How can we achieve trustworthiness and integrity of data in industrial value chains?

Robert A. Martin
15 May 2018

Industrial Internet of Things (IIoT)

Medical

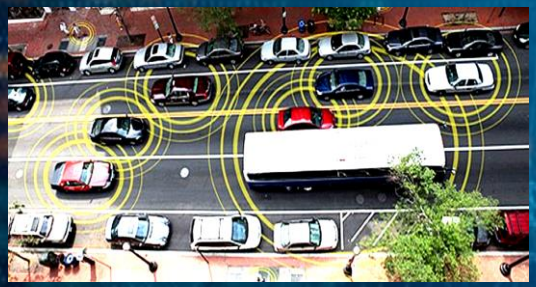
Buildings

Aeronautics

Manufacturing

Energy

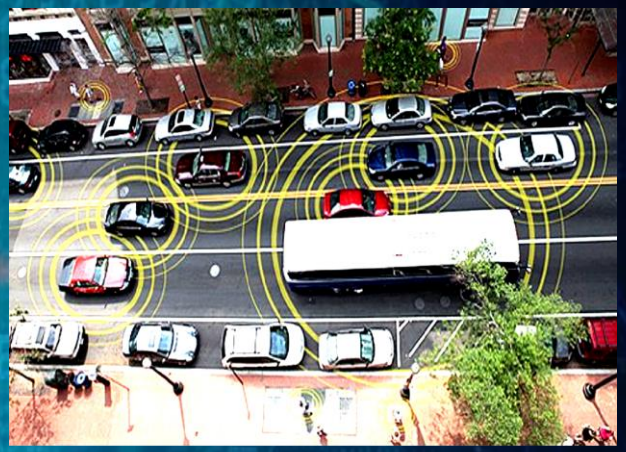
Vehicles

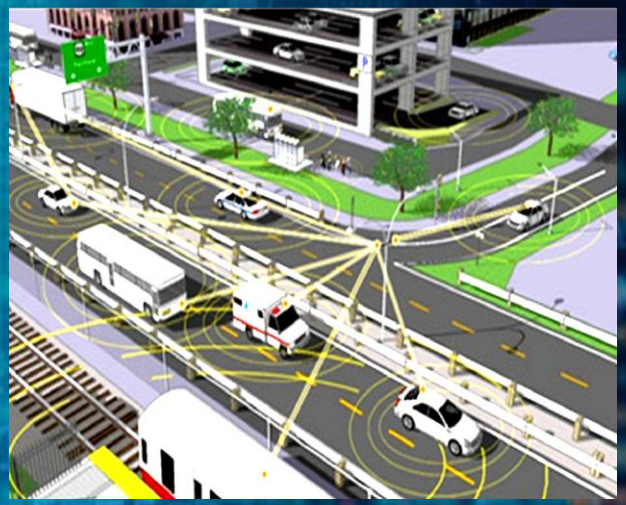


Video Analytics

MITRE

Connectivity and Complexity of Transportation Cyber Systems

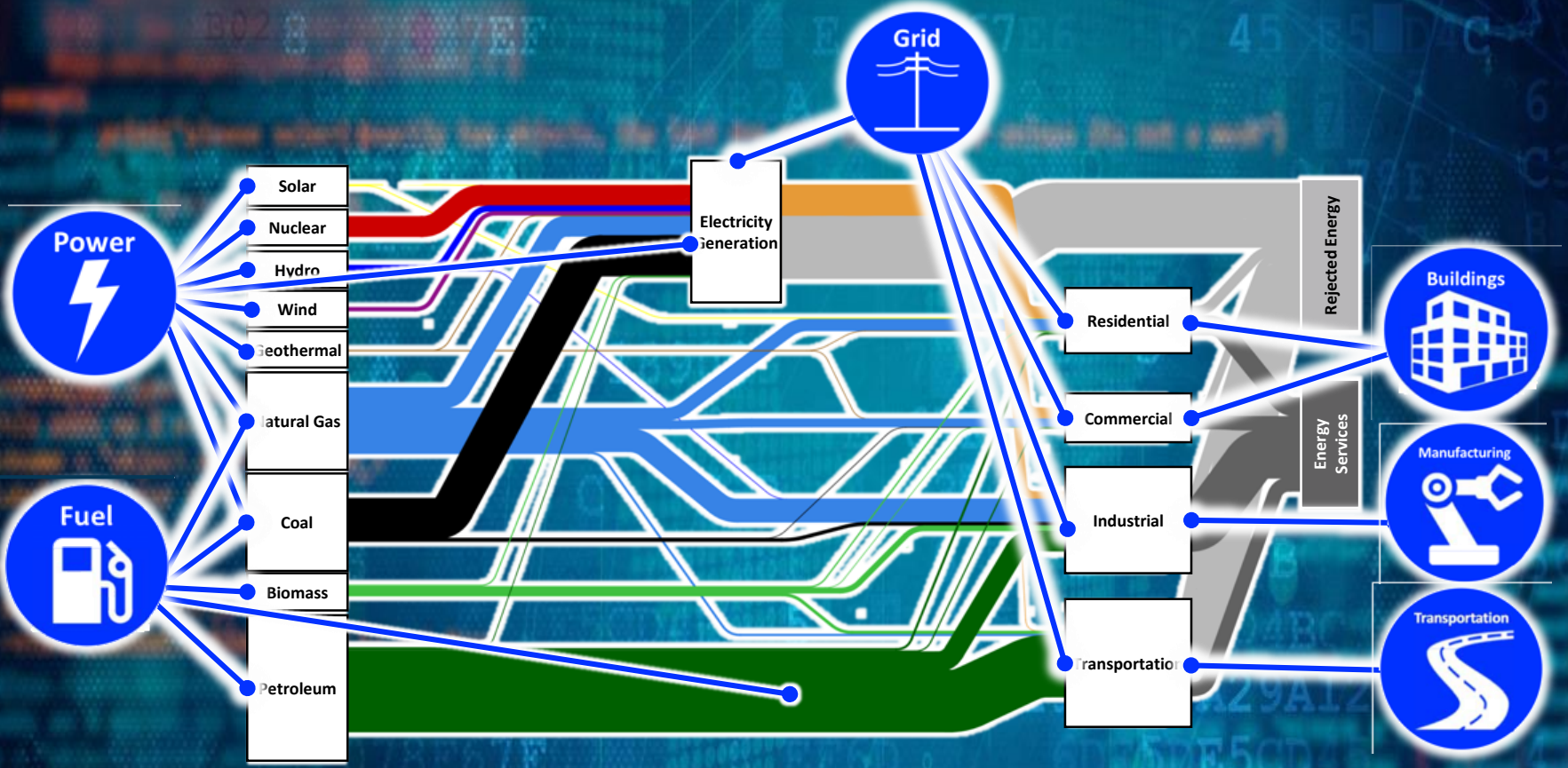




Driverless Cars, ADAS, V2V, V2I, Safety

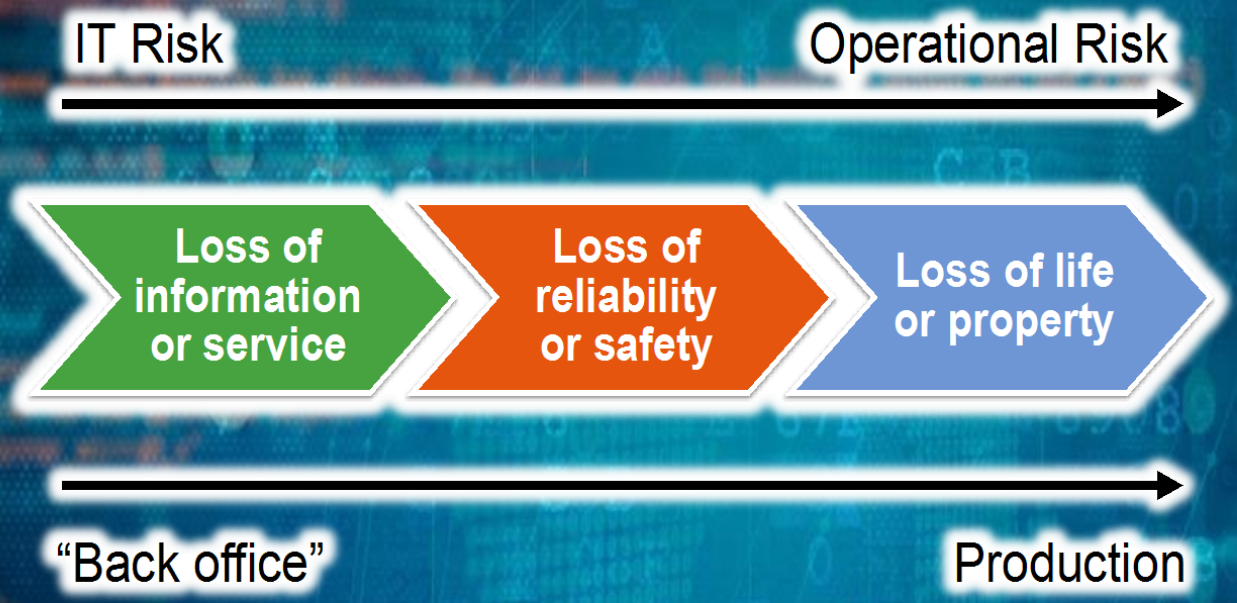
MITRE

Sector-2-Sector connections and dependance drives a need for consistency in all aspects of assurance



