CISQ
Consortium for IT Software Quality

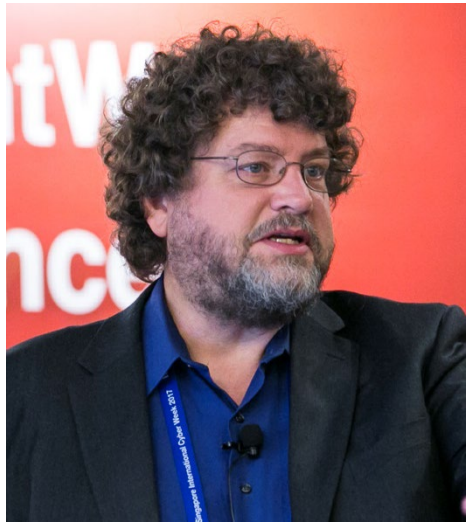
ITAAC
INFORMATION TECHNOLOGY ACQUISITION ADVISORY COUNCIL

INNOVATIVE METHODS FOR PRODUCING CYBERSECURE SOFTWARE

GIRISH SESHAGIRI
EVP and CTO, ISHPI Information Technologies

PAUL SEAY
Northrop Grumman Fellow

BILL NEWHOUSE
Deputy Director, National Initiative for Cybersecurity Education (NICE)



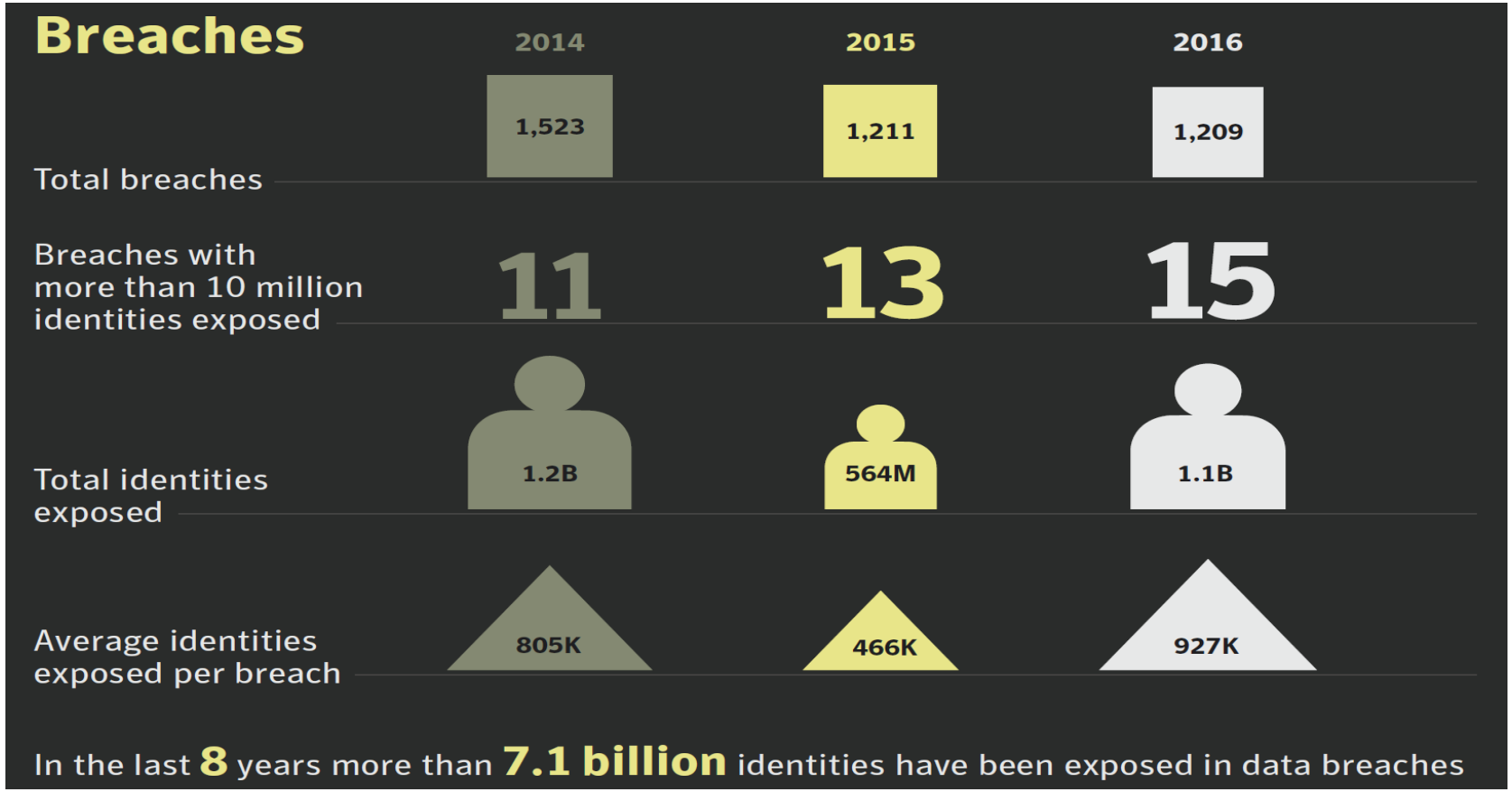
ROBERT MARTIN
Senior Principal Engineer, MITRE

Innovative Methods for Producing Cybersecure Software

Dr. Paul Seay, Northrop Grumman
Robert Martin, MITRE
William Newhouse, NIST/NICE

Moderator: Girish Seshagiri, Ishpi Information Technologies, Inc.

Personal Identity Breaches

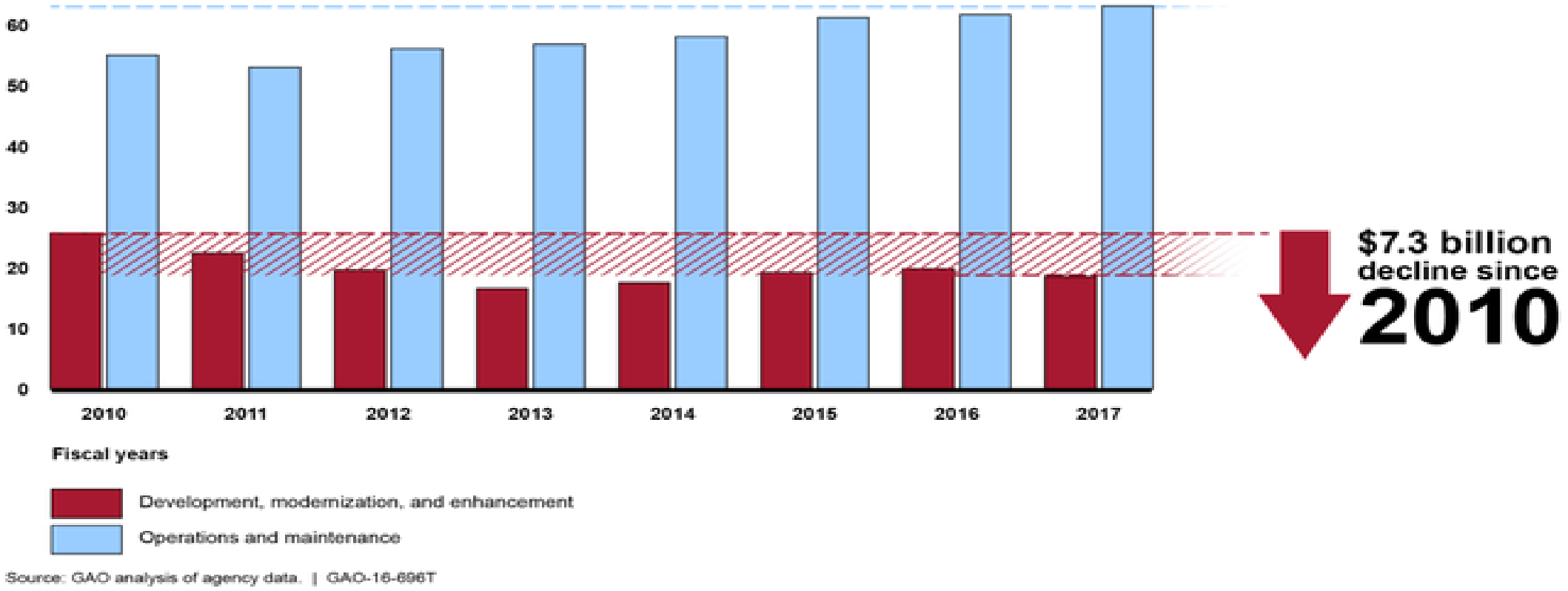


Federal IT Spend in 2015

The **federal** government **spent** more than 75 percent of the total amount budgeted for information technology (IT) for fiscal year 2015 on operations and maintenance (**O&M**) investments. Specifically, 5,233 of the government's approximately 7,000 IT investments are **spending** all of their funds on **O&M** activities.

