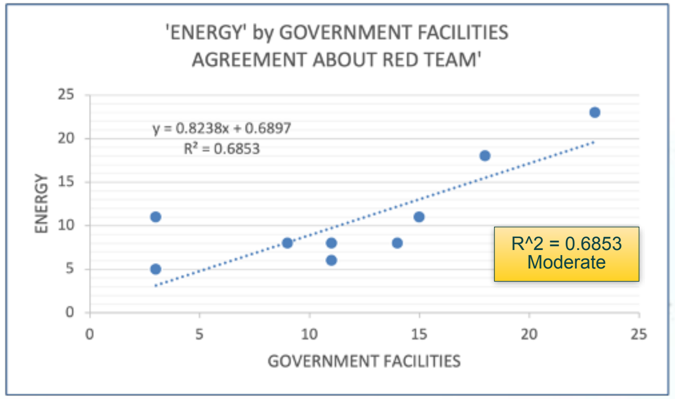


Figure 18: Correlation between Energy and Government Facilities for Red Team Questions

- If someone is trying to defend something that someone else is not attacking, using the Red Team/Blue Team analog, we do not have alignment.
- We know that people are throwing money at these things and not fixing them.

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

Image: Shutterstock, Shutterstock.com, 2022.

Competing Professions

- If two agents disagree entirely on where the system is most vulnerable or uncertain, there is an overall vulnerability.

Requirement Number	Operational Requirement Text	Capability	Sample Cybersecurity Survey Question(s) (Response Options)
O1.1	Inventory IT and OT system devices and system components in the targeted environment.	Identify	Q48. I have access to the physical network topology. (Yes; No; I do not, but I know who does have the physical network topology.)
O1.2	Identify internal and external data flows and connections relative to the target environment.	Identify	Q191. Sensitive network connections between traffic sources and points of encryption are monitored on our organization's network systems. (Yes; No; I do not know.)
O1.3	Enable prioritization of components and system devices.	Identify	Q111. I maintain configuration management of a Control System(s). (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)

Disagreement → Misalignment → Vulnerability

The vulnerability induced by misalignment may be greater than innate system design vulnerability.

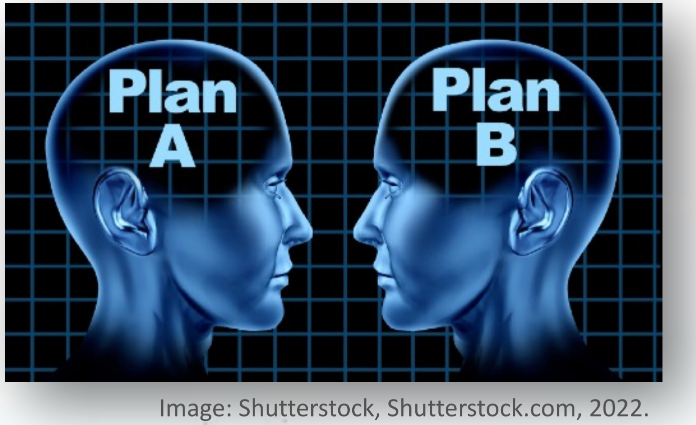
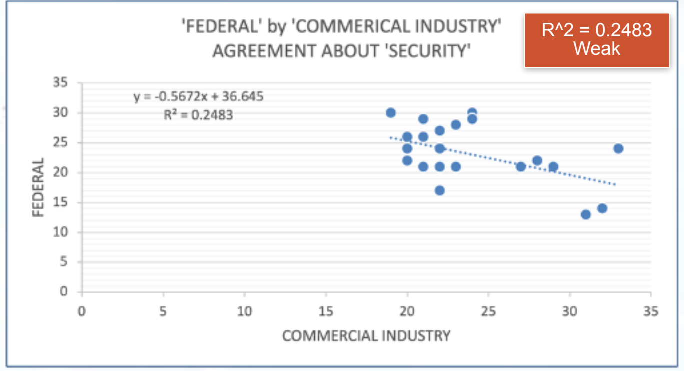
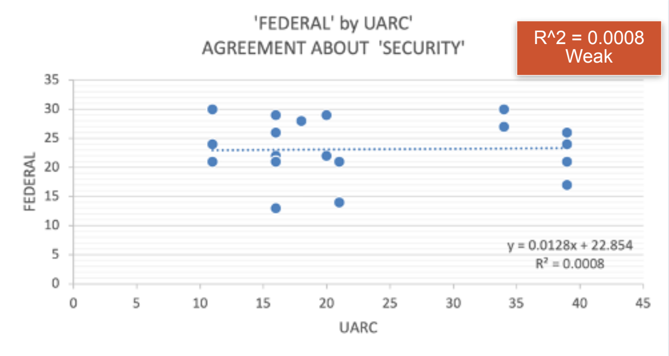