MITRE

Need Secure, Safe, Reliable, and Resilient Behavior that Upholds Privacy Expectations



Gartner

MITRE

Control Systems of Cyber Physical Systems

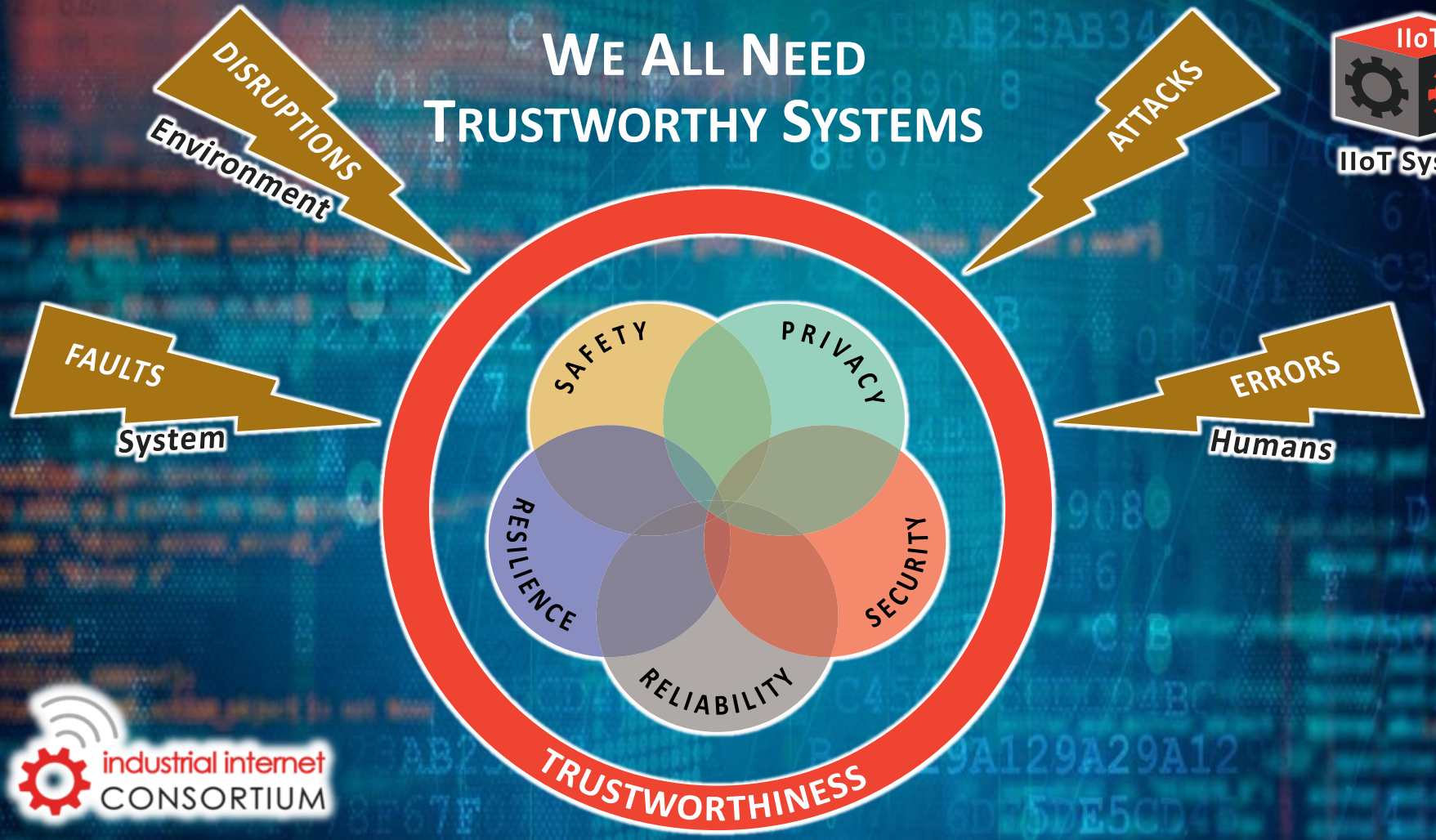
A. Traditional Cyber Risk

B. Cyber-Physical Risk

Human Error | System Faults | Environmental Disruptions

MITRE

We All Need Trustworthy Systems

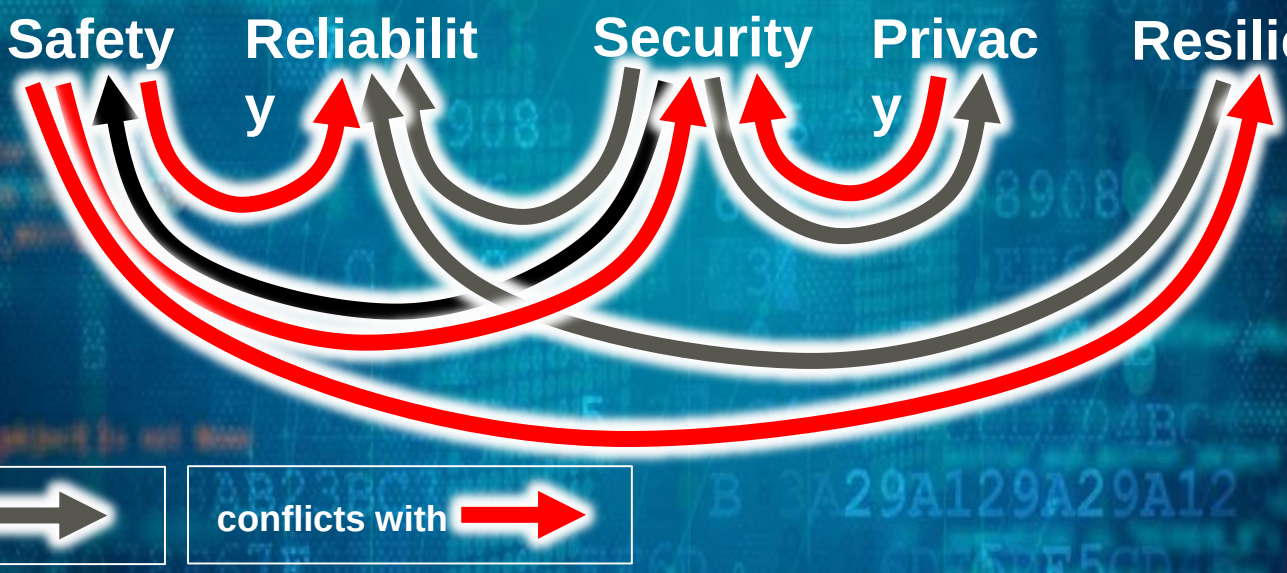


industrial internet CONSORTIUM

MITRE

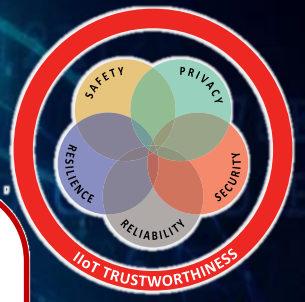
Interactions in Trustworthiness Aspects

- Trustworthiness characteristics may support each other, or may conflict with each other
- Have different objectives and metrics

