Safe and Secure by Design:
Systems Engineering Best Practices for Connected Vehicles

Brett Hillhouse
WW Engineering Solutions Executive
Internet of Things, IBM

bretth@us.ibm.com

From last Sunday's 60 Minutes broadcast to numerous academic, industry and hacker publications, automobiles clearly have security exposures

- Hackers can infiltrate virtually any ECU (Electronic Control Unit) and through all wireless access points

- Hackers can directly create extremely unsafe conditions even through FM Radio ID

- The ease of these hacks exposed the fragility of the vehicle architecture

Displaying an arbitrary message and a false speedometer reading on the Driver Information Center. **Note that the car is in Park.**

"How Secure Is Your New Car? About the Same as Your PC", by Robert Charette, Mai 17, 2010, published in IEEE Spectrum Inside Technology [online] (URL:http://spectrum.ieee.org/riskfactor/green-tech/advanced-cars/how-secure-is-your-new-car-about-the-same-as-your-pc)

"Experimental Security Analysis of a Modern Automobile" from Koscher, K. Czeskis, A. Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., to be published in "*2010 IEEE Symposium on Security and Privacy*", [online] (URL: http://www.autosec.org/pubs/cars-oakland2010.pdf)

***See http://www.youtube.com/watch?v=bHfOzilwXic http://www.autosec.org/pubs/cars-oakland2010.pdf to understand just how vulnerable most vehicle systems are**

Many safety standards address elements of security

- Avionics/aerospace
  - **DO-178B/C** / ED-12B (RTCA/EUROCAE)
  - DO-178B is a widely accepted standard often used as a baseline for other certification efforts outside of avionics
- Medical
  - FDA 510(k) and IEC 60601
- Functional safety in process industry
  - IEC 61508
- Automotive
  - **ISO-26262** and MISRA-C
- Railway systems
  - EN50128 and EN50129
- Nuclear
  - IEC 880, IEC 60880, IEC 61513, IEC 62138

- Emerging security standards such as Open Group O-TTPS:

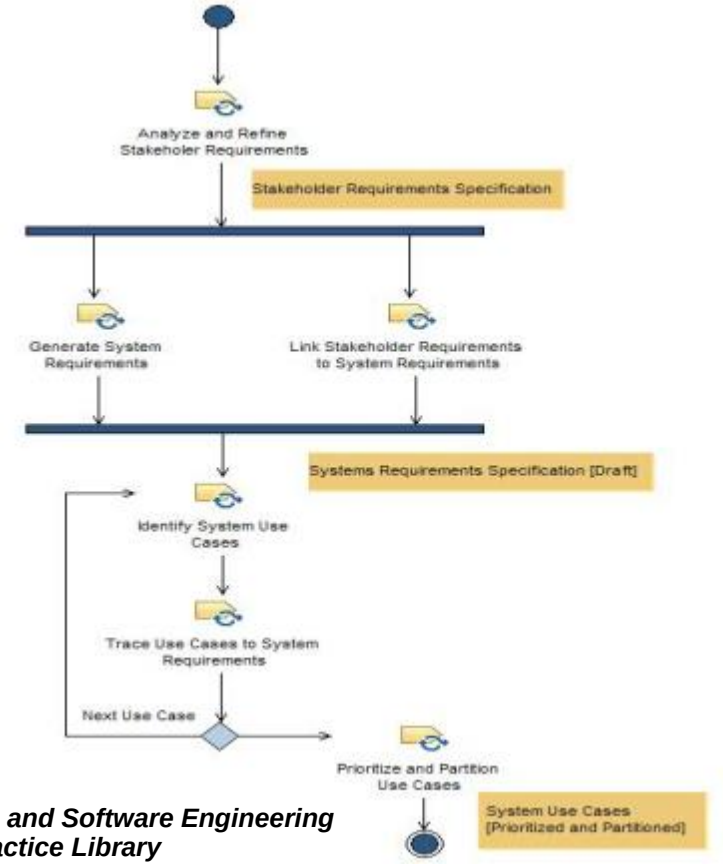
http://www.businesswire.com/news/home/20140203005300/en/Open-Group-Launches-Accreditation-Program-Strengthen-Global#.UvEeXBDZ7F0

Safety and Security are Critical *Aspects* of System Architecture

- No “magic box”
  - Disciplined approach to design
  - Rigorous verification
  - Follow industry best practices
  - Establish and prove process adherence
- System Architecture considers many aspects
  - End-to-end scenarios for safety, security
  - Focus on interfaces and interactions, and particularly APIs
- Other architecture aspects include performance, cost, reliability, etc.