Image: Shutterstock, Shutterstock.com, 2022.



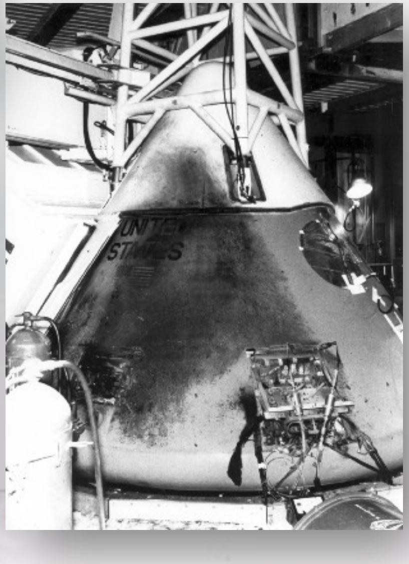
- Figure 19: Federal Agreement by Commercial Industry About Security Considerations (Scalco, 2021)



- Figure 20: Federal Agreement by UARC About Security Considerations (Scalco, 2021)

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

Engineering Value in Disagreement



- **Human Life and Safety**

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

Images: NASA, 2022 and Shutterstock, Shutterstock.com, 2022.

Disagreement — Misalignment — Vulnerability

The vulnerability induced by misalignment may be greater than innate system design vulnerability.

Measuring disagreement in segments of the cybersecurity profession is a means of identifying vulnerabilities.

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

Image: Shutterstock, Shutterstock.com, 2022.

Vulnerability — Alignment — Agreement

The vulnerability induced by misalignment may be greater than innate system design vulnerability.

Measuring disagreement in segments of the cybersecurity profession is a means of identifying vulnerabilities.

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

Image: Shutterstock, Shutterstock.com, 2022.

Command and Control (C2) of Control Systems.

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

Image: Shutterstock, Shutterstock.com, 2021.

INCOSE

COLORADO STATE UNIVERSITY

Thank you!

Questions?

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

References

[1] Department of Defense (DOD), Acquisition Notes, “JCIDS Process,” 2021. URL: https://acqnotes.com/acqnote/acquisitions/cjcsi-3170 [retrieved March 2021].

[2] BARANEK, D. Origins of Topgun. HistoryNet.

[3] PEDERSEN, D. 2019. Topgun An American Story, New York, Hachette Books.

[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[BIDEN, P. J. 2022a. Executive Order on Improving the Nation’s Cybersecurity. In: OFFICE, E. (ed.). Washington, D.C.: Executive Office.

[6] 117th Congress, Congressional Bill, National Defense Authorization Act (NDAA) for Fiscal Year 2022

[7] BIDEN, P. J. 2022b. National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. In: OFFICE, E. (ed.). Washington, D.C.: Executive Office.

[8] TASHEVA, I. 2021. Cybersecurity post-COVID-19: Lessons learned and policy recommendations. *European View*.