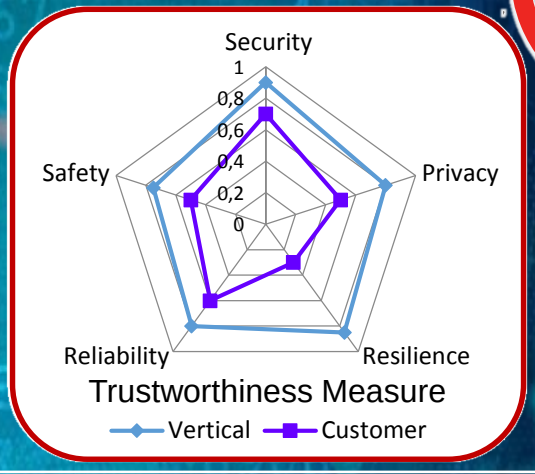


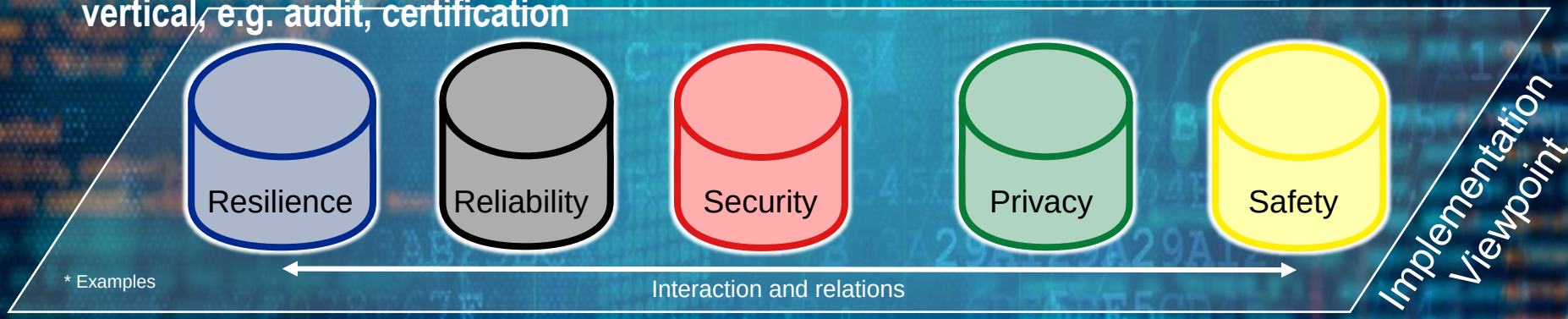
MITRE

The Key System Characteristics of Trustworthiness as a Quality Measure



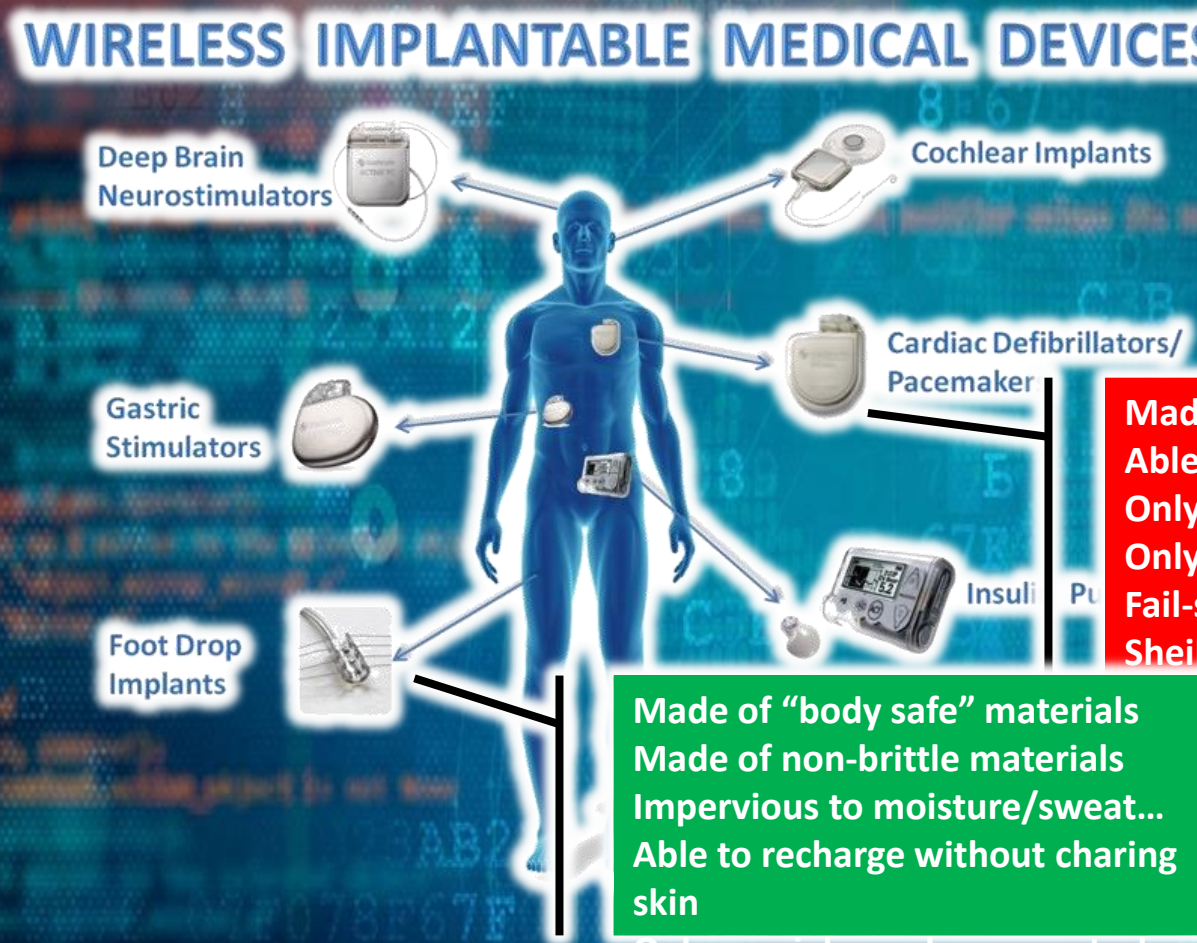
- Industrial IoT Quality is a continuum of system characteristics
  - OT Security (IEC 62443*) meets IT Security (ISO 27000*)
  - Privacy (GDPR*), Resilience (ISO*, IEC*), Reliability (NIS*) are quality features in both OT and IT
  - Determine and ensure quality measures per vertical, e.g. audit, certification

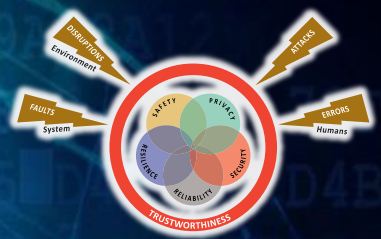




MITRE

Claims of Trustworthiness → Gathering Evidence for Assurance Cases





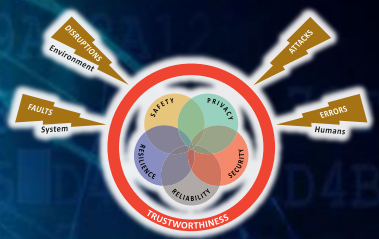
Safety*
EU: IEC 61508/62626
UK: … (after Brexit)
US: IEC 61508
CN: ()
JP: IEC 61508

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…
Sheilded from radiation…

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

MITRE

Claims of Trustworthiness → Gathering Evidence for Assurance Cases



Safety*
EU: IEC 61508/62626
UK: … (after Brexit)
US: IEC 61508
CN: ()
JP: IEC 61508
…

SafA

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…
Sheilded from radiation…
Can be used in a sterilized area
Operational w/o positive control

MITRE

The Key System Characteristic: Safe…

- ❑ 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…
- ❑ Sheilded 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 charing skin

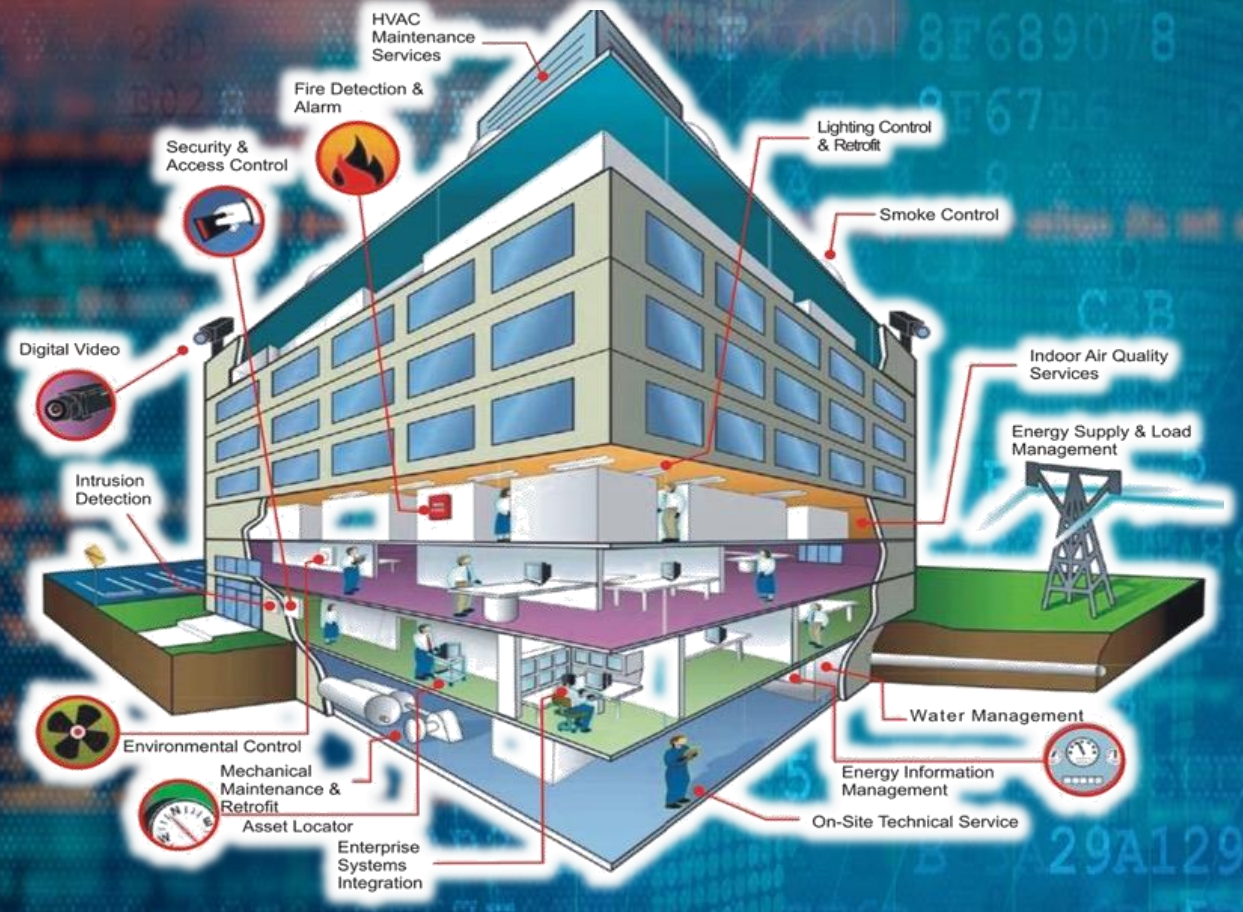
Only

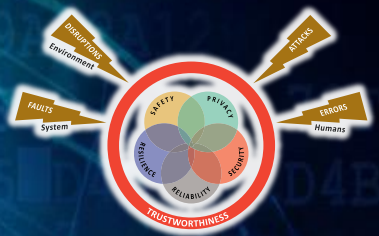
Made of “body safe” materials
Able to recharge without charring skin
Only authorized people can connect
Only special people can control
Fail-safe mode to support life…
Sheilded from radiation…