Source: https://www.gao.gov/assets/680/677436.pdf

Federal IT Spend in 2017



Source: GAO analysis of agency data. | GAO-16-696T

Cybersecurity

- **Defective software** is insecure
  - 90% of attacks are successful by exploiting defects in the software application layer
  - 1 in 20 software defects are vulnerabilities that can be exploited to launch cyberattacks
  - "If you have a quality problem, you have a security problem"
- **Consequences of poor quality software**
  - Impacts - Democracy, loss of life and limb besides just financial loss
  - Potentially more catastrophic than bridge falling down
- Cannot **rely on testing alone** to find and remove software defects
  - Common misconception – "if it passes test, it must be OK"
  - Root cause of "Deliver now, Fix later" culture, technical debt, increase in total ownership cost in many agile projects
- **Reducing vulnerabilities** - number one goal for every agile software team
- High priority national goal to move from reactive to proactive – **from threat detection to threat prevention**

Contact

Girish Seshagiri

girish.seshagiri@ishpi.net

703 426-2790

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The NICE Framework
The National Initiative for Cybersecurity Education (NICE)
Oct 16, 2018

Bill Newhouse, Deputy Director of NICE

Applied Cybersecurity Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)

Accelerate Learning and Skills Development

- *Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers*

Nurture A Diverse Learning Community

- *Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce*

Guide Career Development & Workforce Planning

- *Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent*

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

https://nist.gov/nice

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

Objectives:

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers

3.2 Publish and raise awareness of the NICE Cybersecurity Workforce Framework and encourage adoption

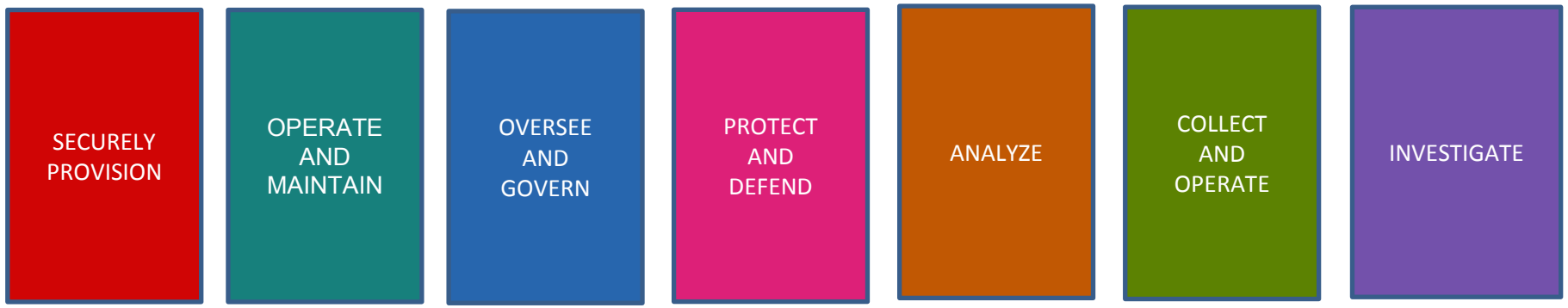
3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals

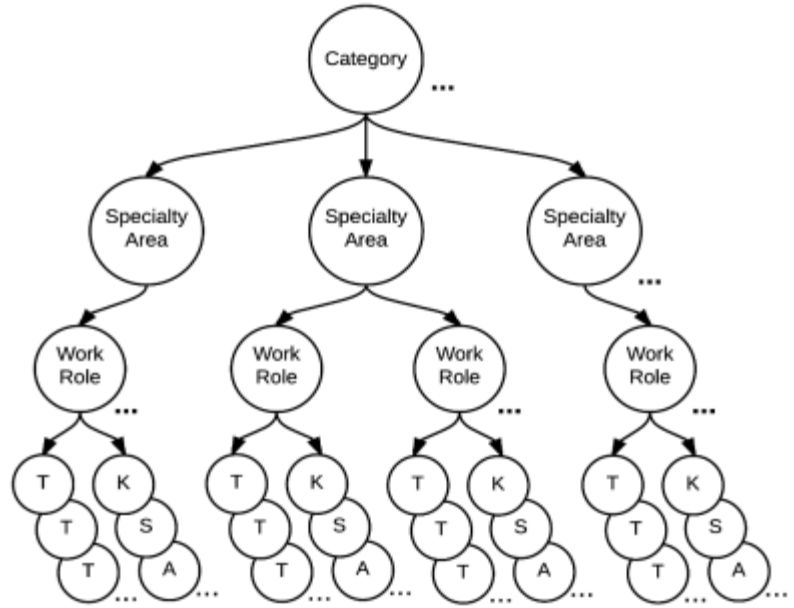
3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning

NICE Framework - https://go.usa.gov/xnXsh

Categories of Cybersecurity Work



- Specialty Areas (33) – Distinct areas of cybersecurity work;
  - Work Roles (52) – The most detailed groupings of IT, cybersecurity or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks.
    - Tasks – Specific work activities that could be assigned to a professional working in one of the NCWF's Work Roles; and,
    - Knowledge, Skills, and Abilities (KSAs) – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.
- Audience:
  - Employers
  - Current and Future Cybersecurity Workers
  - Training and Certification Providers
  - Education Providers
  - Technology Providers



Building Blocks for a Capable and Ready Cybersecurity Workforce

About +
News +
Events +
Resources −
Executive Order 13800
NICE Cybersecurity Workforce Framework
One Pagers
NICE Working Group +
NICE Tutorials
Multimedia

NICE Cybersecurity Workforce Framework

The NICE Framework, NIST Special Publication 800-181, is a national focused resource that categorizes and describes cybersecurity work. The NICE Framework, establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.

The NICE Framework is comprised of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions.
- Specialty Areas (33) – Distinct areas of cybersecurity work.
- Work Roles (52) – The most detailed groupings cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks

NICE Framework Supporting Materials

- NIST Special Publication 800-181, The NICE Cybersecurity Workforce Framework **(August 2017)**
- Reference Spreadsheet for the NICE Framework, NIST SP 800-181 **(January 18, 2018)**
- NICE Framework Revision Process and Documented Revisions

Search the NICE Framework

- **Using Keywords via DHS's Cybersecurity Careers and Training Portal**
- **CyberWatch West database**

Co-Author Resources

Securely Provision (7 Specialty Areas, 11 Work Roles)

Category	Specialty Area	Work Role
Securely Provision	Risk Management	Authorizing Official/Designating Representative
		Security Control Assessor
	Software Development	Software Developer
		Secure Software Assessor
	Systems Architecture	Enterprise Architect
		Security Architect
	Technology R&D	Research & Development Specialist
	Systems Requirements Planning	Systems Requirements Planner
	Test and Evaluation	Testing and Evaluation Specialist
	Systems Development	Information Systems Security Developer
		Systems Developer

Keyword Search

Search Descriptions

A0047: Ability to develop secure software according to secure so...

Apply

Reset

Abilities ID: A0047

Description: Ability to develop secure software according to secure software deployment methodologies, tools, and practices.

Work Roles:

Work Role ID: SP-DEV-001
Work Roles: Software Developer
Work Role Description: Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
Category: Securely Provision
Specialty Area(s): Software Development

Work Role ID: SP-DEV-001

Software Developer

Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Category: Securely Provision **Specialty Area:** Software Development

Abilities

A0007: Ability to tailor code analysis for application-specific concerns.

A0021: Ability to use and understand complex mathematical concepts (e.g., discrete math).

A0047: Ability to develop secure software according to secure software deployment methodologies, tools, and practices.

A0123 : Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

A0170 : Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

Knowledge

K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.

K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

K0004: Knowledge of cybersecurity and privacy principles.

K0005: Knowledge of cyber threats and vulnerabilities.

K0006: Knowledge of specific operational impacts of cybersecurity lapses.

K0014: Knowledge of complex data structures.

K0016: Knowledge of computer programming principles

Tasks

T0009: Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.

T0011: Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.

T0013: Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.

T0014: Apply secure code documentation.

T0022: Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.

T0026: Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.

T0034: Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.

T0040: Consult with engineering staff to evaluate interface between hardware and software.

T0046: Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.

T0057: Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.

T0077: Develop secure code and error handling.

T0100: Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.

T0111: Identify basic common coding flaws at a high level.

T0117: Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.

T0118: Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.

T0171: Perform integrated quality assurance testing for security functionality and resiliency attack.

T0176: Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.

TOP

REDUCING SOFTWARE VULNERABILITY

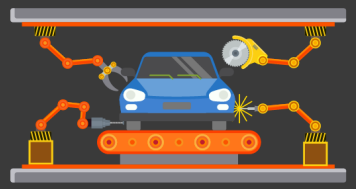
NIST National Institute of Standards and Technology U.S. Department of Commerce

New NIST interagency report (NISTIR) 8151 has five main sets of approaches for reducing vulnerabilities in software. In simple terms, according to NIST's Paul E. Black, these approaches are:

FORMAL METHODS

Math-based verification tools coders can easily apply.