Need for Process Compliance and Best Practices

- **Adopt proven safety and security design practices**
- **Manage compliance** with pre-defined methods and mappings to industry standards and regulations – e.g. **CMMI, Automotive SPICE**
- **Use Model-Driven Development** and practice early validation through simulation
- **Practice Test-First / Test-Driven Development**
- **Ensure Disciplined Requirements Management**
- **Automate Traceability and Reporting**



IBM Rational Systems and Software Engineering Best Practice Library

Best Practice Example: Typical Automotive practices today combine functional requirements with system design / architecture

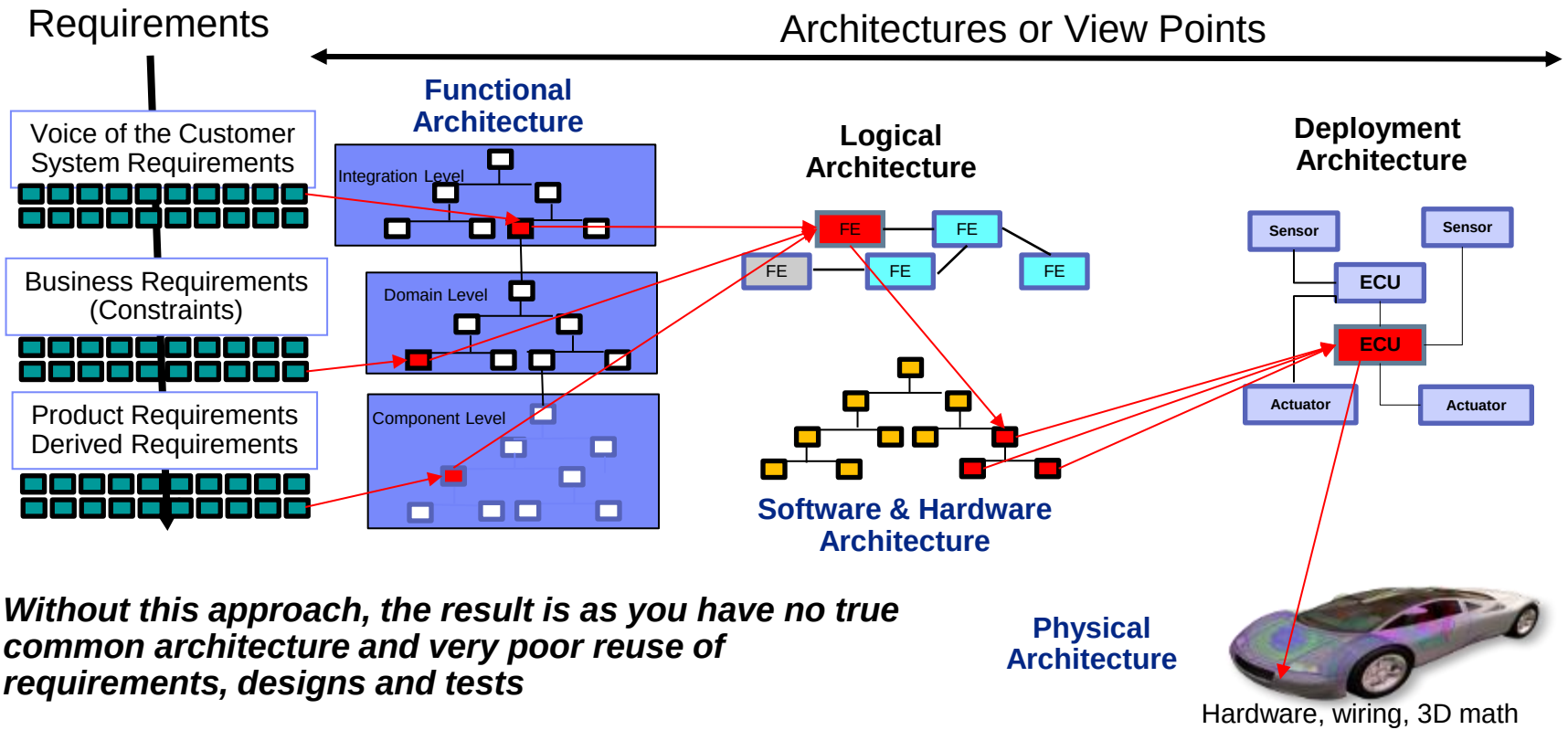
- Allocation has often been 'bundled' into a requirement
  - *"The ECM Safety System implementation shall be partitioned between two real-time processors, the Main Processor and the Main Processor Monitor"*
  - *"The ECM shall transmit the signals Hood Status and Hood Status Validity."*
  - *"The BCM shall provide a Headlamp reminder if…"*

- The goal is to remove the allocation information from the requirement, thus creating a requirement that can be reused across many designs

- Best Practice Example Feature Requirement
  - *"Microprocessors involved with Safety Critical operations shall be able to detect ALU errors, including math library and instruction set."*

- Best Practice Example ECU Requirement
  - *"An ECU Safety System implementation shall be partitioned between two real-time processors"*

System Design / Architecture
Model Based Systems Engineering



Without this approach, the result is as you have no true common architecture and very poor reuse of requirements, designs and tests

Why isn't this more common today in Automotive?