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…
Sheilded from radiation…
Can be used in a sterilized area
Operational w/o positive control

MITRE

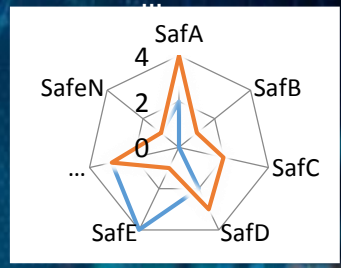
Claims of Trustworthiness → Gathering Evidence for Assurance Cases





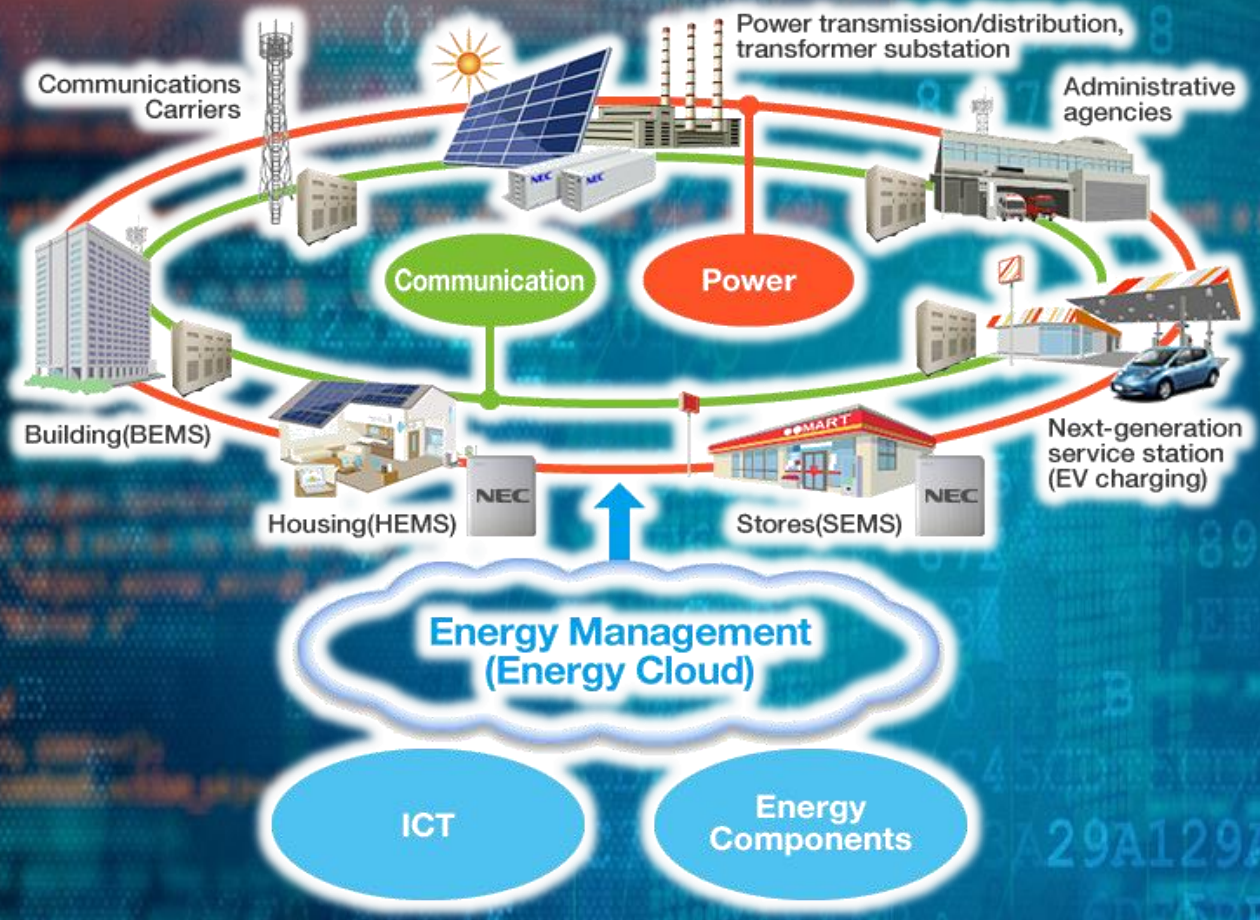
Safety*

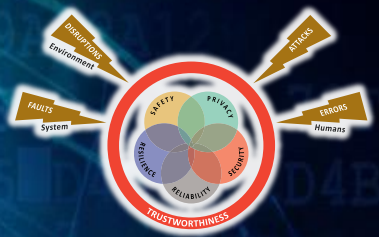
EU: IEC 61508/62626
UK: … (after Brexit)
US: IEC 61508
CN: ()
JP: IEC 61508
…



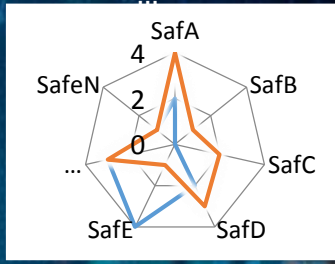
MITRE

Claims of Trustworthiness → Gathering Evidence for Assurance Cases



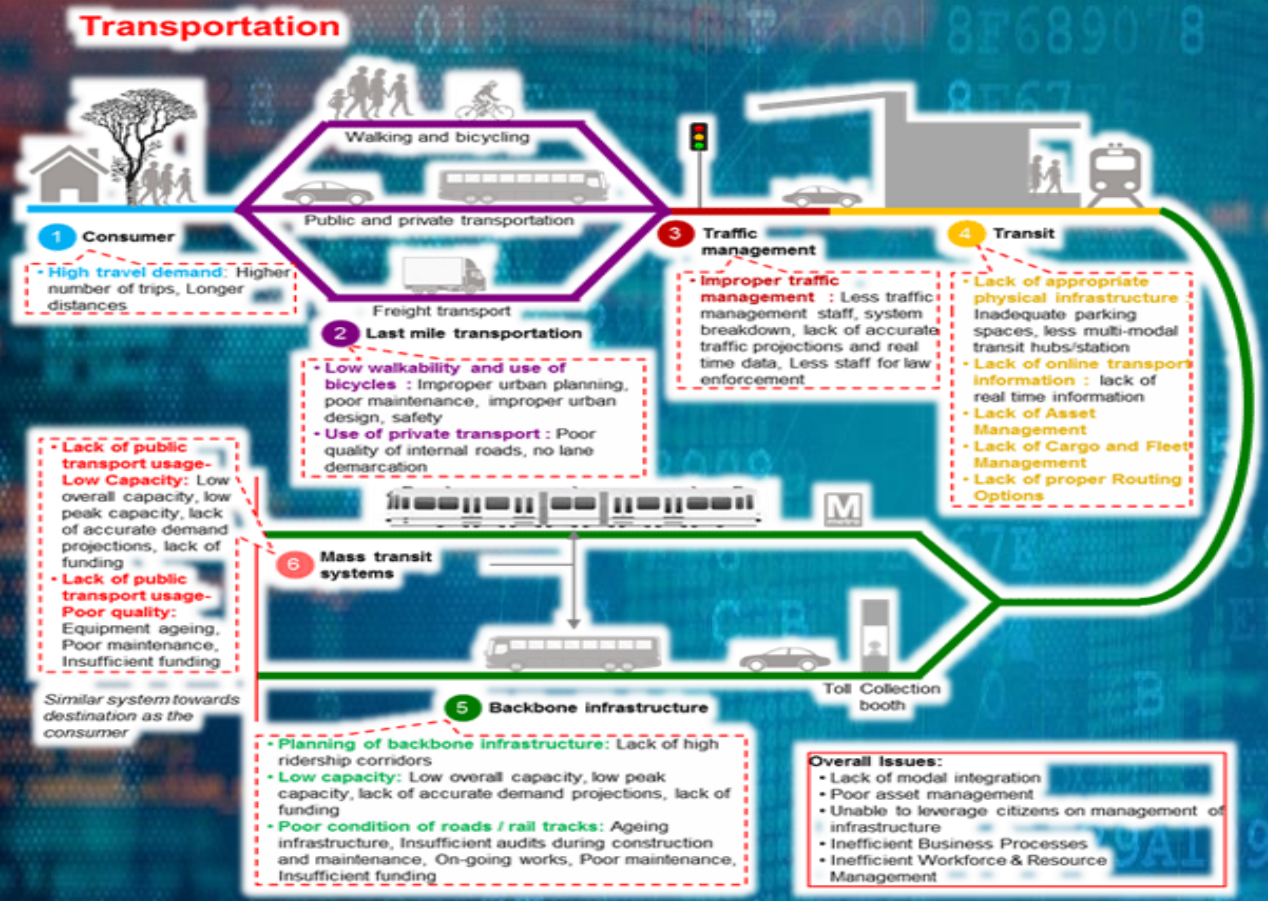


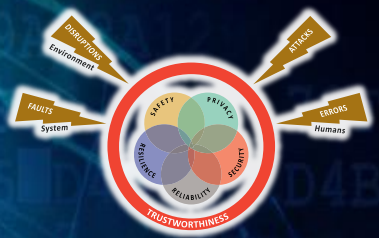
Safety*
EU: IEC 61508/62626
UK: … (after Brexit)
US: IEC 61508
CN: ()
JP: IEC 61508
…