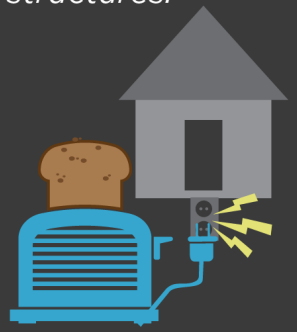
"I drive a car. But even though I know nothing about hi-temperature steel or tire rubber, it just works."



SYSTEM LEVEL SECURITY

Modularizing a computer's programs so if one piece breaks the whole thing doesn't collapse.

"If my toaster breaks it shouldn't fry my house's circuit. But computers don't always have these 'circuit breaker' type structures."



ADDITIVE SOFTWARE ANALYSIS

Connecting analysis tools that currently operate in isolation.

"You get a better suit if the guy who measures your chest and the guy measuring your inseam communicate with each other."

DOMAIN SPECIFIC FRAMEWORKS

Use a more appropriate programming language for the task.

"Why not use a language that has words and concepts and data structures that are specific to that app? In fact they exist and are mature."

MOVING TARGET DEFENSE AND AUTOMATIC SOFTWARE DIVERSITY

"If someone's attacking you, instead of building walls while they find out where you are and drop bombs, it would be nice to be able to pick up and move rather than wait for the airstrike."

Design by Natasha Hanacek/NIST

Useful Links (for use when you get these slides as an event follow-up

- NICE Framework - google “NIST NICE Framework”

Software Quality Group in the Software and Systems Division in Information Technology Laboratory at NIST – google NIST SSD

- National Software Reference Library (NSRL)
- Computer Forensics Tool Verification (CFTT)
- Software Performance
- Software Assurance Metrics And Tool Evaluation (SAMATE)
- Software Assurance Reference Dataset (SARD)
- Computer Forensic Reference Data Sets (CFReDS)

Structured Assurance Case MetaModel

(part of the Innovative Methods for Producing Cybersecure Software Panel)

Robert A. Martin

Sr. Secure Software & Technology Prin. Eng.

Trust & Assurance Cyber Technologies Dept.

