OpenSystems media

Best Practices for Software Trustworthiness in IIoT Applications

Speakers

Marcellus Buchheit, Wibu-Systems USA

Mark Hermeling, GrammaTech

Moderator:

Rich Nass,

Embedded Computing Design

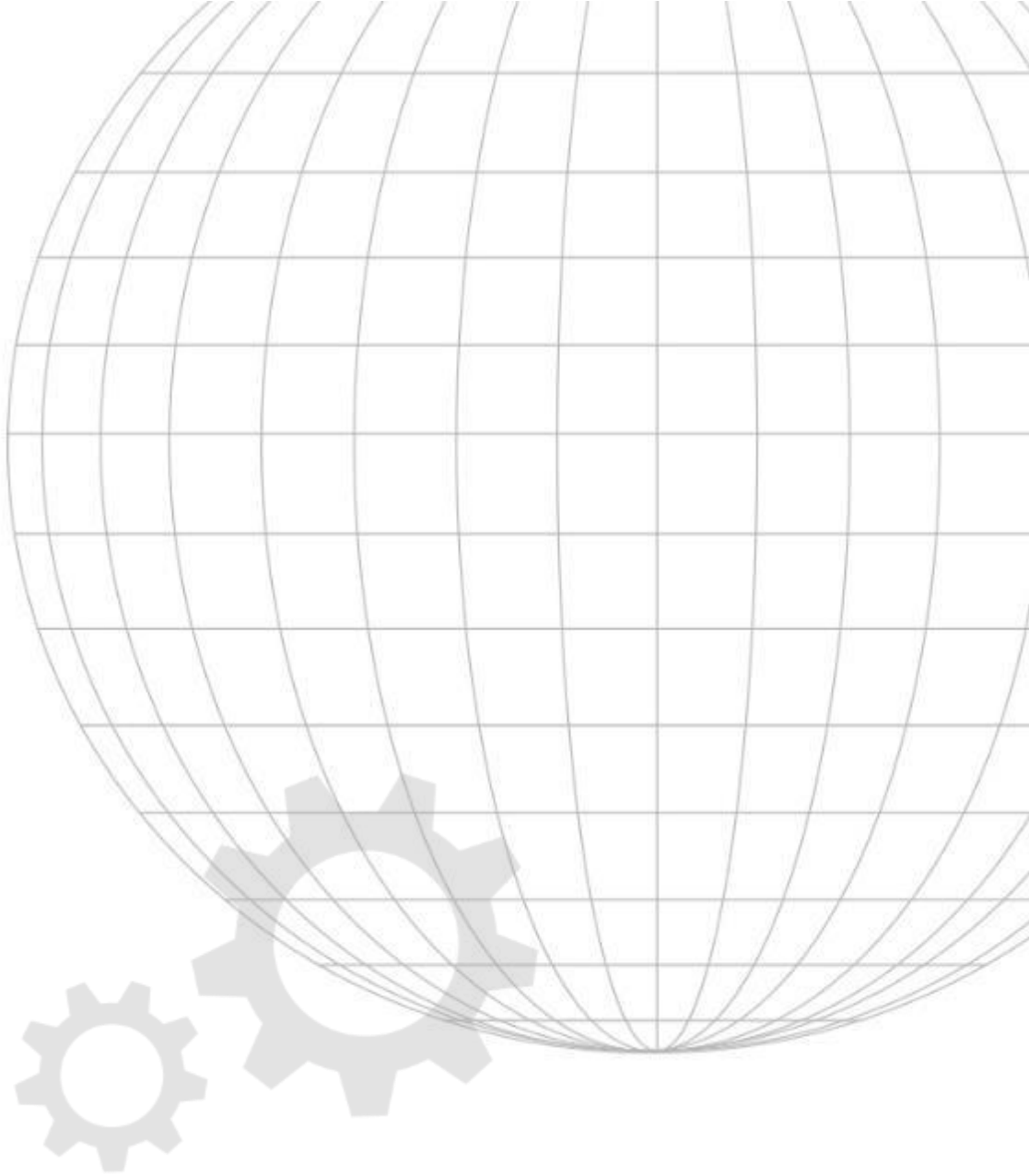
OpenSystems Media

GRAMMATECH

WIBU SYSTEMS

OpenSystems media

AGENDA



Best Practices for Software Trustworthiness in IIoT Applications

Marcellus Buchheit – Wibu-Systems
Mark Hermeling – GrammaTech

June 2020

Agenda

- Introductions
- Best Practices
  - The Institution
  - The Software Lifecyle
  - Operation
  - Software Protection
- From Concepts to Solutions
  - GrammaTech
  - Wibu-Systems
- Q&A and References