- Mechanical background still prevalent in management
- Historically added new hardware/ECU for each new function needed
- Investment in software vs. mechanical development
  - Software Engineering Center of Excellence
  - Career path – systems engineers/architects
  - IT Expenditures
- VP Quality focused on testing
  - Aerospace, Medical Device manufacturers' Quality organizations focused on common processes and methodology in Engineering and Test
- Automotive EE Engineering education largely focused on algorithm development

"We don't have a lot of software engineers in Automotive today. We have a lot of Electrical Engineers who have learned how to write C code – poorly"

Software Lead Engineer – Automotive OEM

Connected car is transformative, and adds another dimension of complexity

Automotive can leverage evolving standards to help address this

To be secure, scalable and efficient, the Internet of Things (IoT) networks will evolve to be more open and decentralized

A secure and scalable IoT solution can be built on a decentralized foundation of three key transactions

Trustless Peer to Peer Messaging

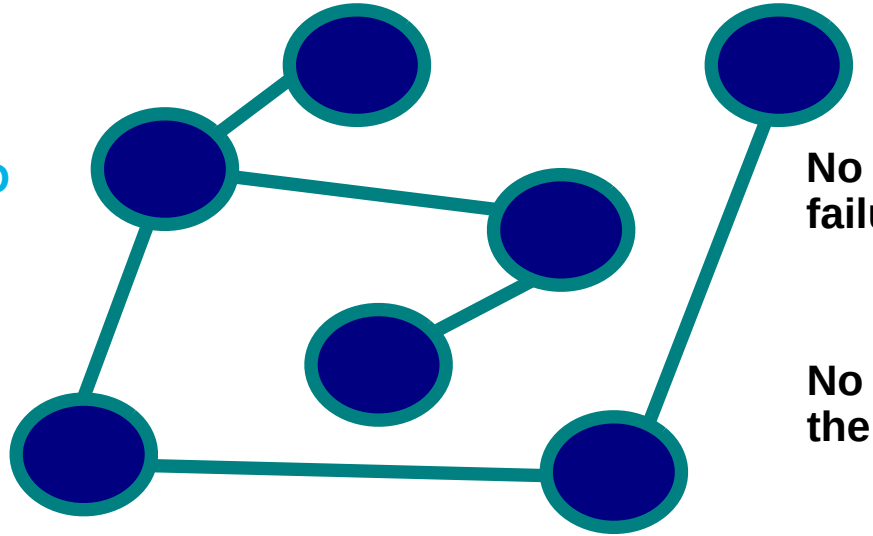
Secure Distributed File Sharing

Autonomous Device Coordination

Autonomous coordination across a decentralized network can be achieved by consensus and validation

Transactions can be confirmed by DISTRIBUTED CONSENSUS

Multiple participants can check on each transaction to provide REDUNDANT VERIFICATION



No single point of failure

No need to trust all the participants

All participants can see all the transactions and many participants verify the work of each transaction

At the heart of decentralized systems such as Bitcoin is a revolutionary platform – the "blockchain"

Traditional banks are built on private, centralized systems:

Account owners

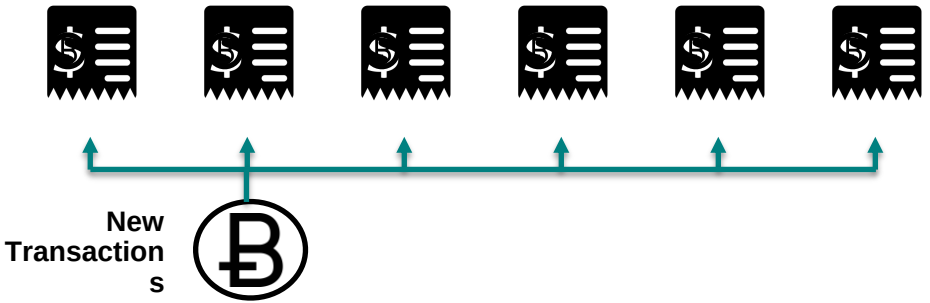
Bank balances

Transaction records

There is one central ledger for accounts, identities, and transactions.

In Bitcoin, the central functions are distributed to all the participants in the system:

Every user has access to their own copy of the transaction ledger in a long ledger called the BLOCK CHAIN



CRYPTOGRAPHY is used to verify transactions and keep information private

New currency is issued to users as a REWARD for doing the computation "work" involved in verifying transactions.

For more information visit ibm.com/rational/solutions/automotive