Cyber Solutions Technical Center

CISQ Cyber Resilience Summit Oct 16 2018

MITRE

Software & SW-enabled Connected Capabilities Are Throughout Enterprises

Medical

Buildings

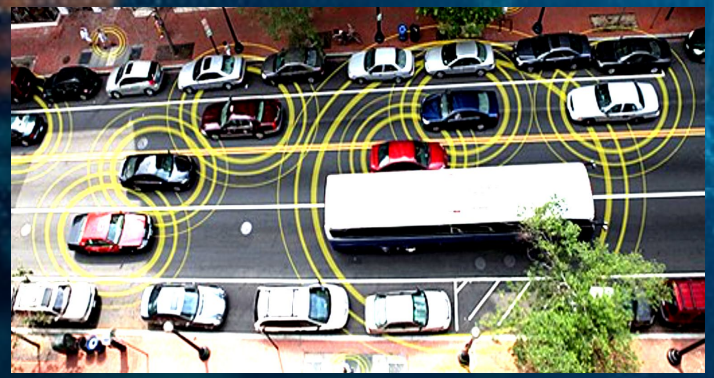
Aeronautics

Manufacturing

Energy

Shipping

Vehicles



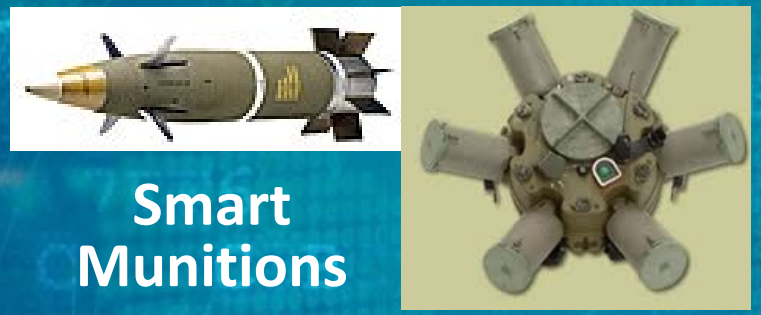
MITRE

Concerns About Software go well beyond IT…

Water Treatment

Status & Health Monitoring

Smart Munitions



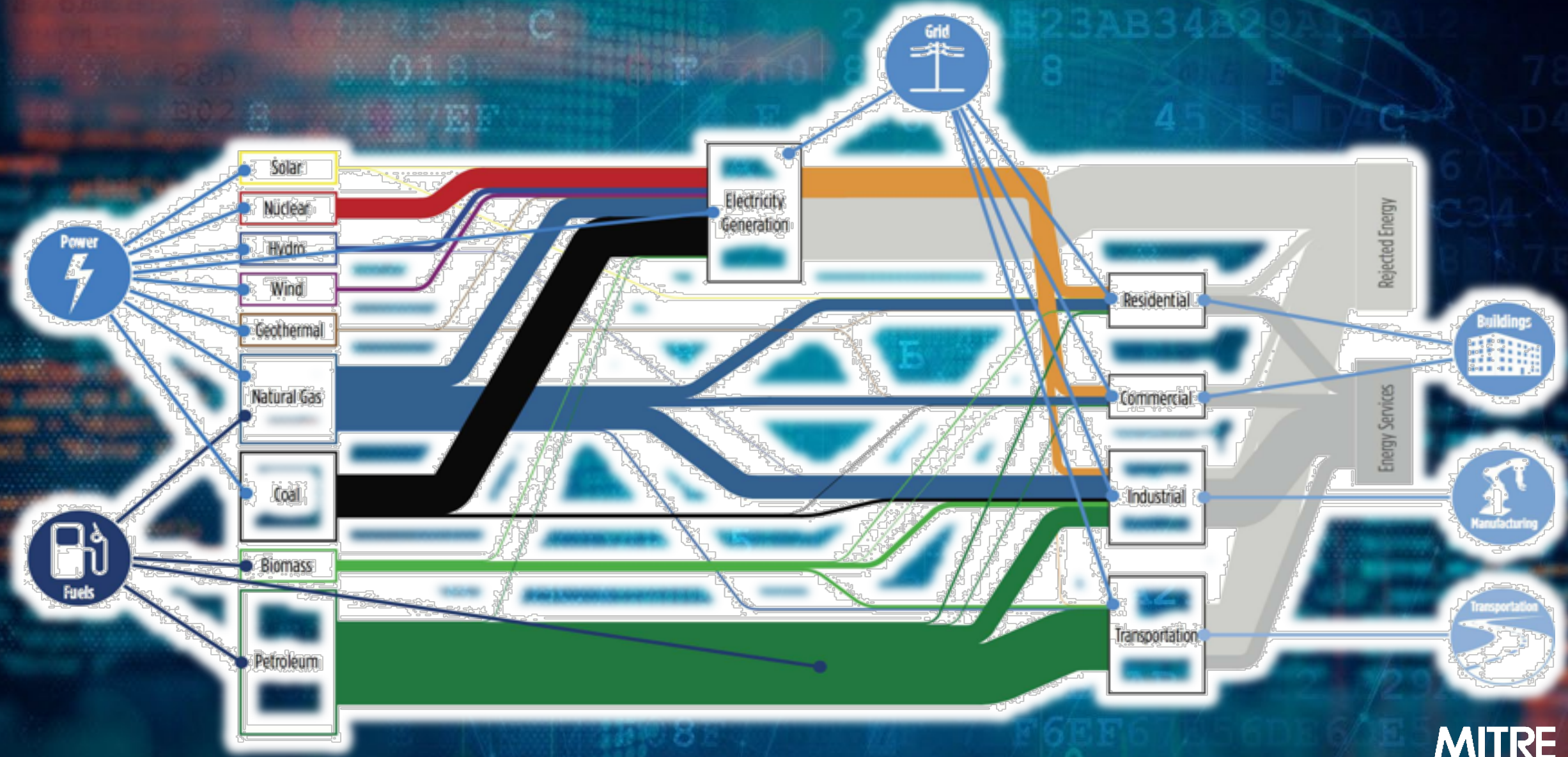
Remote Management

Oil & Gas

Hydro Power & Dam Mngt

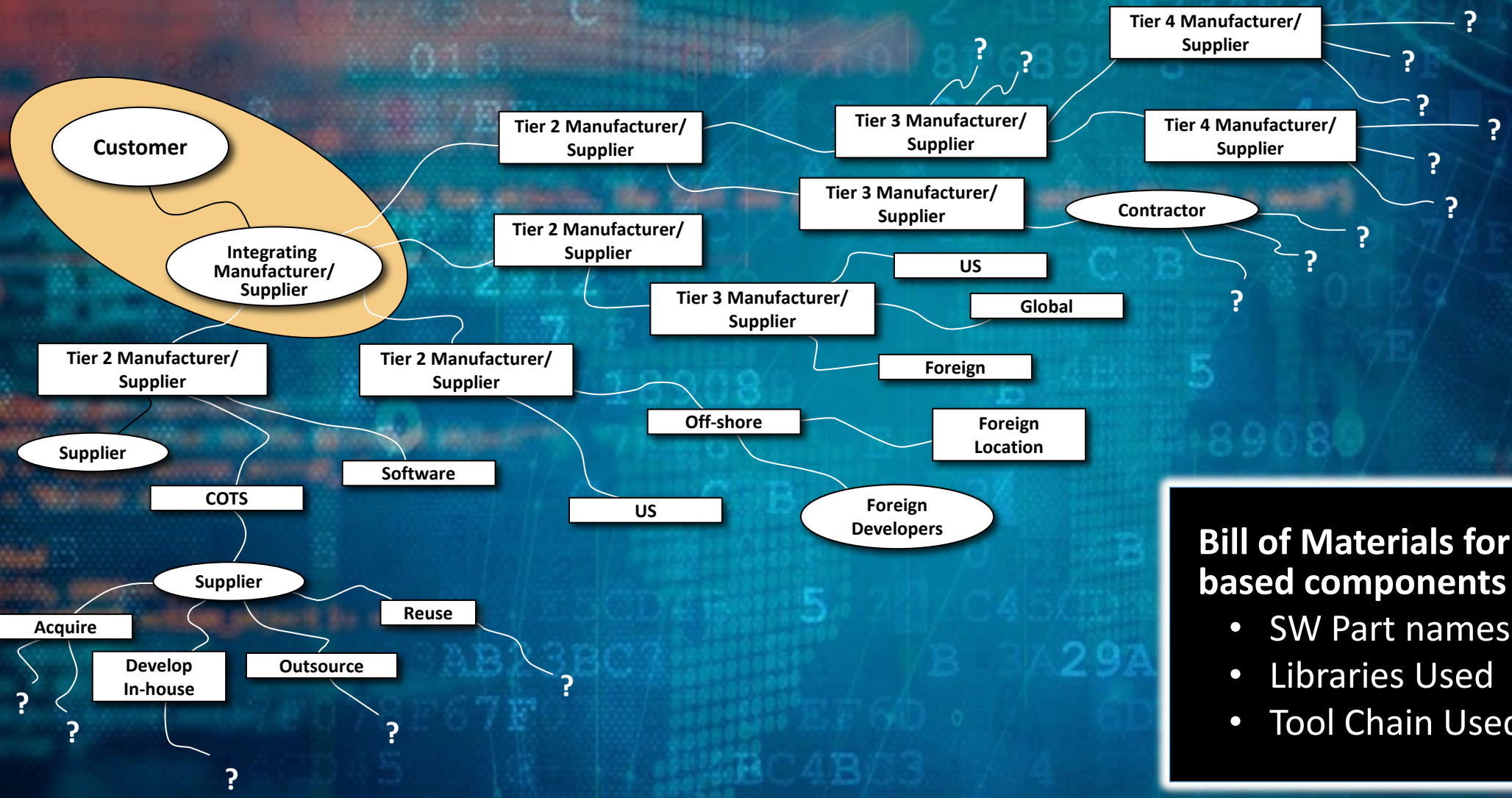
MITRE

Need Standards to Drive Consistency in Discussing and Conveying Assurance due to the Sector-2-Sector linkages