MITRE

Claims of Trustworthiness → Gathering Evidence for Assurance Cases





Safety*

EU: IEC 61508/62626

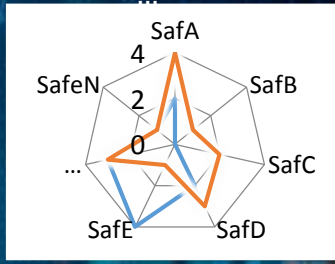
UK: … (after Brexit)

US: IEC 61508

CN: ()

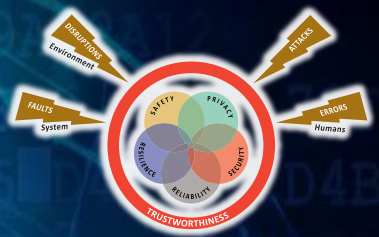
JP: IEC 61508

…



MITRE

Claims of Trustworthiness → Gathering Evidence for Assurance Cases



Safety*

EU: IEC 61508/62626

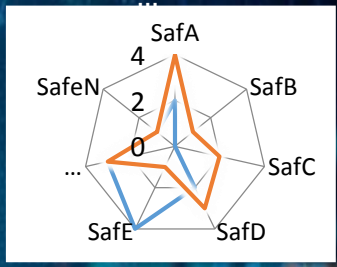
UK: … (after Brexit)

US: IEC 61508

CN: ()

JP: IEC 61508

…

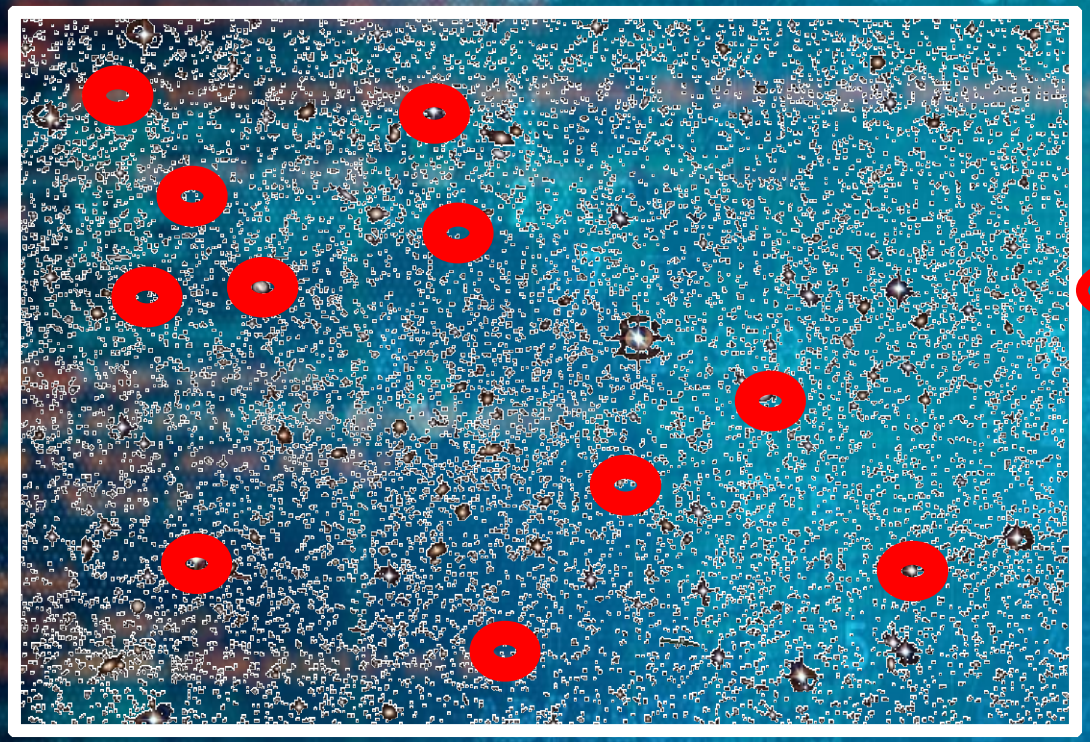


MITRE

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

MITRE

Group Requirements around "families" of IIoT Systems that 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 301-79

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

- 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
alike. One method
the use of assuranc
little or too much a
affect confidence
automatic generati
expedite a develop
perform compliance
framework which
metamodel, and a
generate a safety
conformance of the
use the GPCA infus
this framework can
pump guidance pub

Keywords
Compliance check
systems; safety case

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

The construction an
system are a daun

SIGBED Rev

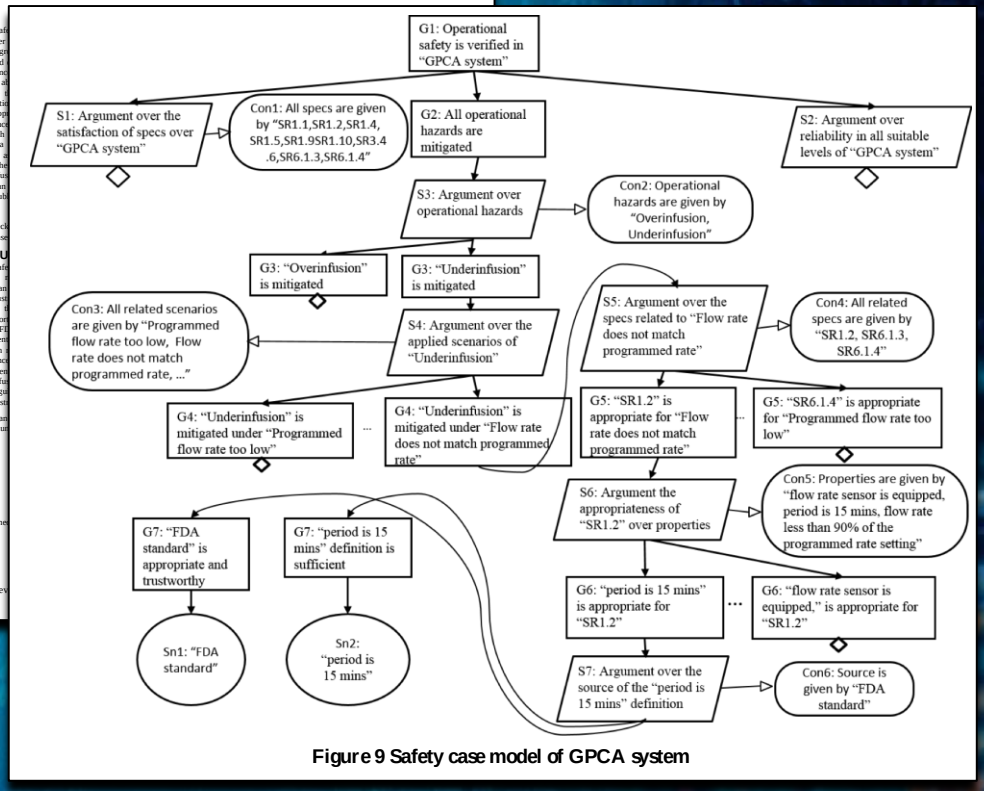
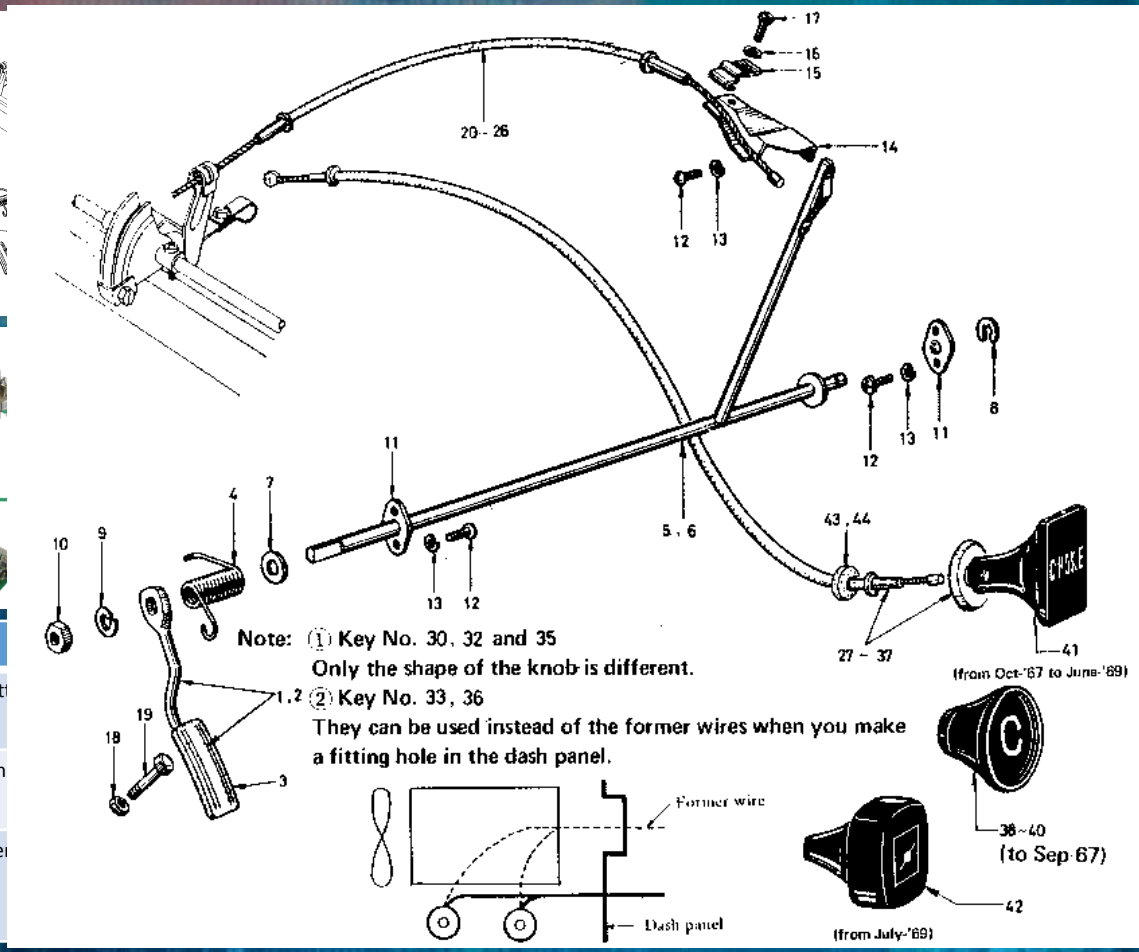