The Industrial Internet Consortium

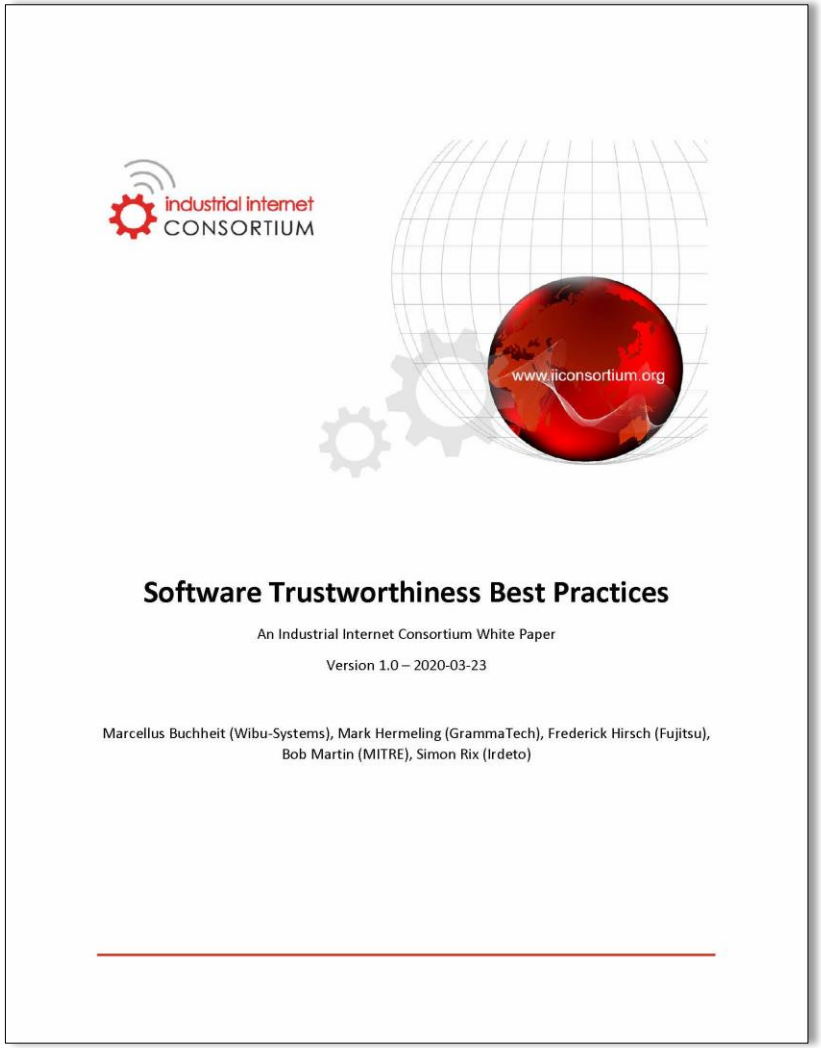
Wibu-Systems and GrammaTech are both members of the Industrial Internet Consortium – A global not-for-profit partnership of industry, government and academia

https://www.iiconsortium.org/about-us.htm

Global Membership
Spanning 30 Countries

www.iiconsortium.org

Who Are We?



