A Market of Assured and Trustworthy Complex Cyber/Physical Systems

Robert A. Martin
Senior Principal Engineer
MITRE Corporation
Everything is Becoming Software-Enabled and Connected, Either through Task Dependency, Supply Chain, or Information Flow

Today Your System is:
- attackable or
- susceptible to a hazard...

When this Other System gets subverted through:
- an un-patched vulnerability;
- a mis-configuration;
- an application weakness;
- a counterfeit item;
- tainted software or hardware; or
- the system’s susceptibility to a hazard...

We need to be assured that not only are our own systems trustworthy but also everything we depend upon...
How is Software-Enabled and Connected (aka Cyber) Becoming so Pervasive?

Context: 1976 Chevy Vega

The only software was behind the wheel – no microelectronics.
Critical Functions Migrated into Software & Microelectronics (SW/HW)

Electric throttle valve control
Control/Communication Transitioned from Point-to-Point Wiring to Network-based
Critical Functions Are Migrating into Connected SW/HW
Multiple Types of Networks Are Appearing

- CAN (Controller Area Network)
- MOST (Media Oriented Systems Transport)
- Ethernet AVB (Audio Video Bridging)
- Ethernet TSN (Time-Sensitive Networking)
- FlexRay
- Brake-by-Wire System
- LIN (Local Interconnect Network)
- Multifunction Keyless System
Many Critical Functions Now Need to be Updated and Sustained…
The Connectivity and Complexity of Connected Software-Enabled Systems is Still Expanding

Driverless Cars, ADAS, V2V, V2I, Safety
All types of Enterprises are Facing these Same Changes...

Medical

Buildings

Aeronautics

Manufacturing

Vehicles

Energy

Shipping
Changes Go Well beyond Traditional Information Technology...
Need Secure, Safe, Reliable, and Resilient Behavior that Upholds Privacy Expectations

- **IT Risk**
  - Loss of information or service
  - Loss of reliability or safety
- **Operational Risk**
  - Loss of life or property

- **“Back office”**
- **Production**
Need Assurance of More Than Security – Need Assured Trustworthy Systems

- Attacks
- Errors
- Humans
- Faults
- Environment

Trustworthiness

- Privacy
- Safety
- Security
- Resilience

Reliability
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
Claims of Trustworthiness → Gathering Evidence for Assurance Cases

Wireless Implantable Medical Devices

- Deep Brain Neurostimulators
- Gastric Stimulators
- Foot Drop Implants
- Cardiac Defibrillators/Pacemaker
- Cochlear Implants
- Insulin Pump

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

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-44
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
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

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

Possible System Trustworthiness Requirements
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
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

For questions regarding this document, please contact: Richard Hawkins, Department of Computer Science, The University of York, York, UK, richard.hawkins@york.ac.uk.

For questions regarding safety assurance cases, contact: Earl Thompson, General Hospital Compliance at 301-796-5770 or via email at earl.thompson@fda.hhs.gov.

Ear/Nose/Throat, General Hospital, Infectious Control, and Ophthalmic Devices Branch, Office of Devices Branch, Office of Device Evaluation at 301-796-2585 or via email at richard.hawkins@york.ac.uk.

For questions pertaining to manufacturer reports, call 301-796-6104 or via email at sharon.kapsch@fda.hhs.gov.


Support for Safety Case Generation via Model Transformation

Chung-Ling Lin, Wuwei Shen
Department of Computer Science
University of Western Michigan
Kalamazoo, MI, USA
(chung-lin@cs.wmich.edu)

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

Figure 9 Safety case model of GPCA system

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-44
The Assurance Case

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

Dependability Engineering Innovation for Cyber Physical Systems

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-44
The Basics of an Assurance Case

Claim = assertion to be proven

Argument = how evidence supports claim

Evidence = required documentation
The Assurance Case for a System Builder using Assured Components

Exchange and Composition of Assurance Cases between tools and programs
The Assurance Case for a System Builder using Assured Components

Exchange and Composition of Assurance Cases between tools and programs
Software is a man-made element that does not follow the laws of physics, chemistry, or other natural orders...