Figure 9 Safety case model of GPCA system

MITRE

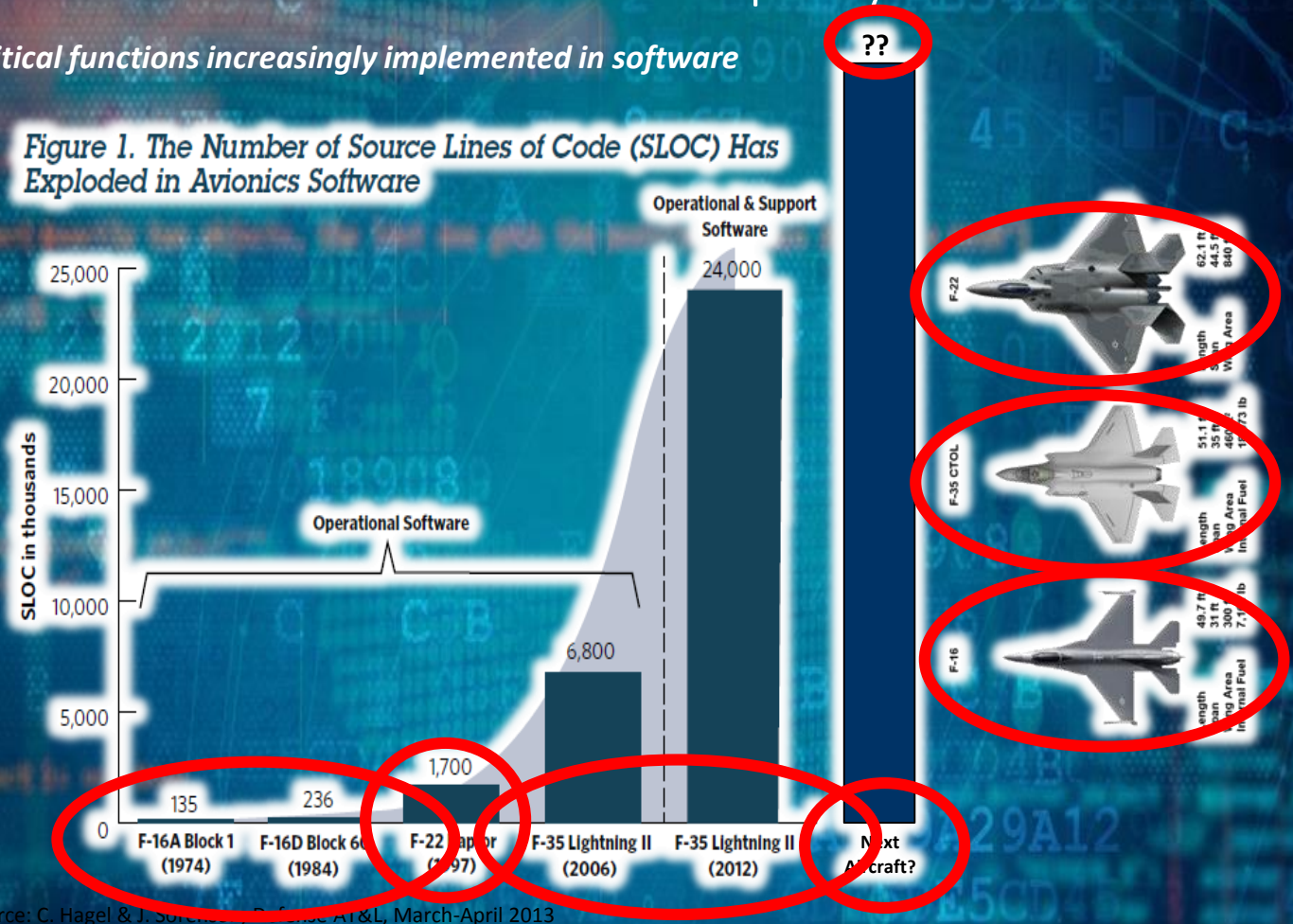
Critical Functions Have Migrated into Software



