BIRMINGHAM CITY
School of Computing
and Digital Technology

Is Agile Certification an Oxymoron?

Paul Kearney

Professor of Cybersecurity (part time)

Outline of talk

- Motivation
- Conventional approach to certification
  - Anatomy of a certification scheme
  - Some initiatives relevant to IoT security
  - Benefits of product security certification
  - Problems with certification (at present)
- Towards Agile Certification
  - Goals for agile certification
  - Of systems and environments
  - Whole lifecycle approach
- Conclusions

Motivation for product security regulation and certification

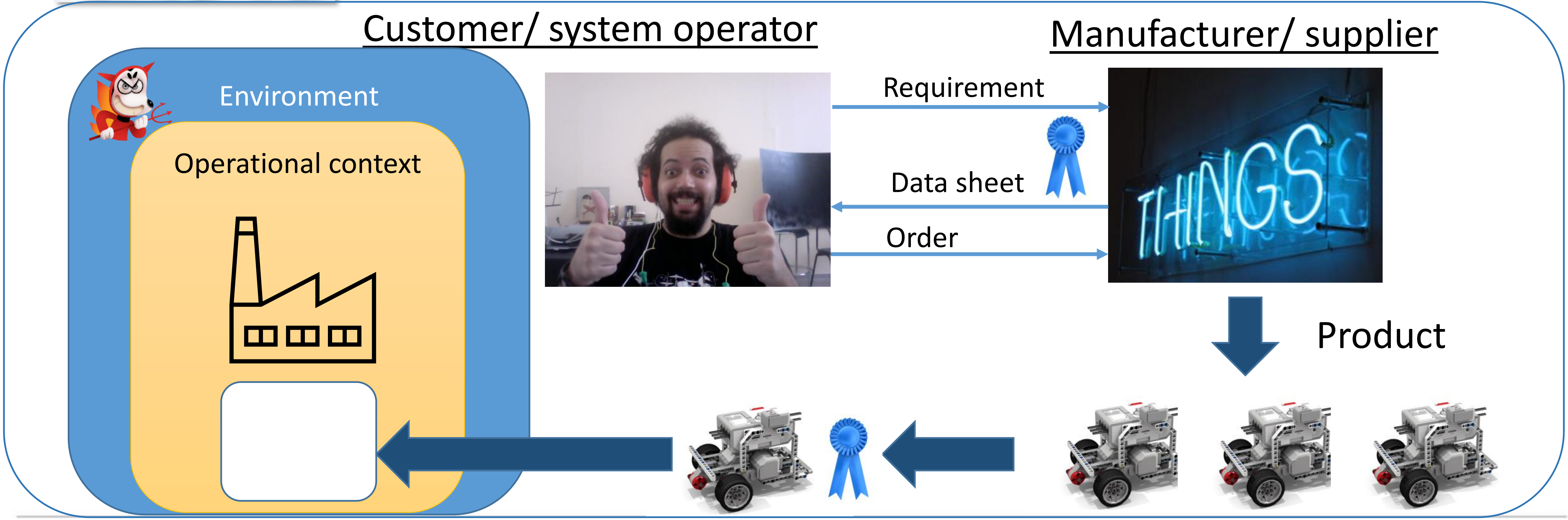
Extract from introduction to proposed EU Cyber Resilience Act

General statement, but particularly true of IoT products

> ***Hardware and software products*** *are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021. Such products* ***suffer from two major problems adding costs for users and the society: (1) a low level of cybersecurity****, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them,* ***and (2) an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.*** *In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, often propagating across the borders of the internal market within a matter of minutes. This can lead to severe disruption of economic and social activities or even become life threatening.*

Three stakeholder perspectives

Regulator / industry body



Customer/ system operator

Manufacturer/ supplier

Environment

Operational context

Requirement

Data sheet

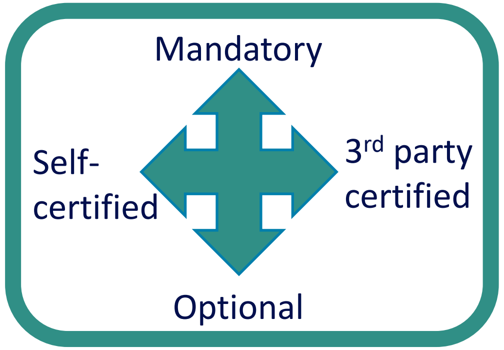
Order

Product

Anatomy of a certification scheme

Product certification:

- Supplier or authority attests that (all instances of) a product complies(/y) with a standard (provided instructions followed).
- Often dealing with a class of products and/or application settings