MITRE

The Supply Chain for Software-Enabled Capabilities is Complex

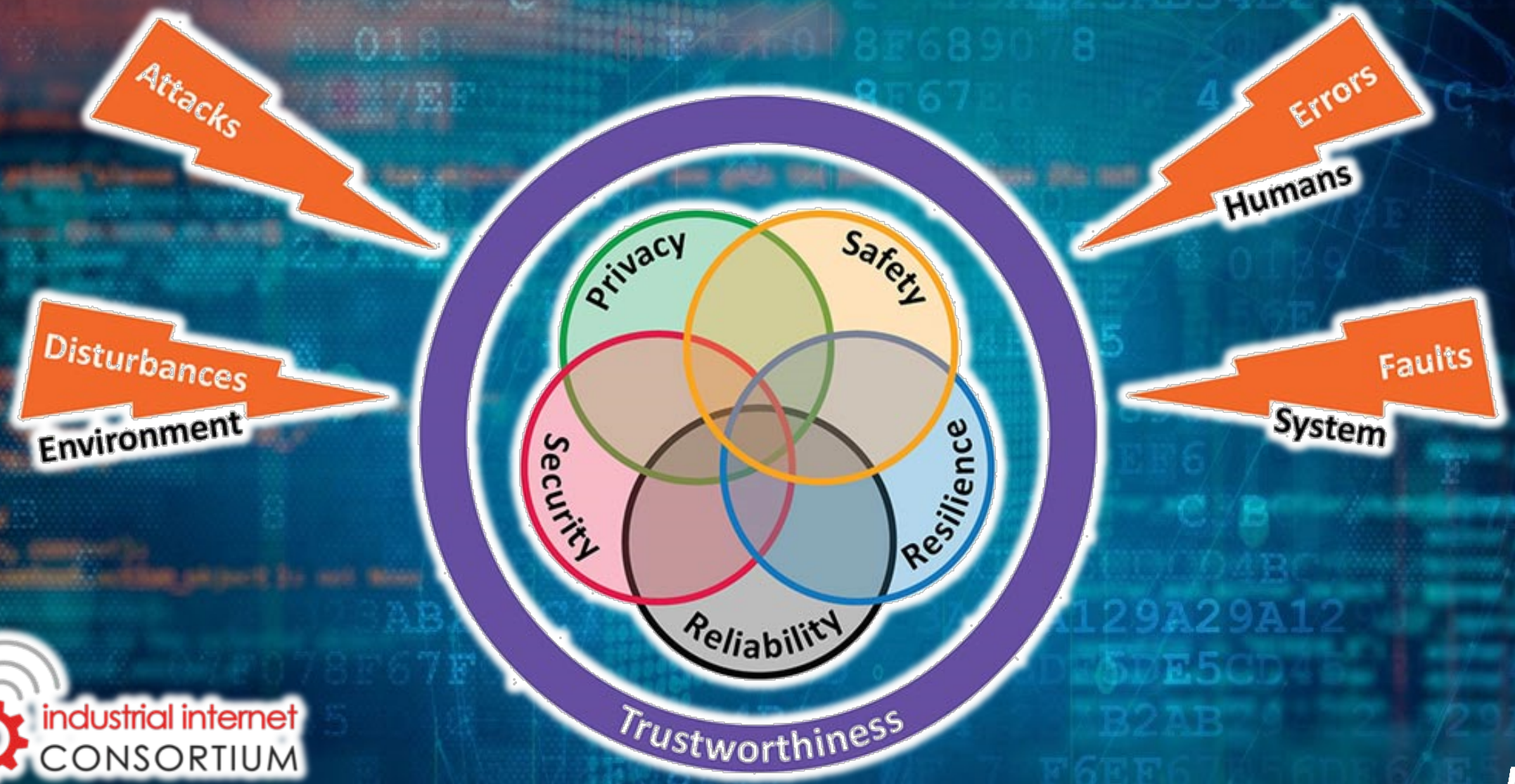


Bill of Materials for software-based components

- SW Part names and versions
- Libraries Used
- Tool Chain Used

MITRE

We Need Assurance of More Than Security – Need Assured Trustworthy Systems

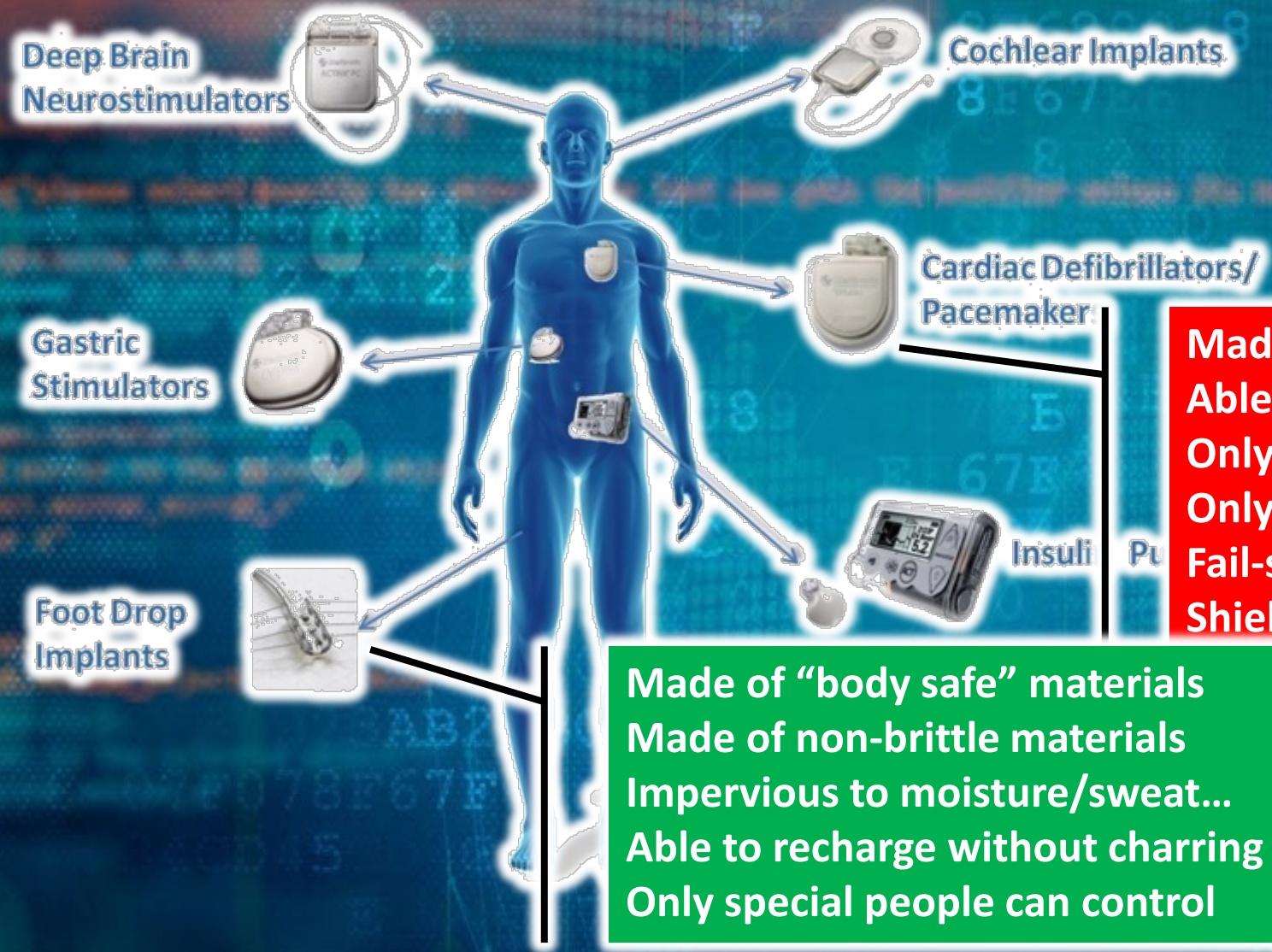


industrial internet CONSORTIUM

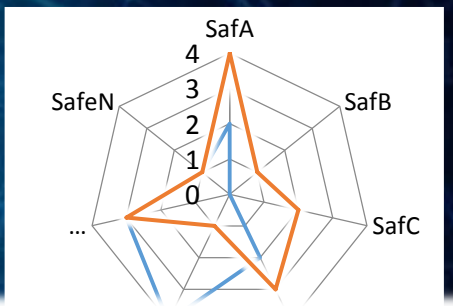
MITRE

Claims of Trustworthiness → Gathering Evidence for Assurance Cases

WIRELESS IMPLANTABLE MEDICAL DEVICES



Safety*



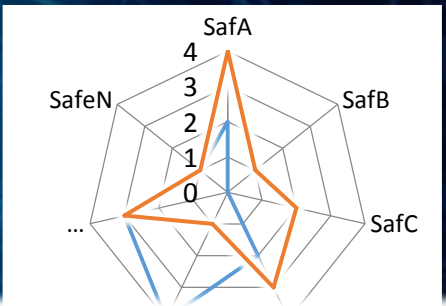
Made of "body safe" materials
Able to recharge without charring skin
Only authorized people can connect
Only special people can control
Fail-safe mode to support life…
Shielded from radiation…

Made of "body safe" materials
Made of non-brittle materials
Impervious to moisture/sweat…
Able to recharge without charring skin
Only special people can control

MITRE

Claims of Trustworthiness → Gathering Evidence for Assurance Cases

Safety*



No interfering with other devices
No off-gassing or hazardous emissions
Only authorized people can connect
Only special people can control
Can be handled w/o special gloves
Fail-safe mode to support life…
Shielded from radiation…
Can be used in a sterilized area
Operational w/o positive control

MITRE

For What it Means to be Safe, A Checklist Will Not Work!

- ❑ Made of “body safe” materials
- ❑ Able to recharge without charring skin
- ❑ Only authorized people can connect
- ❑ Only special people can control
- ❑ Fail-safe mode to support life…
- ❑ Shielded from radiation…
- ❑ Made of non-brittle materials
- ❑ Impervious to moisture/sweat…
- ❑ No interfering with other devices
- ❑ No off-gassing or hazardous emissions
- ❑ Can be handled w/o special gloves
- ❑ Can be used in a sterilized area
- ❑ Operational w/o positive control

Made of “body safe” materials
Made of non-brittle materials
Impervious to moisture/sweat…
Able to recharge without charring skin
Only special people can control

Made of “body safe” materials
Able to recharge without charring skin
Only authorized people can connect
Only special people can control
Fail-safe mode to support life…
Shielded from radiation…

No interfering with other devices
No off-gassing or hazardous emissions
Only authorized people can connect
Only special people can control
Can be handled w/o special gloves
Fail-safe mode to support life…
Shielded from radiation…
Can be used in a sterilized area
Operational w/o positive control

MITRE

But if every System has a “unique” array of requirements how do we manage that?…

MITRE

Group Requirements around “families” of Systems with similar functions, environment, and other context?…

Deep Brain Neurostimulators
Gastric Stimulators
Foot Drop Implants
Cochlear Implants
Cardiac Defibrillators/Pacemakers
Insulin Pumps
Operating Room Equipment
Medical Procedure Support Equipment

MITRE

Infusion Pumps Total Product Life Cycle

Guidance for Industry and FDA Staff

Document issued on: December 2, 2014

The draft of this document was issued on April 23, 2010.

This document supersedes the "Guidance on the Content of Premarket Notification [510(k)] Submissions for External Infusion Pumps," issued March, 1993.

OMB Control Number: 0910-0766
Expiration Date: 5/31/2017

For questions regarding this document, please c
Branch, Office of Device Evaluation at 301-796

For questions regarding safety assurance cases,
Devices Branch, Office of Device Evaluation at
richard.chapman@fda.hhs.gov.

For questions regarding pre-clearance inspectio
Ear/Nose/Throat, General Hospital, Infectious
Compliance at 301-796-5770 or via email at fra

For questions pertaining to manufacturer report
301-796-6104 or via email at sharon.kapsch@f

Center for Devices and Radiological Health
CDRH

- The technological features of the devices.

You should describe how any differences in technology may affect the comparative safety and performance of your device.

5. Safety Assurance Case

Infusion pump 510(k) submissions typically include changes or modifications to software, materials, design, performance, or other features compared to the predicate. Accordingly, FDA expects that most new devices (as well as most changed or modified devices[5]) will have differences in technological characteristics from the legally marketed predicate device even if sharing the same intended use. Under section 513(i) of the Federal Food, Drug, and Cosmetic Act (the FD&C Act), determinations of substantial equivalence will rely on whether the information submitted, including appropriate clinical or scientific data, demonstrate that the new or modified device is as safe and effective as the legally marketed predicate device and does not raise different questions of safety and effectiveness in comparison to the predicate device.

In determining whether your new, changed, or modified infusion pump is substantially equivalent, FDA recommends that you submit your information through a framework known as a safety assurance case.[6]

The safety assurance case (or safety case) consists of a structured argument, supported by a body of valid scientific evidence that provides an organized case that the infusion pump adequately addresses hazards associated with its intended use within its environment of use. The argument should be commensurate with the potential risk posed by the infusion pump, the complexity of the infusion pump, and the familiarity with the identified risks and mitigation measures.

[5] Based on FDA's analysis of these devices, FDA expects that most changes or modifications to infusion pumps could significantly affect the safety or effectiveness of the devices and would therefore require submission of a new 510(k). See 21 CFR 807.81(a)(3). Note that a change to the intended use or technology of a 510(k)-cleared device may render the device not substantially equivalent (NSE) to a legally marketed predicate. For detailed information about substantial equivalence and 510(k) submissions, refer to the FDA guidance entitled, *The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications [510(k)]* (http://www.fda.gov/downloads/MedicalDevices/.../UCM284443.pdf). Any such device may thus be a class III device and require a premarket approval application (PMA), unless the device is reclassified under section 513 of the Federal Food, Drug, and Cosmetic Act.

