Presentation to TMF

Testing the Internet of Things

Test and Verification Solutions

Delivering Tailored Solutions for
Hardware Verification and Software Testing

TVS
Test and Verification Solutions

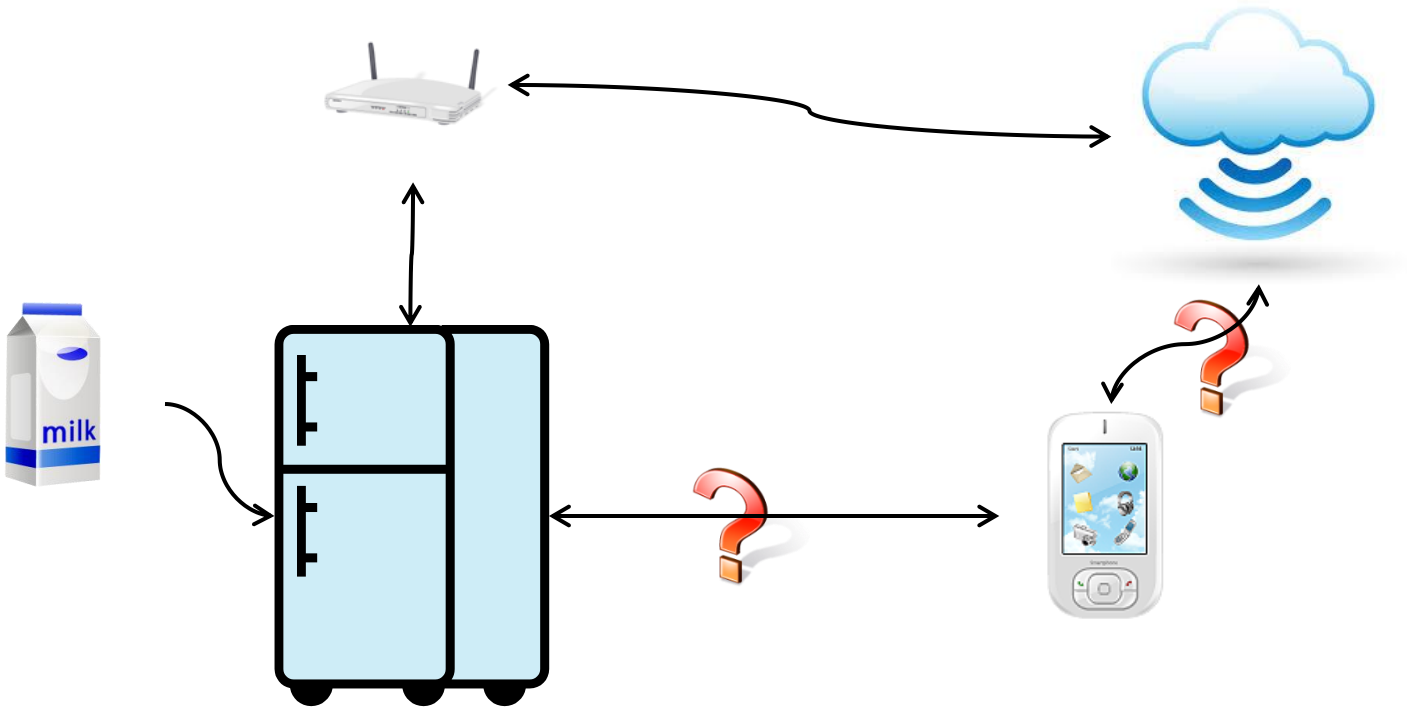
What is the IoT?