- **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
Assurance needs to address the Hazards & Attacks that can impact SW-Based Mission Functions

“Counter Measures - Actions” include:
- choices about architecture, design, physical decomposition, and operational approaches;
- adding/changing security functions, protection schemes, activities & processes;
- use of static & dynamic code assessments;
- attack surface analysis, architecture and design reviews, dynamic testing; and pen testing

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-44
Exploitable Weaknesses, Vulnerabilities & Exposures

- **Weakness:** mistake or flaw condition in ICT architecture, design, code, or process that, if left unaddressed, could under the proper conditions contribute to a cyber-enabled capability being vulnerable to exploitation; represents potential source vectors for zero-day exploits -- Common Weakness Enumeration (CWE) [https://cwe.mitre.org/](https://cwe.mitre.org/)

- **Vulnerability:** mistake in software that can be directly used by a hacker to gain access to a system or network; Exposure: configuration issue of a mistake in logic that allows unauthorized access or exploitation -- Common Vulnerability and Exposure (CVE) [https://cve.mitre.org/](https://cve.mitre.org/)

- **Exploit:** take advantage of a weakness (or multiple weaknesses) to achieve a negative technical impact -- attack approaches from the set of known exploits are used in the Common Attack Pattern Enumeration and Classification (CAPEC) [https://capec.mitre.org/](https://capec.mitre.org/)

The existence (even if only theoretical) of an exploit designed to take advantage of a weakness (or multiple weaknesses) and achieve a negative technical impact is what makes a weakness a vulnerability.
Assurance needs to address the Hazards & Attacks that can impact SW-Based Mission Functions

"Counter Measures - Actions" include:
choices about architecture, design, physical decomposition, and operational approaches;
adding/changing security/safety functions, protection schemes, activities & processes;
use of static & dynamic code assessments, dynamic testing, physical testing, and pen testing;
attack surface & fault-tree analysis, architecture and design reviews

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-44
Utilizing Appropriate Detection Methods to Collect Evidence to Gain Assurance...

Artifacts
- CONOPS
- Requirements
- Architecture
- Design
- Process
- Code
- Binary

Detection Methods
- Design Review
- Code Review
- Attack Surface Analysis
- Static Analysis Tool A
- Static Analysis Tool B
- Dynamic Analysis Tool C
- Fuzz Testing
- Pen Testing
- Blue Teaming
- Red Teaming

Coverage

CVE, CWE, CAPEC, ...

Most Important Quality Issues

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-44
Multiple Sources of Assurance Evidence from Throughout the Lifecycle of the item(s) needing Assurance.
One more thing
Software Quality

- Usable
- Performant
- Portable
- Resilient
- Reliable
- Secure
- Safe
- Maintainable

HTTPS://CQE.MITRE.ORG

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-44
137 CQE's just integrated into CWE

CWE Version 3.2
January 03, 2019

CWE-1047: Modules with Circular Dependencies

Relevant to the view "Research Concepts" (CWE-1000)

Relevant to the view "Development Concepts" (CWE-690)

CWE VIEW: Quality Weaknesses with Indirect Security Impacts

CWE VIEW: CISQ Quality Measures (2016)

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 18-1804-44
Need Standards to Drive Consistency in Discussing and Conveying Assurance due to the Sector-2-Sector linkages
TRANSPARENT ASSURANCE AS A BASIS FOR TRUST - FUTURE

Hardware
- OEM
- ODM
- Modules
- Chips

Software
- Software Integrator
- Solution Provider
- Development Tools
- Software Stack
  - Framework
  - Container
  - Guest OS
  - Hypervisor
  - Firmware

Services
- SaaS (Transactions)
- PaaS
- IaaS

Assurance Case

Trust
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”