[6] For more information about assurance case reports, see, for example: Graydon, P., J. Knight, and E. Strunk, "Assurance Based Development of Critical Systems," Proc. of 37th Annual International Conference on Dependable Systems and Networks, Edinburgh, U.K., 2007; Kelly, T., *Arguing Safety — A Systematic Approach to Managing Safety Cases*, Ph.D. Dissertation, University of York, U.K., 1998; Kelly, T., "Reviewing Assurance Arguments - A Step-by-Step Approach," Proc. of Workshop on Assurance Cases for Security - The Metrics Challenge, Dependable Systems and Networks, July 2007; Kelly, Tim, and J. McDermid, "Safety Case Patterns – Reusing Successful Arguments," Proc. of IEE Colloquium on Understanding Patterns and Their Application to System Engineering, London, Apr. 1998; Weinstock, Charles B. and Goodenough, John B., "Towards an Assurance Case Practice for Medical Devices," Carnegie Mellon Software Engineering Institute, October 2009; Hawkins, Richard, et. al., *A New Approach to Creating Clear Safety Arguments*, Safety-critical Systems Symposium, Southampton, UK, February 2011; UK Ministry of Defence, Defence Standard 00-56, *Safety Management Requirements for Defence Systems – Part 1 and Part 2*, June 2007.

Support for Safety Case Generation via Model Transformation

Chung-Ling Lin, Wuwei Shen
Department of Computer Science
Western Michigan University
Kalamazoo, MI, USA
{chung-ling.lin, wuwei.shen}@wmich.edu

Richard Hawkins
Department of Computer Science
The University of York
York, UK
richard.hawkins@york.ac.uk

ABSTRACT
Assessing the saf
systems under ever
confidence is a gr
able. One method
the use of assuranc
little or too much al
affect confidence
automatic generatio
expedite a develop
perform compliance
framework which
metamodel, and a
generate a safety a
conformance of the
use the GPCA infus
this framework can
pump guidance pub

Keywords
Compliance check
systems; safety case

1. INTRODU
Assessing the safe
systems, such as
constraints with an
challenge for indust
to address this is
safety case in short
Administration (FD
guidance document
pumps [2], which
use safety assurance
organize and presen
claims of their infus
infusion pump gu
automatically consis

The construction an
system are a chal

SIGBED Rev

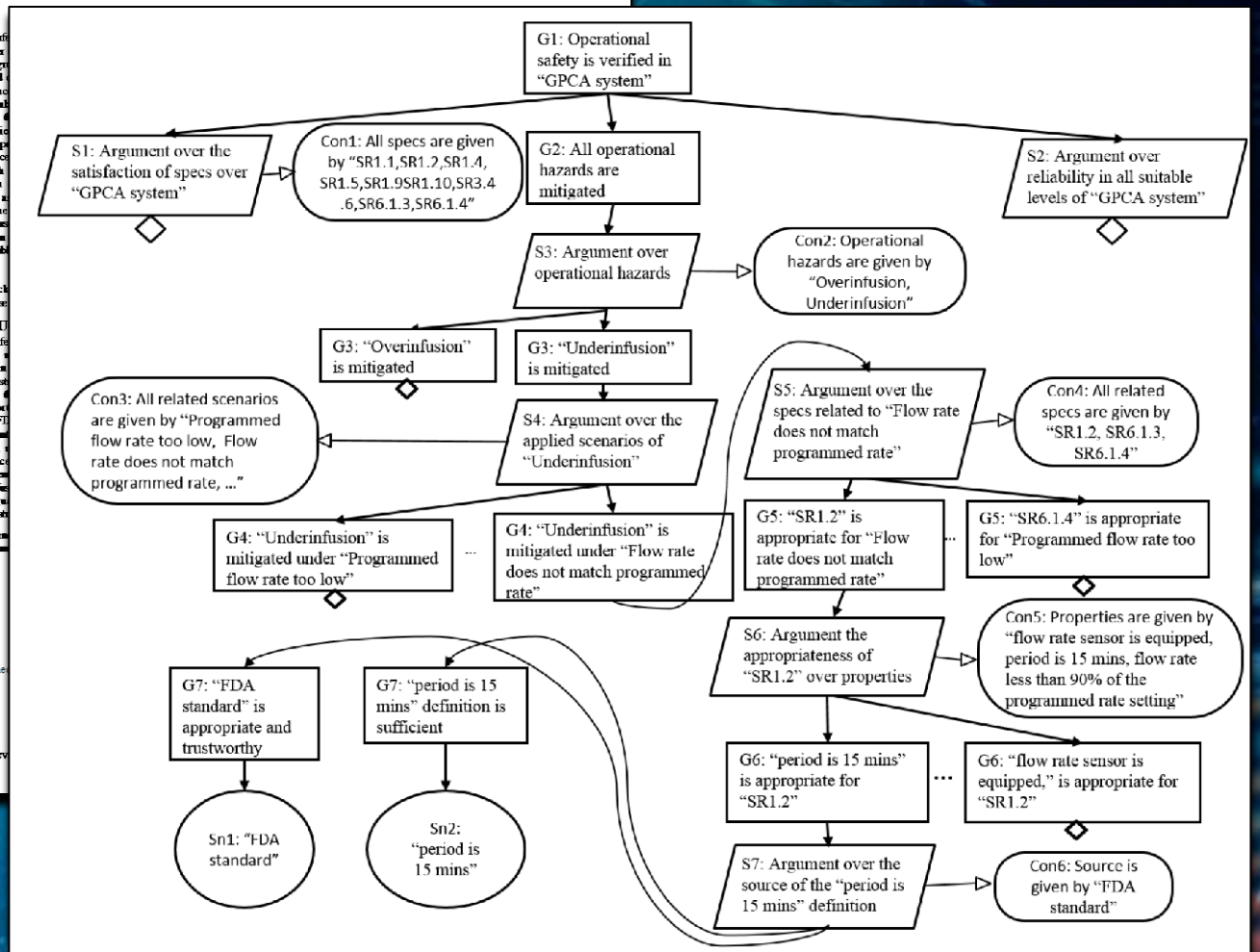
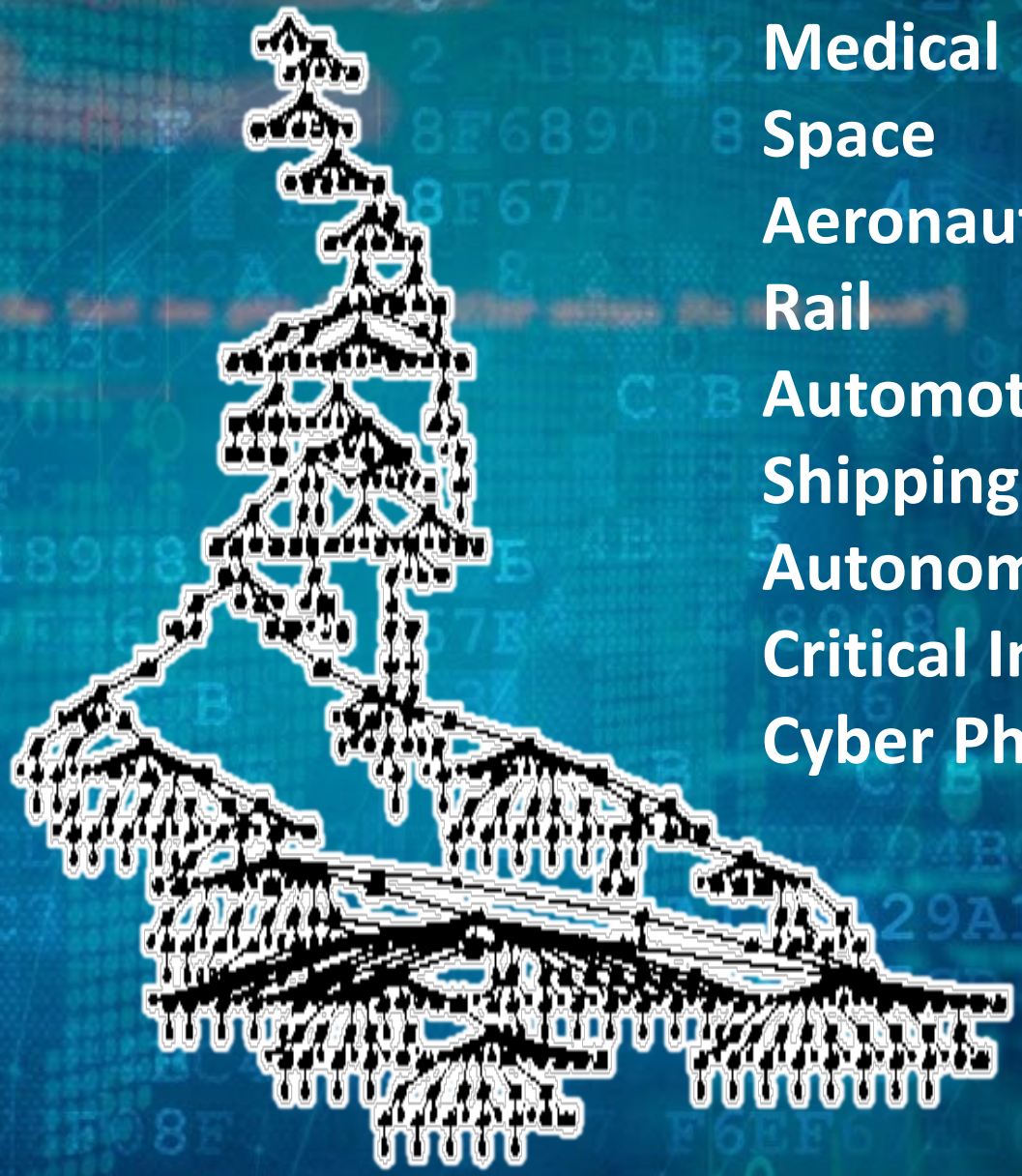