- **Wikipedia**
  - The Internet of Things refers to the interconnection of uniquely identifiable embedded computing like devices with the existing Internet infrastructure
- **Need to consider the technology**
- **But better understood through the applications**

Technology

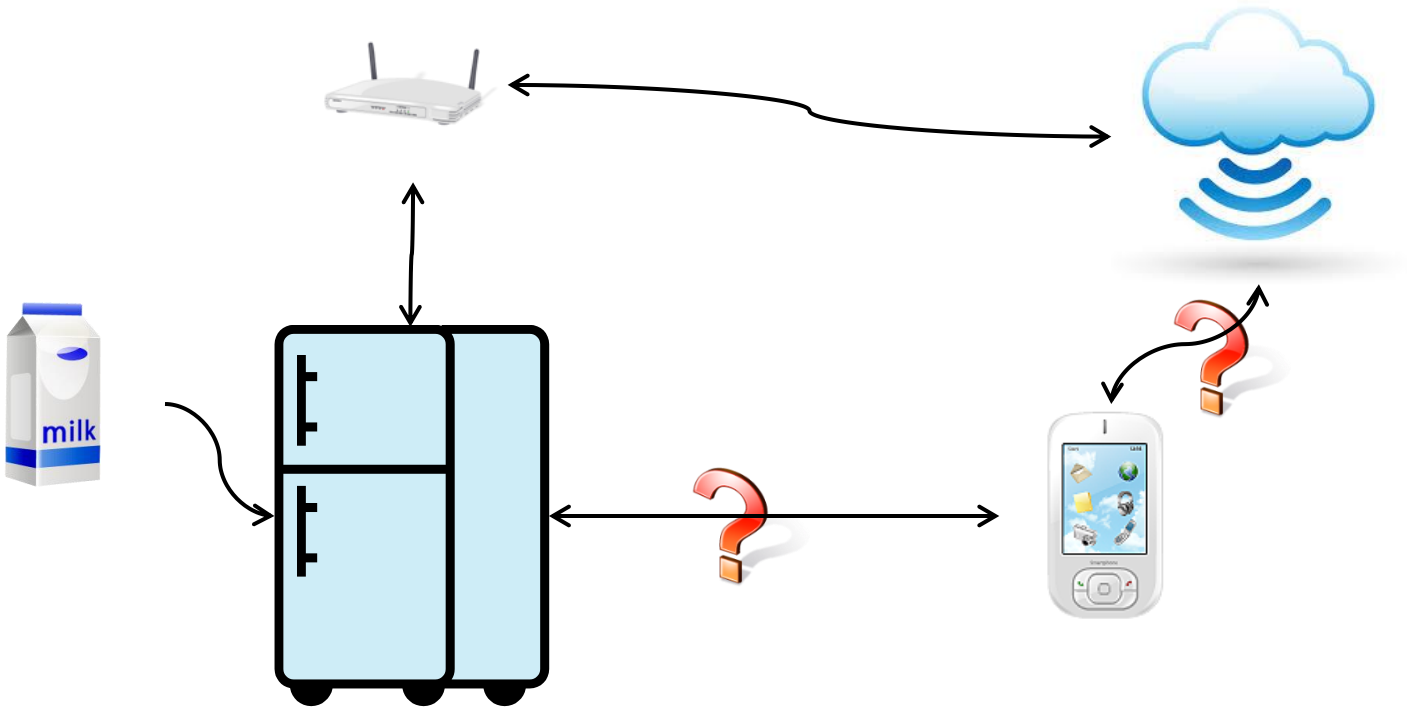
- Possibly RFID (Radio Frequency Identification) tags + EPC (Electronic Product Code) -> EPCIS (EPC Information Services)
- Linked by ONS (Object Naming Service)
- PET (Privacy Enhancing Technologies): VPN (not global), TLS (slow), DNSSEC (not adopted globally), Onion routing (slow), PIR (impractical), P2P (maybe), Hypercat (maybe)
- Competing standards not yet reconciled