- Whitepaper:
  five authors,
  two are present in today's webinar

Marcellus Buchheit
(Wibu-Systems)

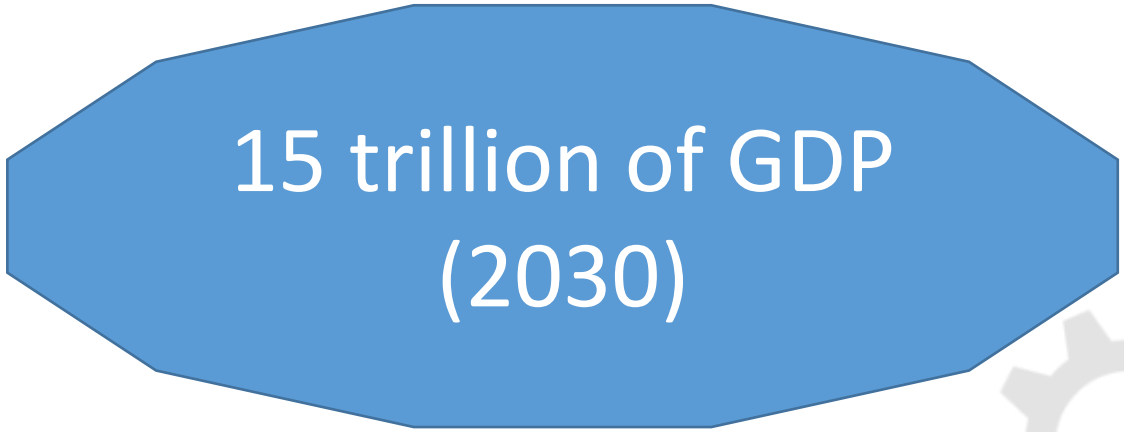
Mark Hermeling
(GrammaTech)

- Industrial Internet Consortium
  - Trustworthiness Task Group
  - part of Security Working Group

- Link of Free Download:
  https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf

Industrial Internet Of Things

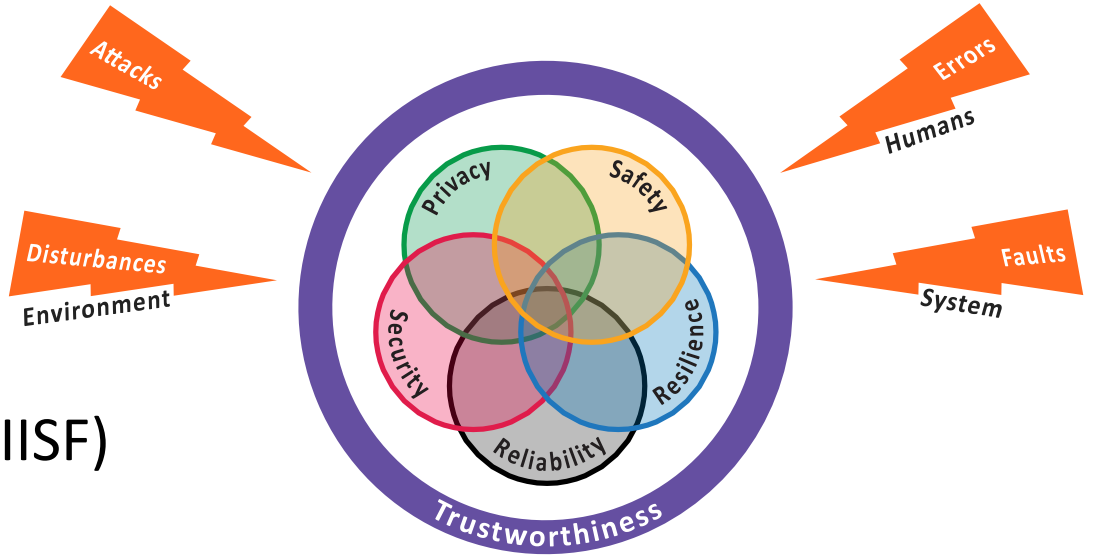
- Connected sensors, instruments and other devices
- With the goal of delivering benefits to humanity
- Aiming for improved productivity and efficiency or other economic benefits
- Many different industries
  - Manufacturing
  - Oil and gas
  - Power and water
  - Smart Grid
  - …
- Control, data and logic



https://en.wikipedia.org/wiki/Industrial_internet_of_things

The Trustworthiness Challenge

- Software is key in many systems that we depend on daily
- Confidence and trust are key
  - Correct operation
  - In hostile environments
  - Protecting IP



- IIC has several good papers on IIoT:
  - Industrial Internet Security Framework (IISF) https://www.iiconsortium.org/IISF.htm
  - Security Maturity Model (SMM) https://www.iiconsortium.org/smm.htm
- But the software angle needed more focus

Best Practices

- Paper was written to give more detail on how to deal with trustworthiness and to give software project managers guidance on what they should think about.