Figure 9 Safety case model of GPCA system

MITRE

The Assurance Case



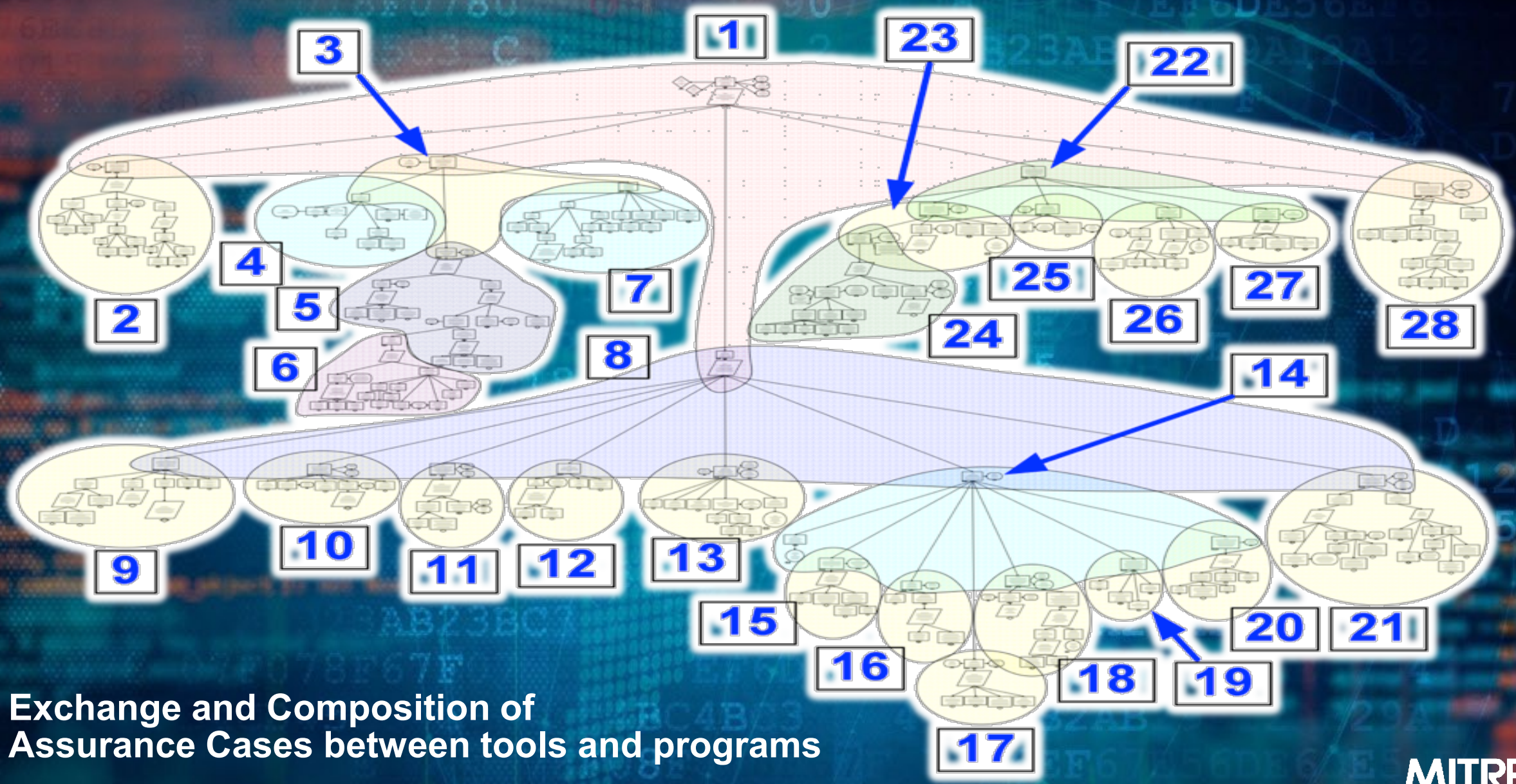
- Medical
- Space
- Aeronautics
- Rail
- Automotive
- Shipping
- Autonomous
- Critical Infrastructure
- Cyber Physical Systems…

DEIS
Dependability Engineering Innovation for Cyber Physical Systems

CITADEL
CRITICAL INFRASTRUCTURE PROTECTION USING ADAPTIVE MILS

MITRE

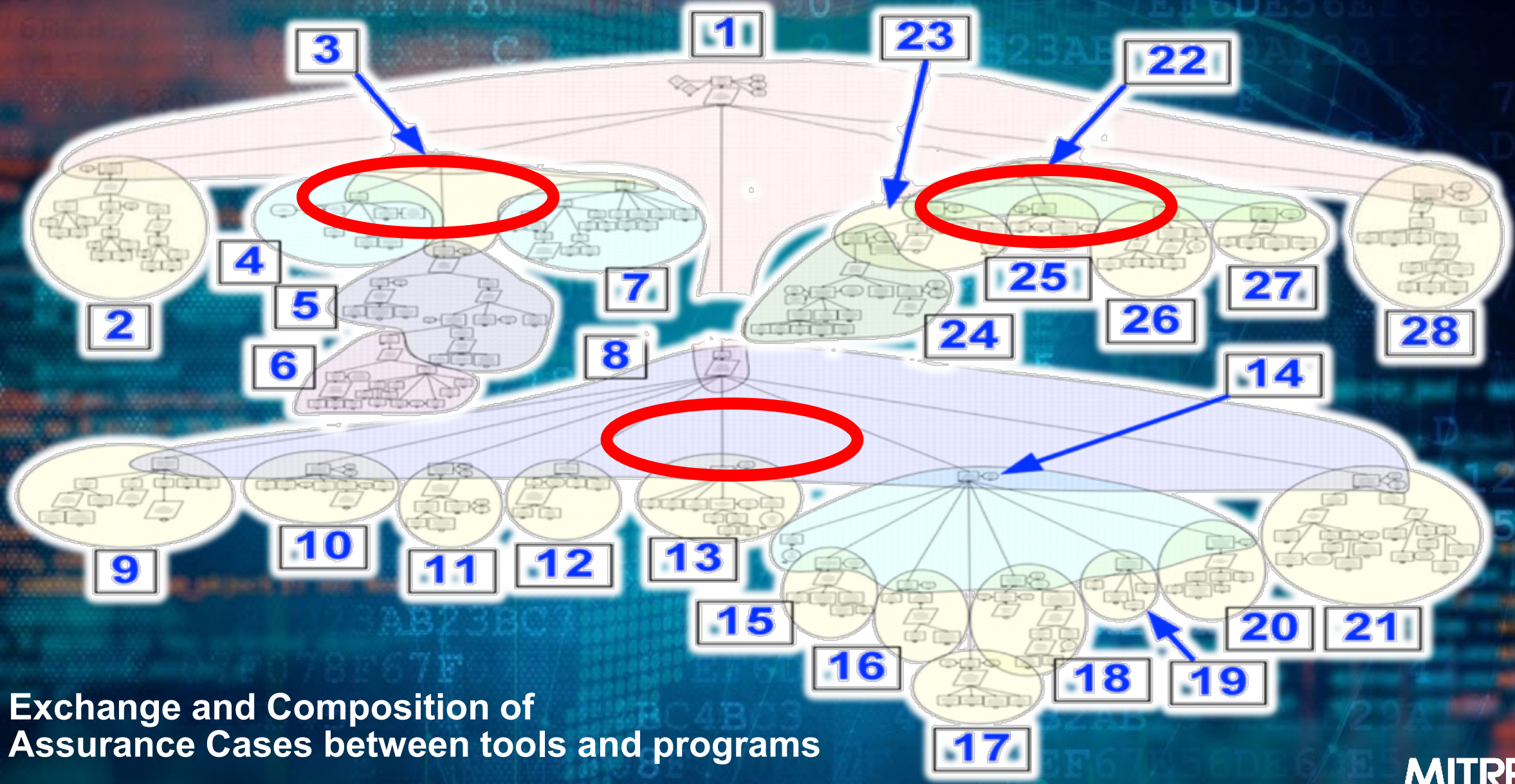
The Assurance Case for a System Builder using Assured Components