A simple “well known” application: The Smart Fridge



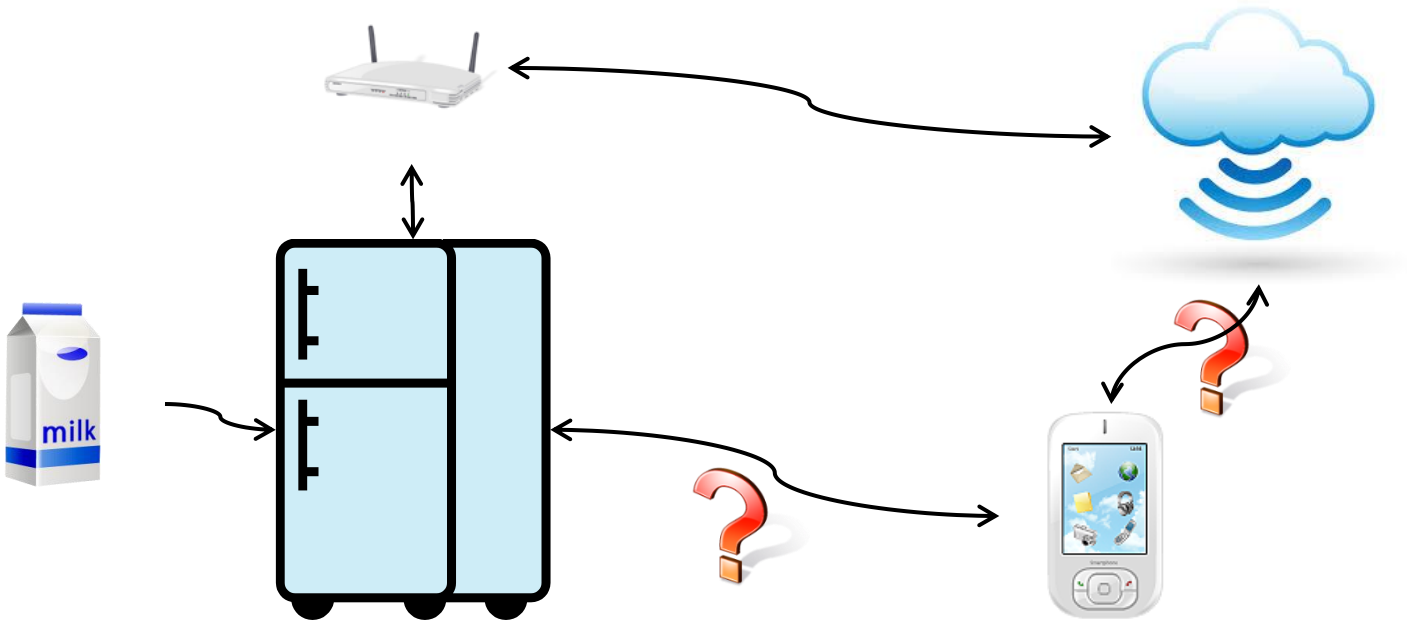
- **Who is involved?**
  - The milk manufacturer
  - The app developer

Testing the milk bottle



- **Responsibility of the manufacturer**
  - Ensuring it obeys the protocols
  - Ensuring an application can access the required data
  - Security
- **Responsibility of the app developer**
  - Errors in the milk bottle interaction
  - Data integrity
  - Security