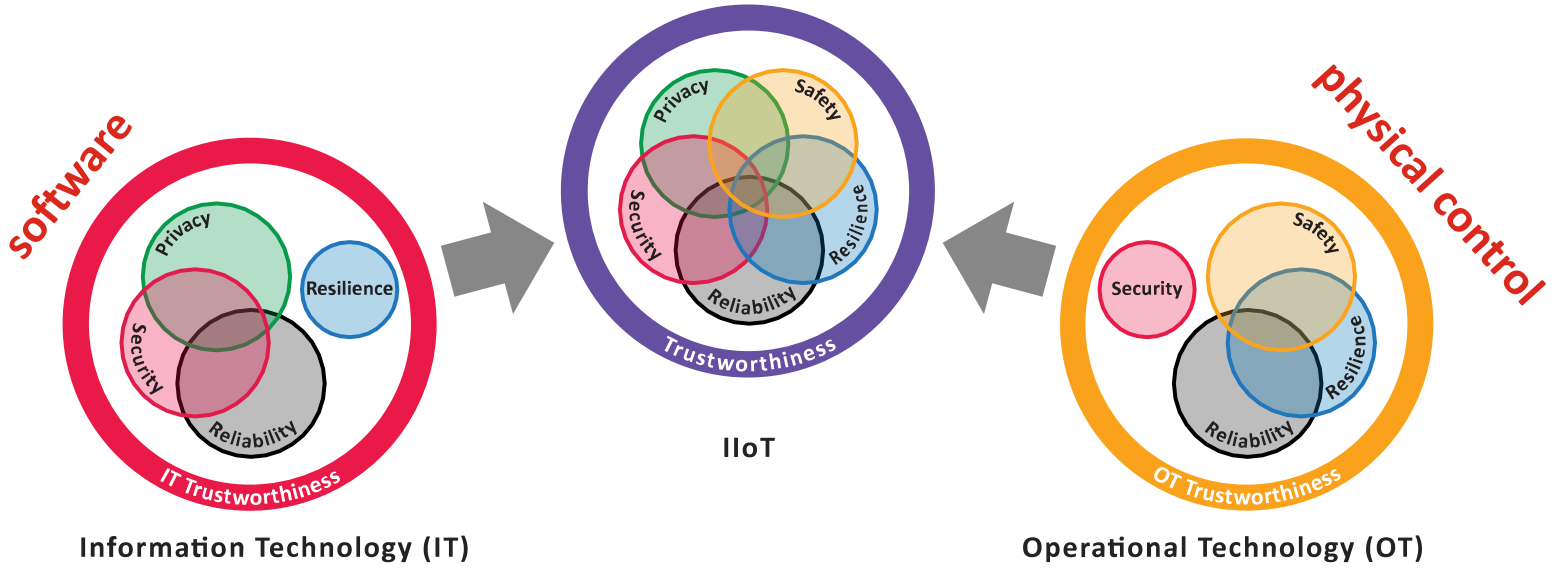
Overview about the Whitepaper:

- The Institution (Marcellus)
- Software Lifecyle (Mark)
- Operation (Marcellus)
- Software Protection (Marcellus)

Institutional Trust and Confidence in Software

- **IIoT Systems as industrial "physical control" systems can be *dangerous*:**
  - Accidents threatening *health* and *life* of people, endanger *environment*
  - Solution: *Systematic* approach to *trustworthiness* (maturity model etc.)
- **Software becomes a major part of IIoT "physical control":**
  - Software errors are not just *threats* to *information/money* but *people/environment*
  - Software design/setup/operation:
    same *strict guidelines* needed as mechanical engineering
    - Bad Example: Boeing MCAS software module of 737Max
  - Additional threats: *Remote malicious hacker attacks* to software via Internet
    - Part of future strategic warfare:
      "Military-style" hackers attack *public infrastructure* and *large private industrial systems*