[9] RIBEIRO, A. 2021. Ransomware strikes rise sharply, fueled by profit potential. *Industrial Cyber*.

[10] NETWORKS, N. 2021. What You Need to Know to Fight Ransomware and IoT Vulnerabilities Including Recommendations for Enhancing Cyber Resilience. *OT/IoT Security Report.* nozominetworks.com: Nozomi Networks, Inc.[9] NETWORKS, N. 2021. What You Need to Know to Fight Ransomware and IoT Vulnerabilities Including Recommendations for Enhancing Cyber Resilience. *OT/IoT Security Report.* nozominetworks.com: Nozomi Networks, Inc.

[11] TURTON, W. & MEHROTRA, K. 2021. Hackers Breached Colonial Pipeline Using Compromised Password. *Bloomberg*.

[12] 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

[13] SCALCO, A. & SIMSKE, S. 2022. Modeling Uncertainty of Agreement to Achieve Stakeholder Alignment and Overcome Control System Cyber Vulnerability. *In:* INCOSE (ed.) *FuSE.*

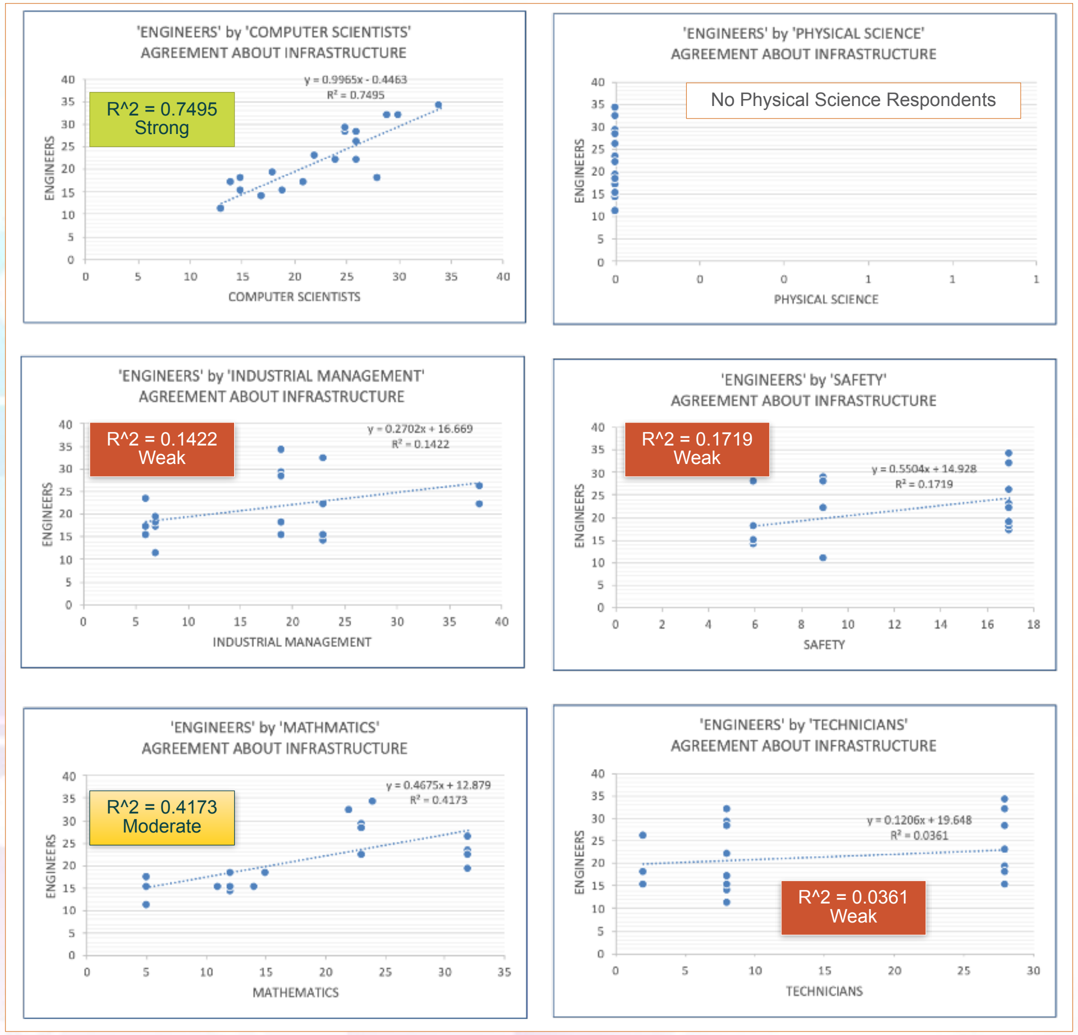
[14] Simske, S. and Scalco, A., “Cyber-physical Systems/Control System (CPS/CS) Workforce Questionnaire,” 2019. Colorado State University (CSU) Institutional Review Board (IRB), Protocol Number 20-102009H.