Testing the app

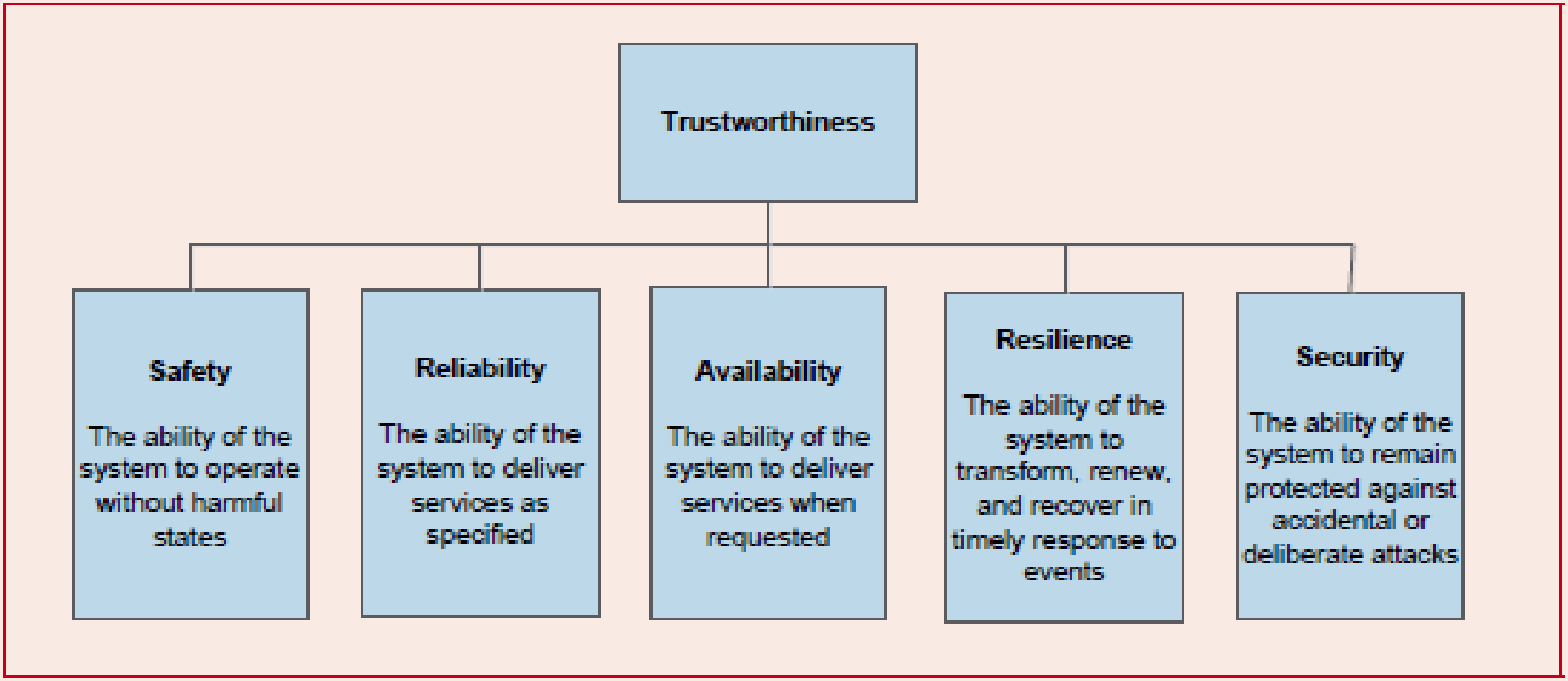


- **Responsibility of the manufacturer**
  - Anything???
- **Responsibility of the app developer**
  - Usual distributed app functional testing
  - These are autonomous systems
    - So a lot of non-functional aspects to verify

V&V of Autonomous Systems Software

- **PAS 754:**2014
  - UK Trustworthy Software Initiative (TSI)

Figure 1 – Facets of trustworthiness



V&V of Autonomous Systems Software

- **Traditional structured approach to testing**
  - Unit, integration, subsystem, system
- **But system level testing changes**
  - Noise in the system
  - Discovering boundaries of correct performance
  - Emergent behaviours
- **Facets of trustworthiness**
  - Safety, Reliability, Availability, Resilience, Security

Scare Stories?

- **Car was “programmed” to stop in fast lane**
- **Drone ditches into housing estate**
- **Criminals steal Amazon deliveries**
- **Disappearing cars – cars drive themselves into arms of thieves**

Toyota Prius cars that are being recalled to fix a hybrid control unit glitch that can cause the cars to automatically shut down and enter a limp-home failsafe mode

Online marketplace eBay is forcing users to change their passwords after a cyber-attack compromised its systems. The US firm said a database had been hacked between late February and early March, and had contained encrypted passwords and other non-financial data.