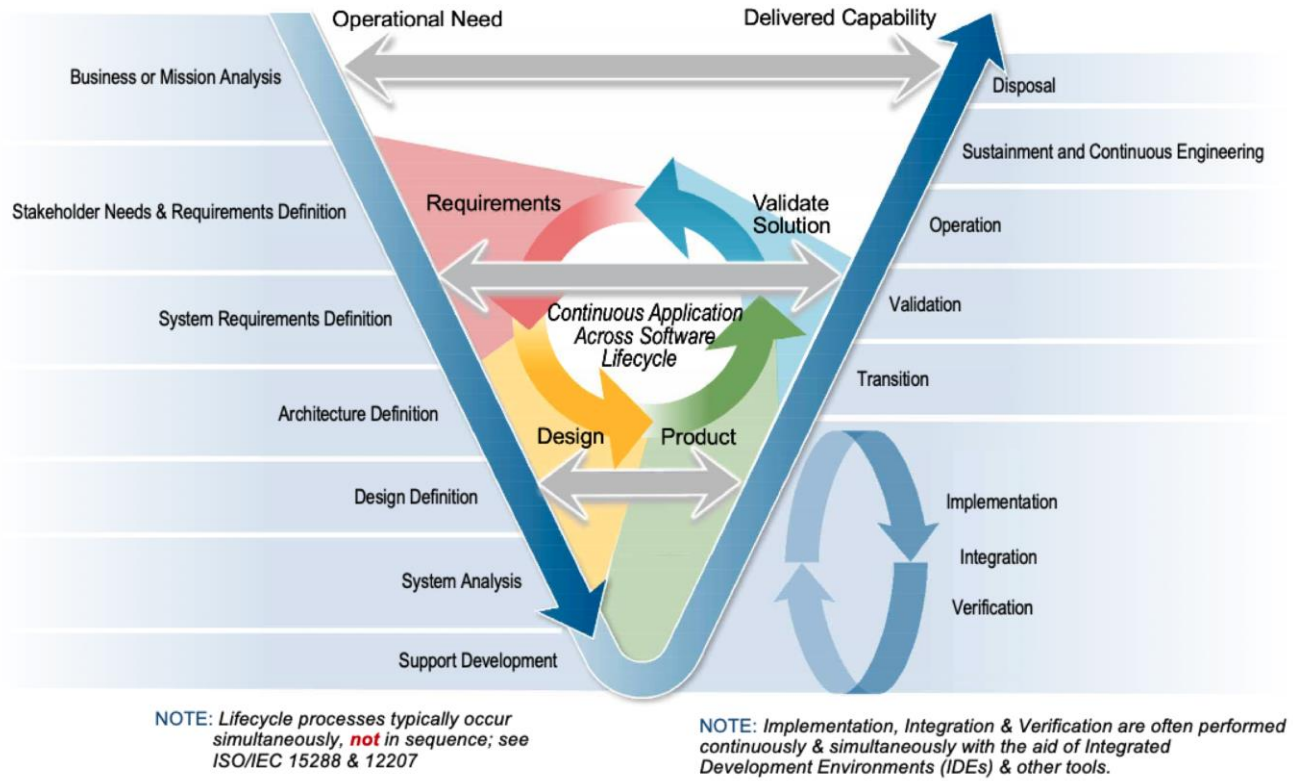
The Software Lifecyle



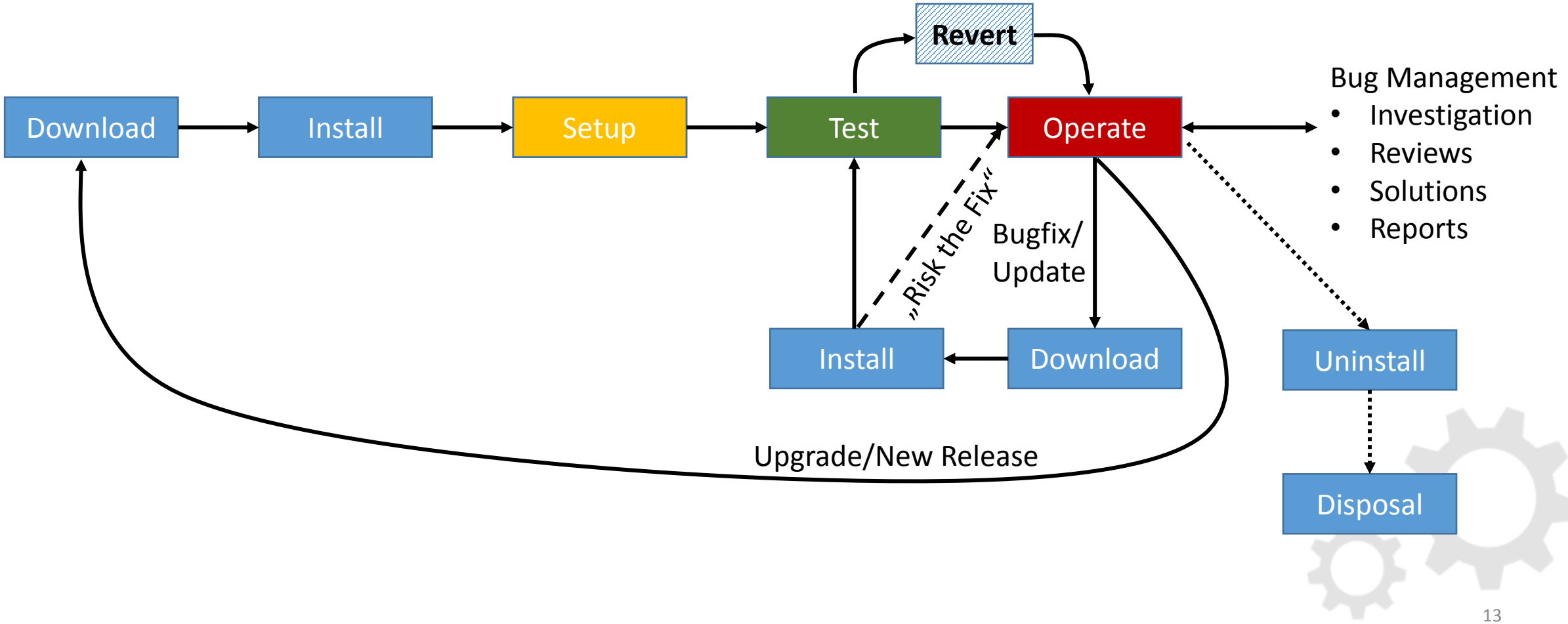
- Different phases of software
  - Software-as-written, software-in-delivery, software-at-rest, software-in-operation, software-end-of-support, software-end-of-life

Software Creation Needs Careful Consideration

- Different software development processes
  - From Waterfall to DevSecOps
- Requirements
- Architecture and Design and Review
- Coding and Review
- Assurance
  - Unit and functional testing
  - Static analysis
  - Security testing
- Risk Analysis



Software Operation: Management



Software Operation: Protection

- **Direct malicious attack to installed software**
  - *Static attack* to files (executables, setup config files, registry, databases)
  - *Dynamic attack* to running software
- Attackers need detailed knowledge about software
- **Protection against static attacks: signing and verification**
  - Signing of code, data in media files, registry and databases
  - Signing of setup files (XML)
- **Protection against knowledge transfer (“Know-How Protection”)**
  - Encryption of code, setup files, registry, databases
  - Obfuscation of code

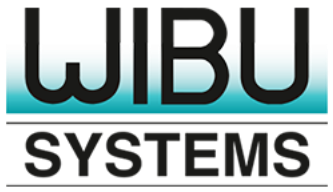
Software Protection Challenges

- Clean, easy-to-update code: easy to evaluate
- *Signing*, *encryption* and *obfuscation* adds *another* level of *complexity*
- **Result for Trustworthiness:**