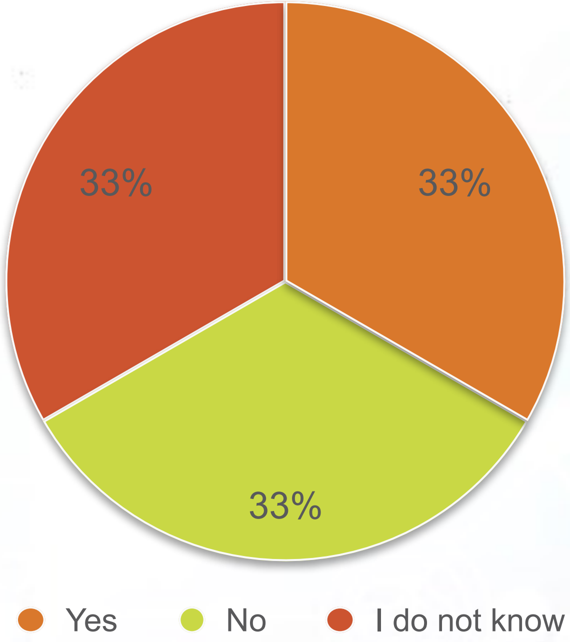
[15] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[16] COLLIER, K. 2021. 50,000 security disasters waiting to happen: The problem of America's water supplies. *NBC News.* NBC News.