Exchange and Composition of Assurance Cases between tools and programs

MITRE

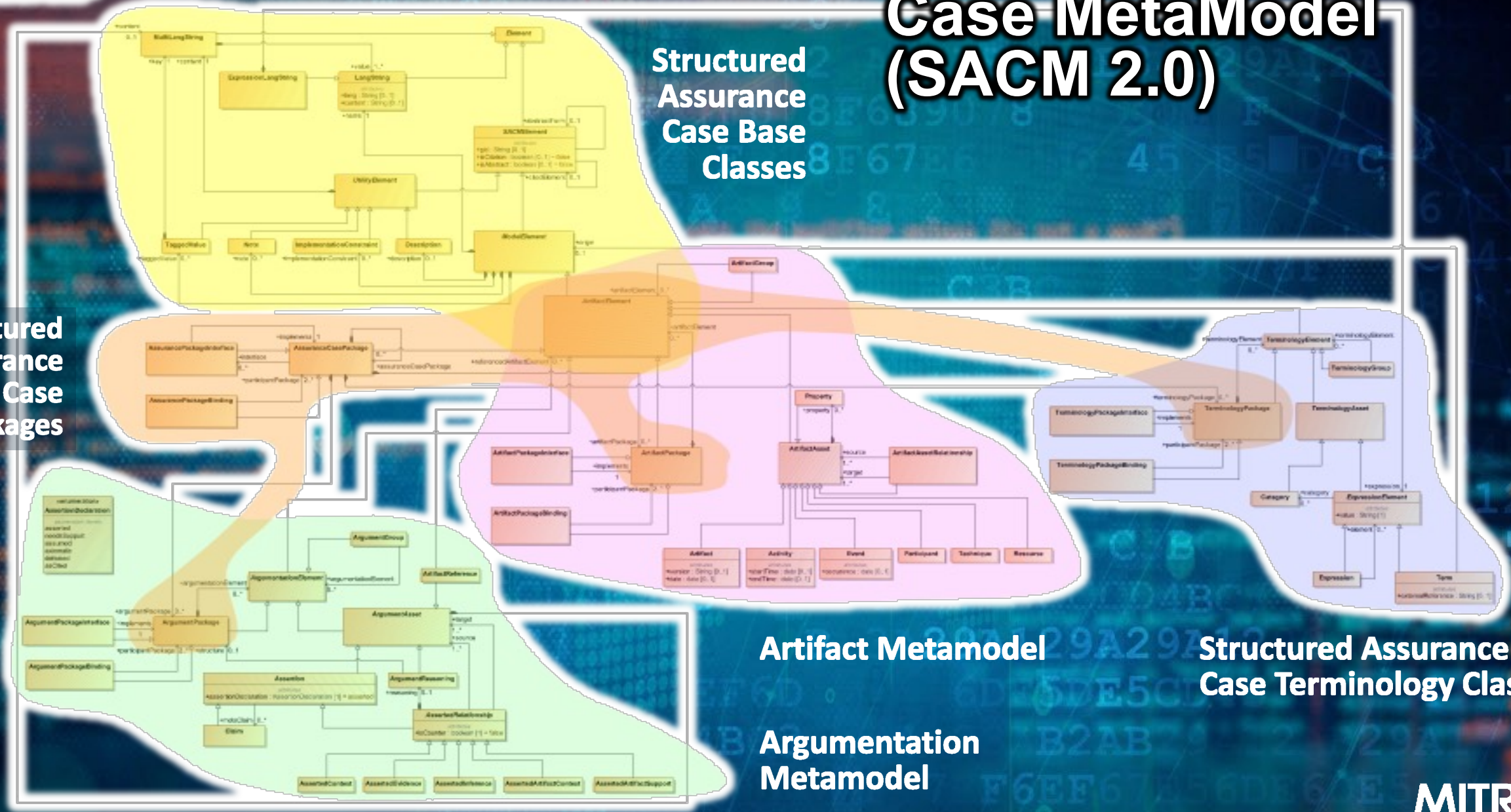
The Assurance Case for a System Builder using Assured Components



Exchange and Composition of Assurance Cases between tools and programs

MITRE

Structured Assurance Case MetaModel (SACM 2.0)



Questions?

IIC Journal of Innovation – September 2018 issue on Trustworthiness
https://www.iiconsortium.org/journal-of-innovation.htm

"Assuring Trustworthiness in an Open Global Market of IIoT Systems via Structured Assurance Cases"
https://www.iiconsortium.org/news/joi-articles/2018-Sept-JoI_Assuring_Trustworthiness-FINAL2.pdf

WPI's State-of-the-Art Seminar in Systems Engineering: Development of Trustworthy and Secure Systems
Wednesday October 17, 2018 at Worchester Polytechnic Institute, Worcester, MA
Registration: http://go2.wpi.edu/l/170792/2018-07-24/sq5z4


industrial internet CONSORTIUM

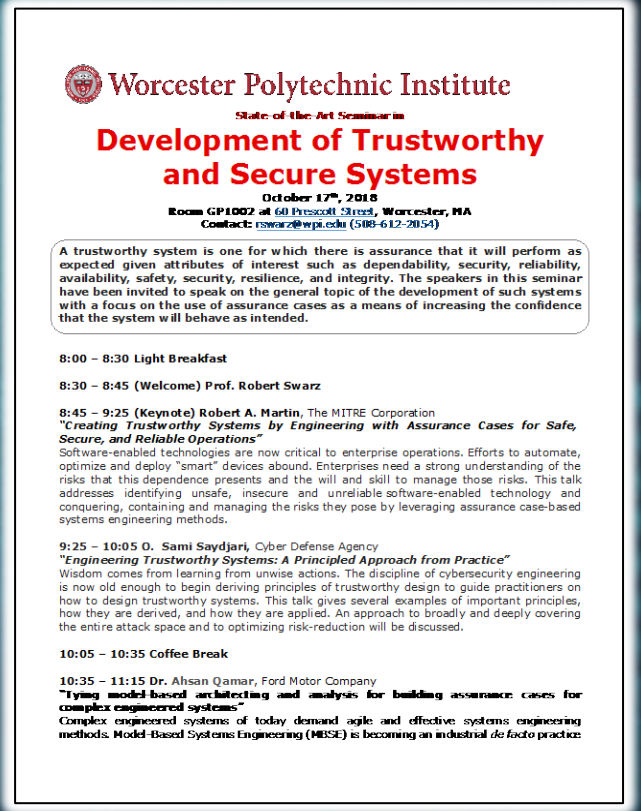
www.iiconsortium.org

Assuring Trustworthiness in an Open Global Market of IIoT Systems via Structured Assurance Cases

Authors:
Robert A. Martin
Senior Principal Engineer
The MITRE Corporation
ramartin@mitre.org

Ken Modeste
Director
Connected Technologies, UL LLC
Ken.Modeste@ul.com

September 2018 - 44 -


Worcester Polytechnic Institute

State of the Art Seminar in

Development of Trustworthy and Secure Systems

October 17th, 2018
Room GP1002 at 60 Prescott Street, Worcester, MA
Contact: rswarz@wpi.edu (508-612-2054)

A trustworthy system is one for which there is assurance that it will perform as expected given attributes of interest such as dependability, security, reliability, availability, safety, security, resilience, and integrity. The speakers in this seminar have been invited to speak on the general topic of the development of such systems with a focus on the use of assurance cases as a means of increasing the confidence that the system will behave as intended.

8:00 – 8:30 Light Breakfast

8:30 – 8:45 (Welcome) Prof. Robert Swarz

8:45 – 9:25 (Keynote) Robert A. Martin, The MITRE Corporation
"Creating Trustworthy Systems by Engineering with Assurance Cases for Safe, Secure, and Reliable Operations"
Software-enabled technologies are now critical to enterprise operations. Efforts to automate, optimize and deploy "smart" devices abound. Enterprises need a strong understanding of the risks that this dependence presents and the will and skill to manage those risks. This talk addresses identifying unsafe, insecure and unreliable software-enabled technology and conquering, containing and managing the risks they pose by leveraging assurance case-based systems engineering methods.

9:25 – 10:05 O. Sami Saydjari, Cyber Defense Agency
"Engineering Trustworthy Systems: A Principled Approach from Practice"
Wisdom comes from learning from unwise actions. The discipline of cybersecurity engineering is now old enough to begin deriving principles of trustworthy design to guide practitioners on how to design trustworthy systems. This talk gives several examples of important principles, how they are derived, and how they are applied. An approach to broadly and deeply covering the entire attack space and to optimizing risk-reduction will be discussed.

10:05 – 10:35 Coffee Break

10:35 – 11:15 Dr. Ahsan Qamar, Ford Motor Company
"Tying model-based architecting and analysis for building assurance cases for complex engineered systems"
Complex engineered systems of today demand agile and effective systems engineering methods. Model-Based Systems Engineering (MBSE) is becoming an industrial *de facto* practice

MITRE