  - Increase in *security/privacy*
  - Reduction in *reliability/resilience/safety*
- **Solution:**
  - *Keeping* protection as much as possible *out of original design/coding steps*
  - Static description of *protection methods* (parameter-based)
  - *Automatic tools* to add protection
- **Similar in Coding History:**
  - Fortran/C/C++ with *Highly Optimizing Compiler* instead *Optimized Assembler* code

From Concepts to Solutions…

- Software Trustworthiness, implemented by solutions from

GrammaTech Inc, founded 1988 by Tim Titelbaum and Thomas Reps, headquartered Ithaca, NY



Wibu-Systems AG, founded 1989, headquartered Karlsruhe Germany
North America Office in Edmonds, WA

GrammaTech, Inc – Static Application Security Testing

- Weaknesses and vulnerabilities in software-as-written and software-in-delivery
  - Source code and binaries
- Helping people test closer to software creation
  - Static analysis is perfect for this
  - Find bugs and vulnerabilities closer to the software creation process

CODESONAR®

- Deep static analysis for safety and security in DevSecOps
  - IEC61508, ISO26262, EN50128 and DO-178C
  - CWEs, MISRA, CERT-C, AUTOSAR
- Elaborate explanations and code navigation capabilities
- Customizable

Industrial Manufacturing

Software update crashed immediately after deployment. Turns out they forgot to run static analysis on one of the components and it had a null-pointer dereference.