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

Q182 Timestamp Data



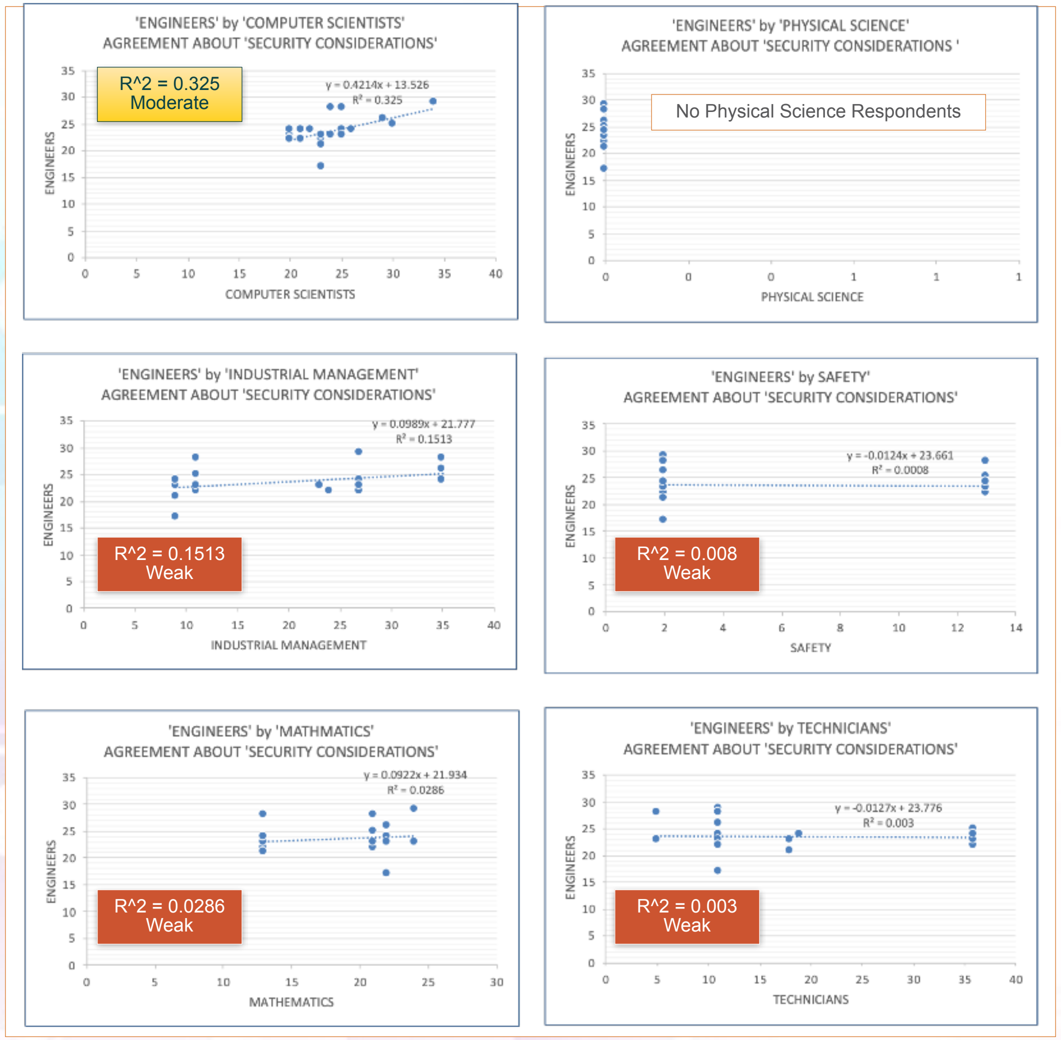


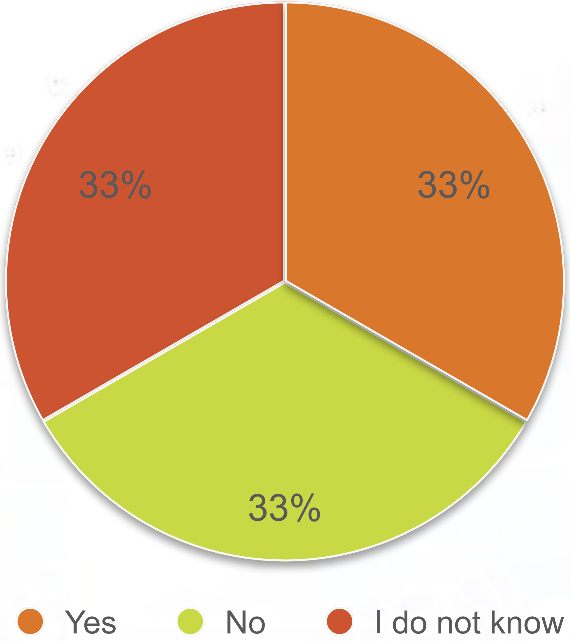
Q182 In my current job function, timestamp data is used to reference persistent time-based trends for OT systems (e.g., cyber-physical systems and control systems.

- Figure 13: Engineers by Other Occupation Agreement About Infrastructure, Questions 48 — 68 (Scalco, 2021)

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

Q202 Software-Defined Networking (SDN)





Q202 Software-Defined Networking (SDN) is implemented in our organization.

- Figure 14: Engineers by Other Occupation Agreement About Security Considerations, Questions 181 — 203 (Scalco, 2021)

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