MITRE

Growth of Software in Avionic Weapons Systems

Critical functions increasingly implemented in software



Source: C. Hagel & J. Sureck[illegible], Perspective AT&L, March-April 2013

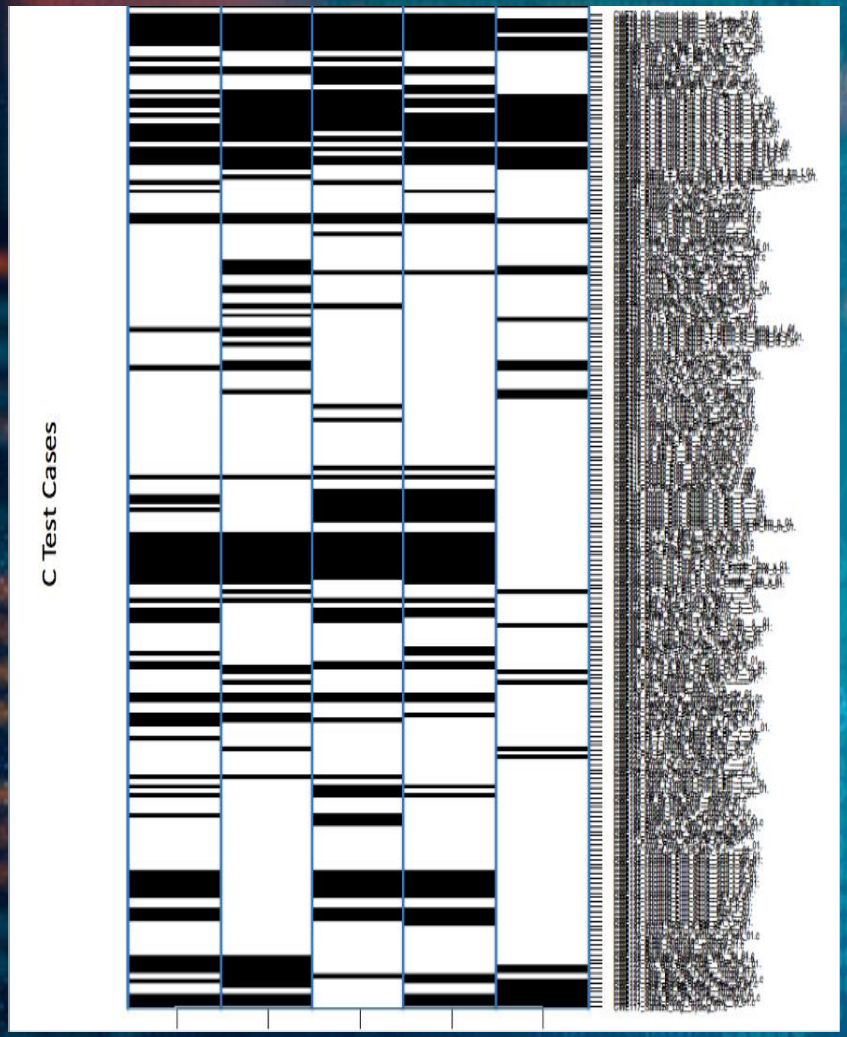
MITRE

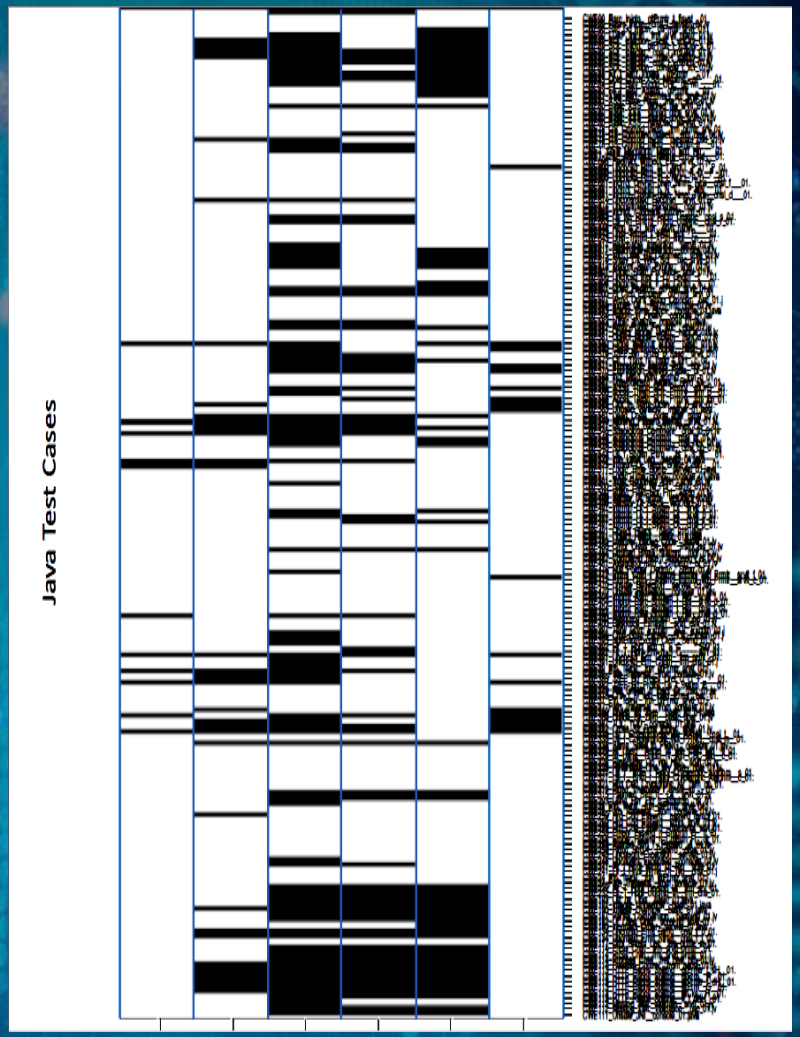
The challenge going forward is that many things are based on the man-made element of software…

- Science of Building
  - Motivated by Hammurabi's Babylonian law code, literally set in stone, of accountability
    - 4,000 years of learning about the properties of materials
  - Constrained by the laws of physics:
    - Newton's classical mechanics.
    - Einstein's theory of relativity.
    - Boyle's law of gases, conservation laws, the four laws of thermodynamics.
- Architecting Buildings
  - 4,000 years of learning to work around the weaknesses in materials
- Engineering Buildings
  - 4,000 years of guild/apprentice → engineering practices and certifications – licensed profession
  - science of materials developed and incorporated in building codes, inspection regimes

- Science of Software
  - ~100 years of mathematics and logic;
  - based on little-understood man-made constructs:
  - a variety of chip architectures
  - a variety of compiler vendors
  - a variety of operating system vendors
  - slight vagrancies in software specifications allow for different implementations by vendors
- Architecting Software
  - Driven by economics, time-to-market, cost of creation with no feed-back regarding accountability
- Engineering Software
  - EULA absolves consequences of failure
  - Blind reuse (frameworks, libraries, open source)
  - not a licensed profession
  - no pervasive understanding of the "materials science" of software
  - need inspection, mitigation, and practical methods for making software appropriately strong

MITRE



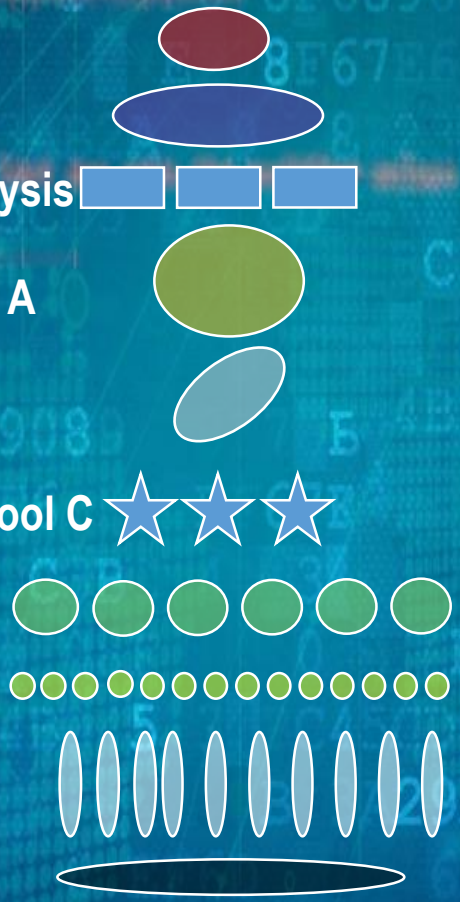


MITRE

Utilizing Appropriate Detection Methods to Collect Evidence to Gain Assurance…

Artifacts	Detection Methods
	Design Review
CONOPS	Code Review
Requirements	Attack Surface Analysis
Architecture	Static Analysis Tool A
Design	Static Analysis Tool B
Process	Dynamic Analysis Tool C
Code	Fuzz Testing
Binary	Pen Testing
Running Binary	Blue Teaming
Environment of System	Red Teaming
Use of Mission Software	