CodeSonar found the null-pointer immediately and flagged it as high priority.

Medical Device - Asia

An automated test-case was sometimes behaving erratically and they could not find the root cause for several weeks.

CodeSonar flagged an uninitialized variable as the root cause.

CodeSonar: Introducing Static Analysis To Your Projects

- Rapid way to improve software quality and reduce cost
- First steps
  1. Go.grammatech.com, download CodeSonar
  2. Perform a scan on your software
  3. Review the feedback, fix the high-priority warnings
- Fine-tune the analysis, add/remove tests
- Integrate into your process and maintain
  1. Mark the remaining warnings as ‘baseline’
  2. Prevent the introduction of new warnings during your code review process

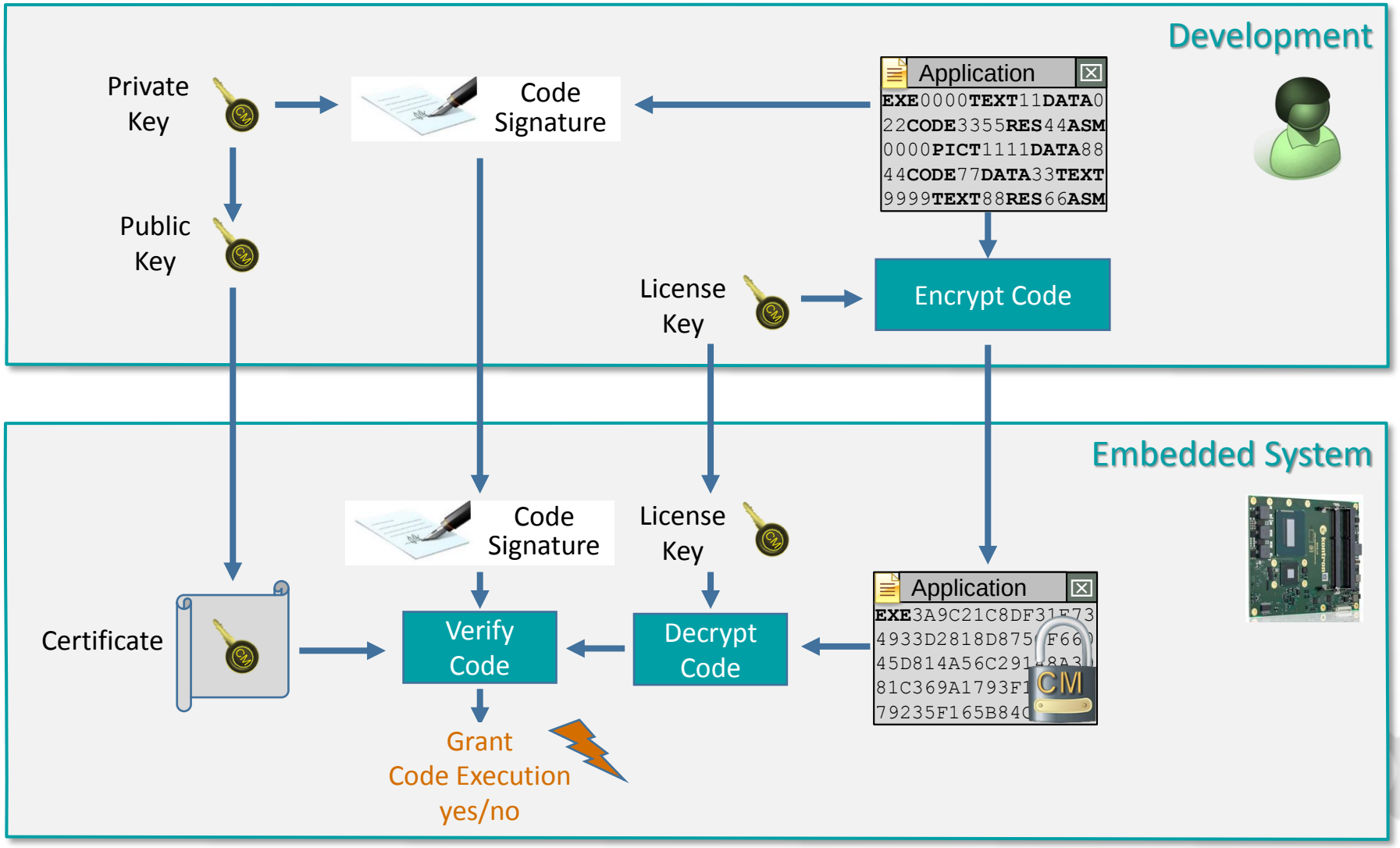
Wibu-Systems: Software Licensing and Code Protection