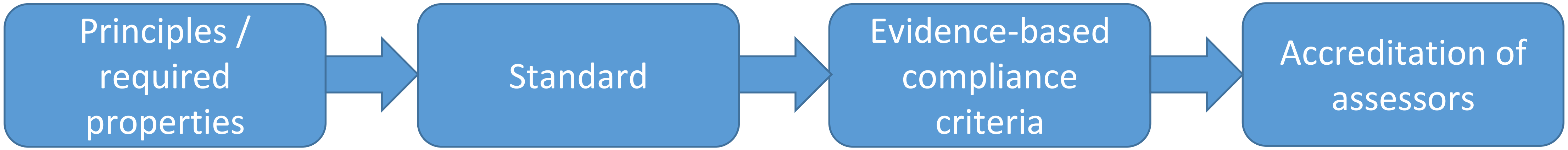

Mandatory

Self-certified

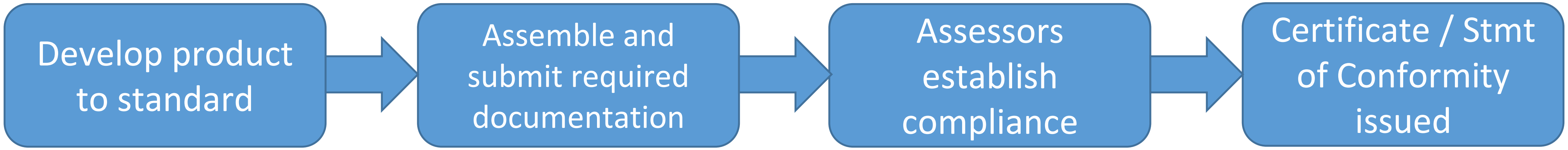
3rd party certified

Optional

Development of scheme


Principles / required properties → Standard → Evidence-based compliance criteria → Accreditation of assessors

Application of scheme


Develop product to standard → Assemble and submit required documentation → Assessors establish compliance → Certificate / Stmt of Conformity issued

Some relevant legislation, frameworks and standards

Essential/baseline requirements similar, but scope for harmonisation

- ➢ **European Cybersecurity Certification Framework (ECCF)**
- Established by EU Cybersecurity Act (passed in 2019)
- Union Rolling Work Programme of certification schemes – IoT and IACS schemes may be coming soon
- ➢ **Proposed European Cyber Resilience Act**
- Regulation on cybersecurity of "*products with digital elements*" whose use includes a data connection to a device or network
- Would be mandatory. Fines of up to €15M or 2.5% of global turnover
- ➢ **UK Code of Practice for Consumer IoT security**
- ➢ **UK Product Security and Telecomms Infrastructure Bill**

- ➢ **European Standard ETSI EN 303 645**
- Cyber Security for Consumer Internet of Things: Baseline Requirements
- TS 103 701 specifies conformance methodology
- ➢ **NIST CSWP.02042022-2**
- Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products
- Builds on IR8259/A/B
- Proposes baseline product criteria as well as labeling and conformity assessment considerations
- ➢ **IoTSF Assurance Framework**

EU Cybersecurity Certification Framework

Minimum security objectives for a cybersecurity certification scheme

(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;

(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;

(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;

CIA

(d) to identify and document known dependencies and vulnerabilities;

(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;

(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

Dependencies and vulnerabilities

(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

Auditability

(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;

Recoverability

(i) that ICT products, ICT services and ICT processes are secure by default and by design;

Security by Design and Default

Benefits of product security certification schemes

… at least in theory

➢ **Regulator:**

- Incentivise suppliers to improve security of products
- Protect honest suppliers from unfair competition
- Educate customers
- More secure and resilient services available to society

➢ **Supplier:**

- Clarify security properties required for target market sector
- Marketing value, evidence of trustworthiness
- Certification may be required for entry into some markets

➢ **Customer:**

- Simplifies procurement process
- Reduces work required for assurance of system security
- Evidence of best practice for its customer and regulator

Problems with certification (at present)

- Time consuming and labour intensive. Delays market entry, increases cost and hence price. Leads to competitive disadvantage outside regulated industries.
- Unless valued intrinsically by customers, limited incentive to certify products.
- Pace of technical change faster than certification timescale.
- Certification schemes take a long time to develop and tend to lag the market.
- Variety of products and contexts mean that many different standards/profiles are required.
- Certification applies to one product version at a point in time:
  - What/how much can be changed before re-certification required?
  - What happens when threat environment for that product class changes?
  - What happens when operational environment for that product class changes?
  - Standards get updated. A product certified against one version may fail against a later version.
- Supply chain issues. Trust in/between certification authorities.
- Does certification actually increase security?
- Security ‘does not compose’.