Example Automotive Applications

- **Passengers using cars services**
  - Accessing wifi, music+videos, time to destimation, etc
- **Smart parking**
  - Help to find a parking space
  - Automated parking
- **Augmented Awareness**
  - ADAS (Advanced Driver Assistance Systems)
  - Driver stays in charge
    - Identifies a cyclist in the blind spot
- **Driverless Cars**
  - Autonomous Systems Software

Safety Critical Automotive Applications

- **Passengers using cars services**
  - Accessing wifi, music+videos, time to destimation, etc
- **Smart parking**
  - Help to find a parking space
  - Automated parking
- **Augmented Awareness**
  - ADAS (Advanced Driver Assistance Systems)
  - Driver stays in charge
    - Identifies a cyclist in the blind spot
- **Driverless Cars**
  - Autonomous Systems Software

Safety Standards

- **IEC61508:** Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- **DO178:** Software considerations in airborne systems and equipment certification
- **EN50128:** Software for railway control and protection systems
- **IEC60880:** Software aspects for computer-based systems performing category A functions
- **IEC62304:** Medical device software -- Software life cycle processes
- **ISO26262:** Road vehicles – Functional safety

Key Elements

- Plans & Standards
- Requirements
- Design Specifications
- Reviews and Analyses
- Testing (against specifications)
  - Unit
  - Software Integration
  - Software System
- Test Coverage Criteria
- Traceability
- Independence

IEC61508

- **Dynamic analysis and testing**

Technique	SIL 1	SIL 2	SIL 3	SIL 4
Structural test coverage (entry points) 100%	HR	HR	HR	HR
Structural test coverage (statements) 100%	R	HR	HR	HR
Structural test coverage (branches) 100%	R	R	HR	HR
Structural test coverage (conditions, MC/DC) 100%	R	R	R	HR
Test case execution from boundary value analysis	R	HR	HR	HR
Test case execution from error guessing	R	R	R	R
Test case execution from error seeding	-	R	R	R
Test case execution from model-based test case generation	R	R	HR	HR
Performance modelling	R	R	R	HR
Equivalence classes and input partition testing	R	R	R	HR

Is Reliable Software Expensive?

40-50% project effort on avoidable rework

Extra 50% cost to develop high integrity software

Extra 75% cost to maintain low integrity software

Source: Boehm – Software Management Article 2001

Presentation to TMF

Interthreat of Things – The security considerations

Test and Verification Solutions

Delivering Tailored Solutions for Hardware Verification and Software Testing

TVS
Test and Verification Solutions

FUD (Fear, Uncertainty and Doubt)

- **So far there have been very few malicious IoT attacks.**

http://www.dailymail.co.uk/sciencetech/article-2384826/Satis-smart-toilets-Japan-hacked-hijacked-remotely.html

http://uk.pcmag.com/news/13737/japanese-smart-toilet-vulnerable-to-hackers

- **IoT devices are currently insecure.**
- **Criminal hackers are usually motivated by money, not publicity.**
- **When 'Things' start processing financial data attacks will become commonplace.**
- **Updates to deployed 'Things' will be infrequent.**

http://www.bbc.co.uk/news/technology-28344219

http://www.ducksley.com/2013/12/cia-drone-blows-up-google-driverless-car/

Attack Vectors

- **Huge increase in attack surface**
- **Initial criminal attacks will probably follow known vectors:** ***Mapping the Objects and Servers; Identifying functionality; Bypassing client-side controls; Attacking authentication, session management, and access controls; Injecting code; Path traversal; Application logic and erasing audit trail; Other users (XSS / XSRF / hi-jack / redirection etc); Exploiting information disclosure; Overflow; Attacking Architecture, servers and source code.***
- **Expect massive use of automation in attacks.**

Innovation & Risk

- New technology will be closely followed by new attacks, then new defences.
- Reduced barriers to entry will create more IoT entrepreneurs and technologists, with no security skills.
- Creativity tools will probably be security-lite
- Threat assessment will be important.
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014

Can ‘Things’ be turned off?

(Faraday cages, ‘killing’ the tag, dissolution of connection)

Defences

- Secure by design
- Secure coding practices
- Tested for security
- Perimeter (network) defences
- Secure Technology, Processes, and People