- **History of the Company: Software License Protection**
  - You can run only a *licensed* (= individually paid) software copy
  - Protection of the *execution*, not of the distribution/installation
  - Challenge: *Hackers* try to remove licensing protection
  - Solution: Better *protection* against *hacking* of licensing code
- **Software Licensing: Many Small Businesses with Small Quantities**
  - *Individual* integration into source code: *time intensive, failure-intensive*
  - Solution: *Automatic* tools to bind licensing to code, using *encryption*, *sealing* etc.
  - Ax/IxProtector with C/C++/.NET/Java for *compiled/tested binary* executables
  - Licensing bound to whole module (exe/dll) or single functions/methods

Wibu-Systems: Code Protection Against Malicious Attacks

- **Protection of Code against Reverse Engineering**
  - *Encryption of Code* (processor binary, MSIL, Java-Byte)
  - *Obfuscation of Naming* (MSIL, Java) and *Code* (processor binary)
  - *Signing of Modules* (exe/dll) and *Automatic Validation* during Execution (loading)
- **Protection of Embedded Code (Linux, VxWorks, QNX etc.)**
  - *Signing of Executables*
  - *Modified Loader* to check Signing of Executables
  - *Trust Chain* from *Loader* back to BIOS (*root of trust*)
- All Implementation Tools with *Low Impact* to *Performance*/original design

CodeMeter Embedded: Code Security during Field Update



Example: CodeMeter Software Licensing and Code Protection

Portable Medical Ventilator (COVID-19),
Fritz Stephan, Germany

- Feature-On-Demand licenses in field
- Protection against reverse engineering

https://www.wibu.com/us/case-studies/success-stories/story/detail/fritz-stephan-germany-medical-devices.html

References

- Link to paper *Software Trustworthiness Best Practices*
  https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf
- Introduction to IIoT
  https://en.wikipedia.org/wiki/Industrial_internet_of_things
- IIC *Industrial Internet Security Framework* (IISF)
  https://www.iiconsortium.org/IISF.htm
- IIC *Security Maturity Model* (SMM)
  https://www.iiconsortium.org/smm.htm
- Download of GrammaTech CodeSonar
  https://Go.grammatech.com
- CodeMeter Software Licensing and Code Protection Example
  https://www.wibu.com/us/case-studies/success-stories/story/detail/fritz-stephan-germany-medical-devices.html


Questions

Contact Details

- GrammaTech
  - https://go.grammatech.com
  - Mark Hermeling : mhermeling@grammatech.com
- Wibu-Systems
  - https://www.wibu.com
  - Marcellus Buchheit : mabu@wibu.com
- Forum for further questions and discussions (you are very welcome!)
  - https://community.iiconsortium.org/categories/webinars

OpenSystems media

AUDIENCE Q & A

Marcellus Buchheit,
Co-founder Wibu-Systems AG, President and CEO, Wibu-Systems USA>

Mark Hermeling,
Senior Director of Product Marketing, GrammaTech

GRAMMATECH

WIBU SYSTEMS

OpenSystems media

THANKS FOR JOINING US

Event archive available at
ecast.opensystemsmedia.com

E-mail us at
jgilmore@opensystemsmedia.com