Goals for Agile Certification (1)

- Scheme is, and remains, fit for purpose:
  - Always relevant to the needs of customers in selecting products, operating them securely as part of a larger system, and assuring the security properties of the system.
- Lean and mean, little overhead in cost or time
  - Certification should add value, not reduce it
- Harmonisation and modularity of certification schemes
  - Can leverage one certification to gain another
- 'Whole lifecycle' approach
  - Certification-related activities integrated with other processes, and integrated end-to-end. DevSecOpsCert?

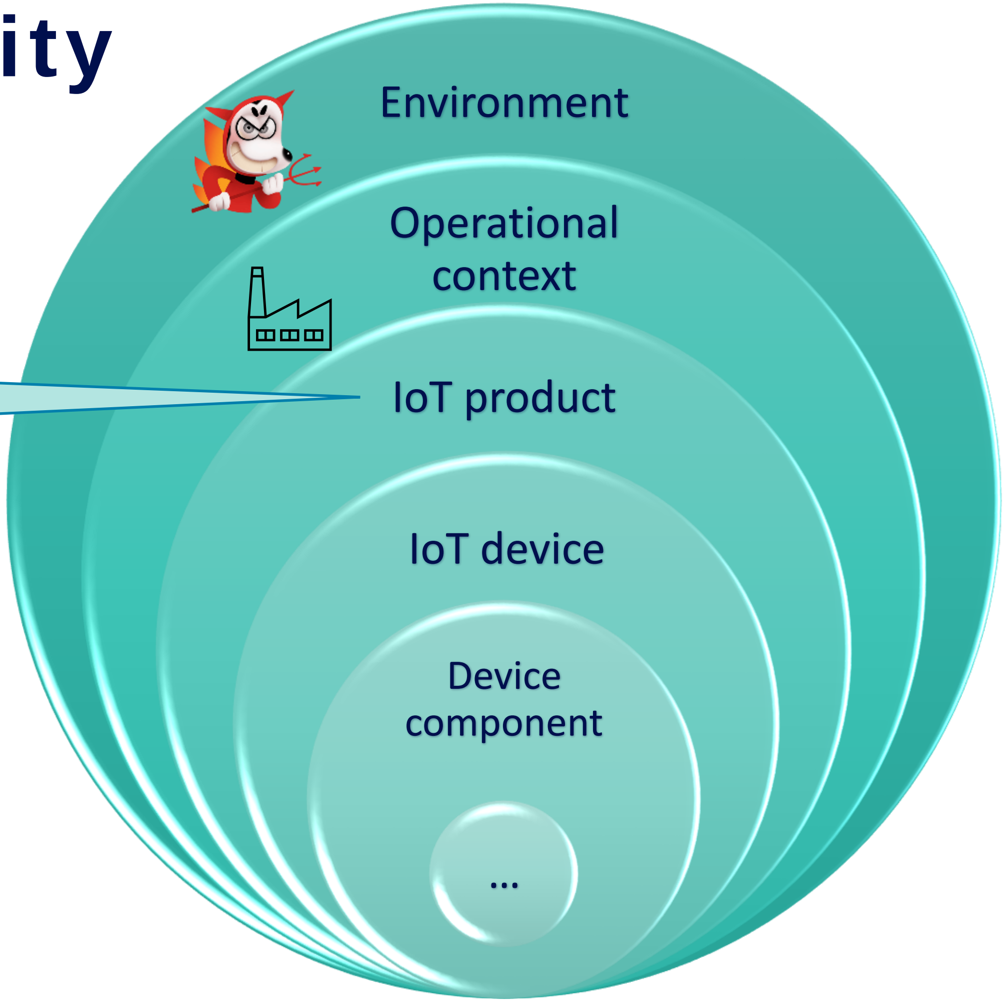
Goals for Agile Certification (2)

- Holistic approach linking scheme, certification and operational lifecycles
  - Certification status can change in response to changes to scheme, threat, operational experience, etc. Allows for retrospective update, withdrawal or exemption of already-certified products and their instances.
  - Operational experience can drive changes to certification scheme.
- Intelligent automation and support
  - Clear declarative semantics that is meaningful to person and machine. 'Logic' for reasoning about claims, evidence and trust.
- Recursive (de)composability
  - verify/predict security properties of systems from the properties and relationships of their components.

Recursive (de)composability

It's turtles all the way down!