Coverage

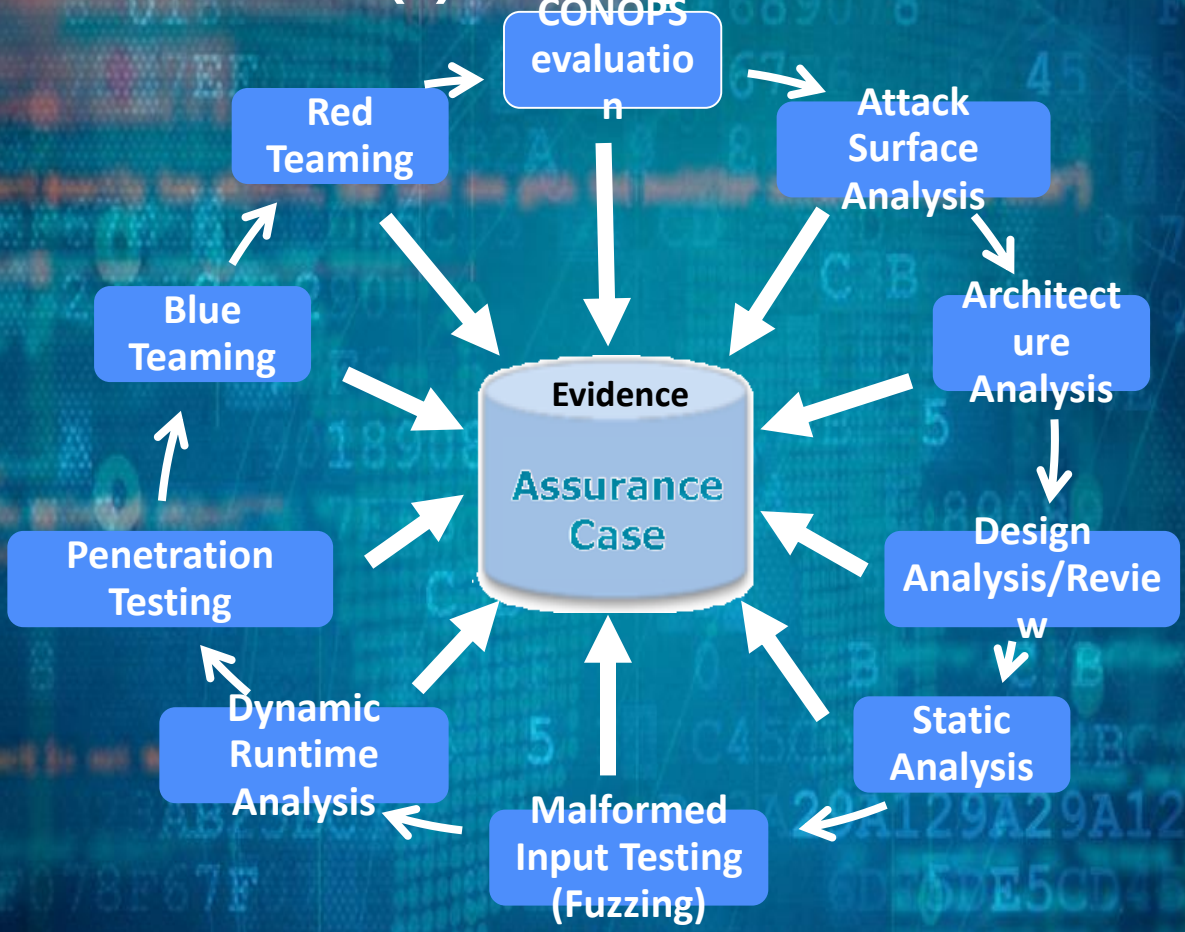


CVE, CWE, CAPEC, …

Most Important Quality Issues

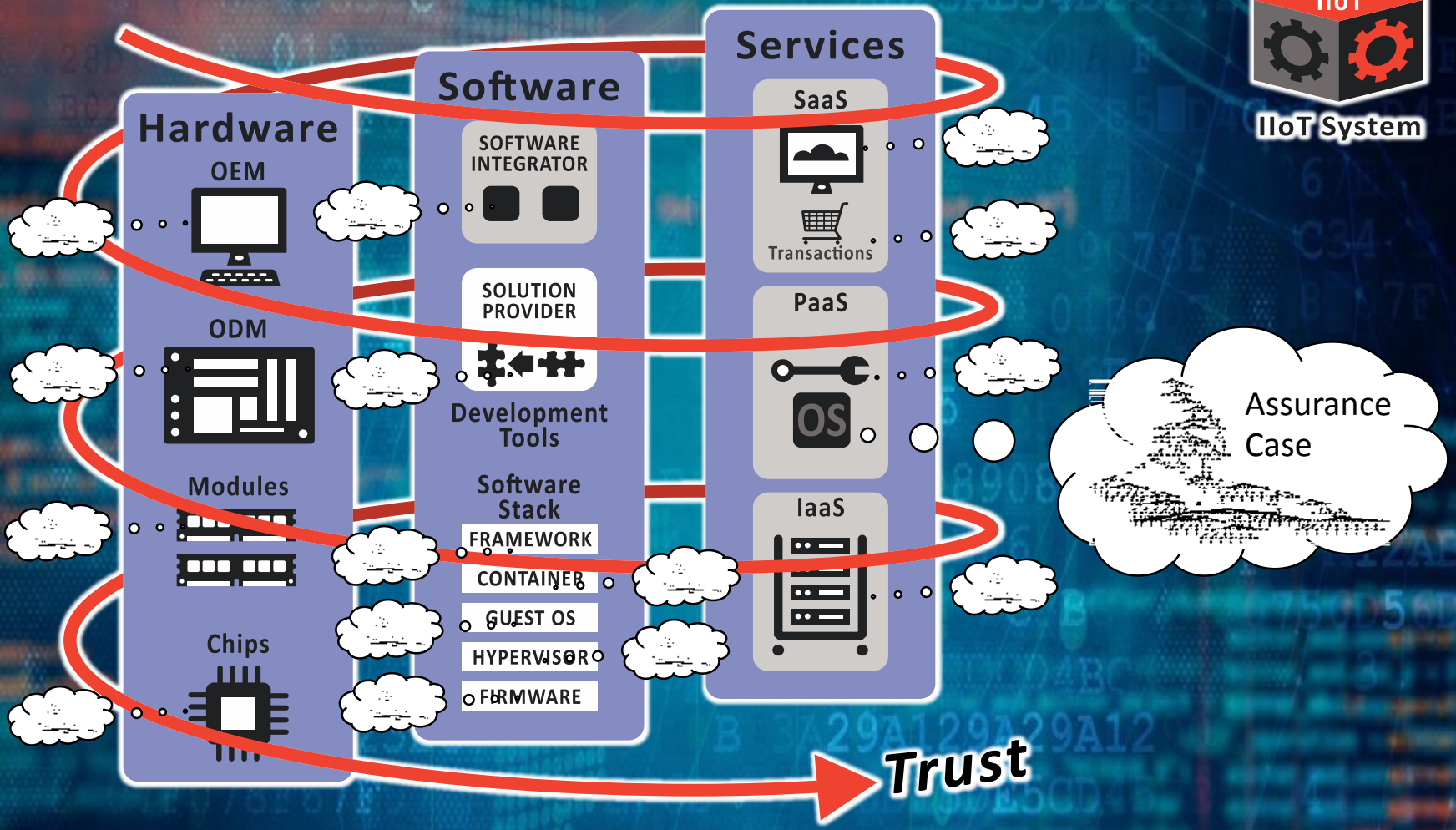
MITRE

Multiple Sources of Assurance Evidence from Throughout the Lifecycle of the item(s) needing Assurance.



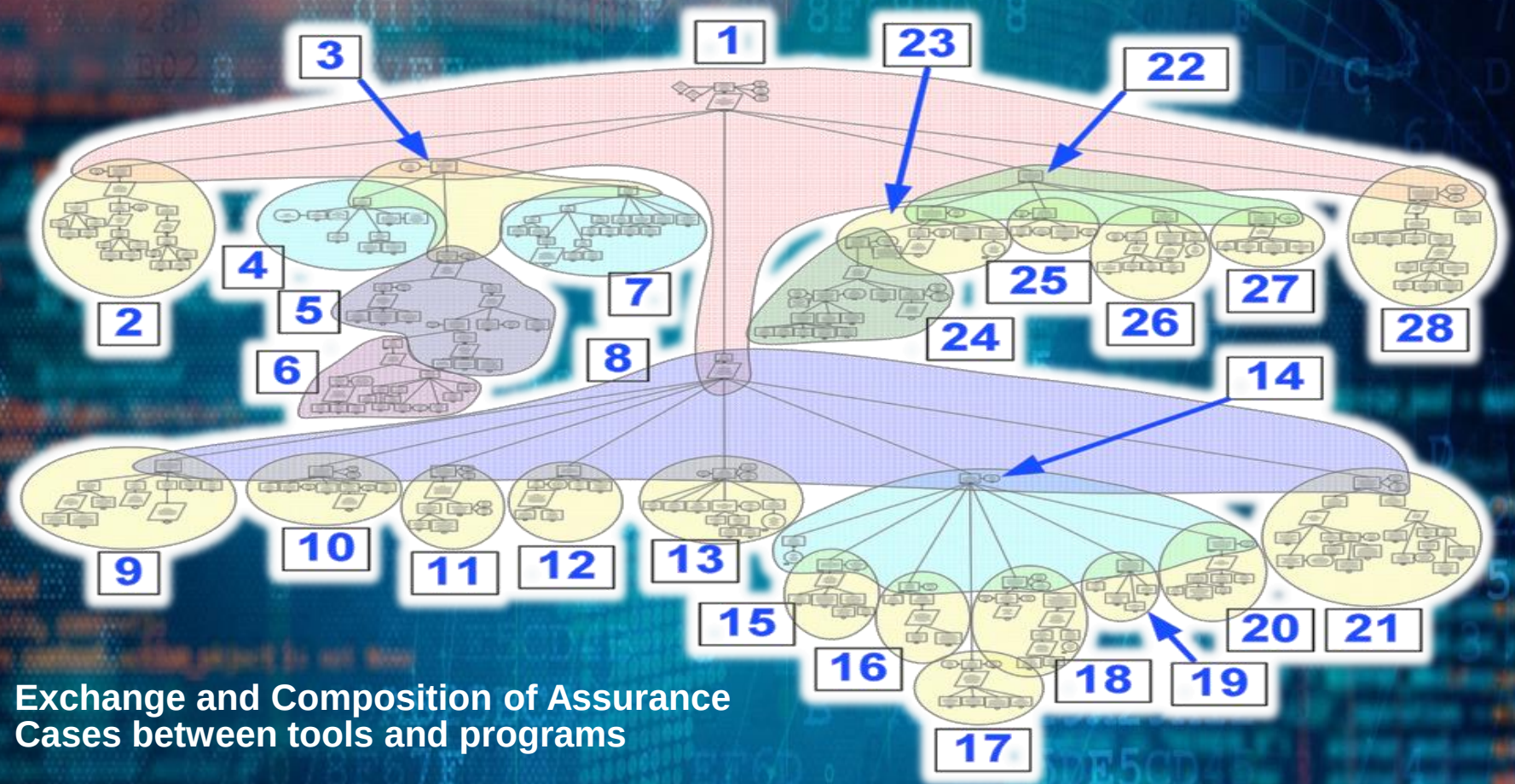
MITRE

Trust Relationship between Component Builders - FUTURE



MITRE

The Assurance Case for a System Builder using Assured Components



Exchange and Composition of Assurance Cases between tools and programs

MITRE

Industrial Internet Reference Architecture - IIRA 1.8
https://www.iiconsortium.org/IIRA.htm
Industrial Internet Security Framework - IISF 1.0
https://www.iiconsortium.org/IISF.htm
Open Group Dependability Framework – O-DA
https://publications.opengroup.org/c13f
Structured Assurance Case Metamodel - SACM
https://www.omg.org/spec/SACM
Assurance and Safety Case Environment (ASCE)
https://www.adelard.com/asce/choosing-asce/
Astah GSN
http://astah.net/editions/gsn
SafeTbox
https://www.iese.fraunhofer.de/en/competencies/safety_engineering/tools_safety/safetbox.html
D-Case Editor: A Typed Assurance Case Editor
https://github.com/d-case/d-case_editor

PLATTFORM INDUSTRIE4.0

Federal Ministry for Economic Affairs and Energy

ramartin@mitre.org

industrial internet CONSORTIUM

MITRE