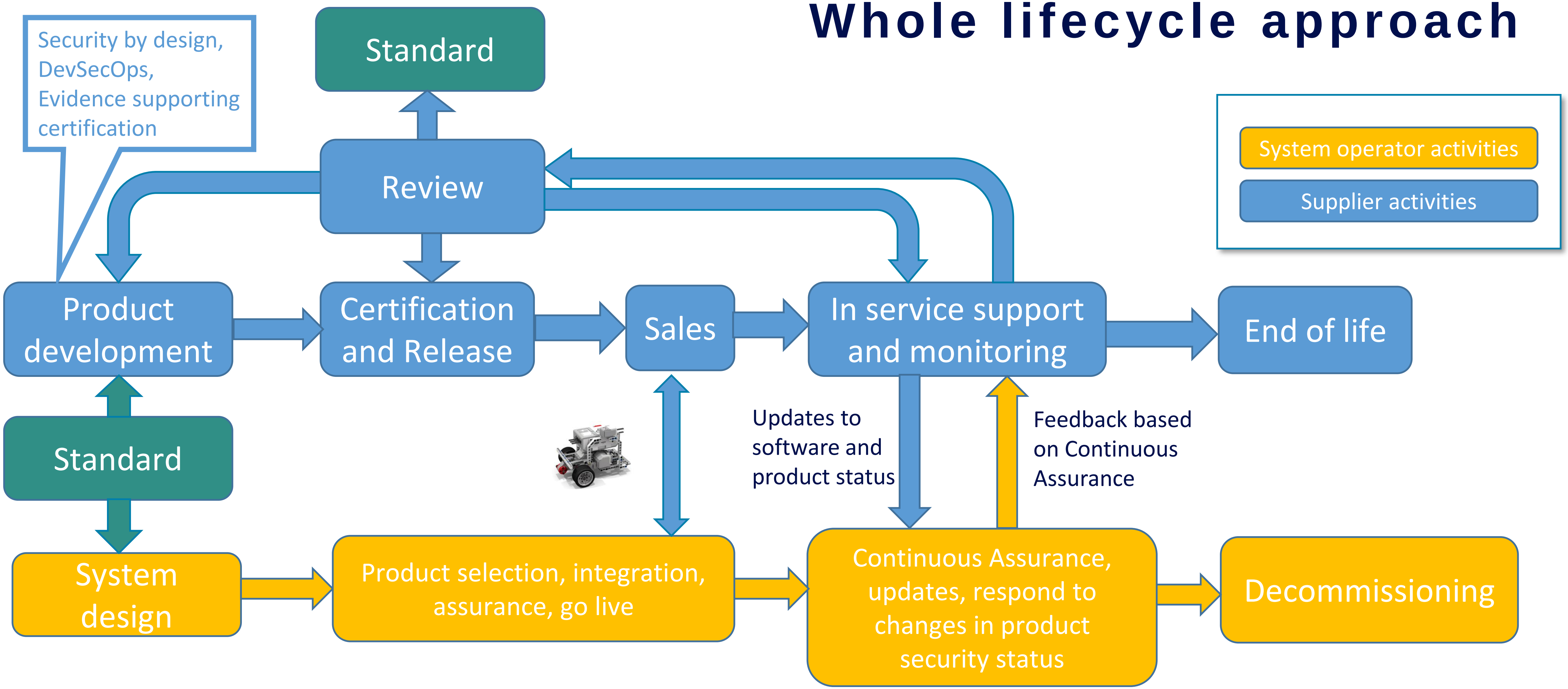
NIST CSWP: IoT device plus components that are necessary to use it.



Want 'algebra' or 'recipe book' for verifying/predicting security properties of systems made up of components combined in a particular way.

- Library of design patterns?
- Reference architectures and building blocks?

Whole lifecycle approach



Security by design, DevSecOps, Evidence supporting certification

Standard

Review

Product development

Certification and Release

Sales

In service support and monitoring

End of life

Standard

System design

Product selection, integration, assurance, go live

Continuous Assurance, updates, respond to changes in product security status

Decommissioning

Updates to software and product status

Feedback based on Continuous Assurance

System operator activities

Supplier activities

Conclusions

- Need to raise the level of cybersecurity in IoT products and the systems they are deployed in is widely recognised.
- Many initiatives to address this through mandatory regulations and voluntary certification schemes.
- Conventional schemes involve a static assessment of a specific product, and are lengthy, ‘paper heavy’, and resource and capital intensive, which acts as a disincentive to their adoption.
- Agile Certification takes a dynamic, whole lifecycle approach to reduce costs, automate maintenance, be scalable, sustainable, and timely in delivery.
- Need to establish an Agile Certification research agenda to bring together related strands of work to address the many challenges.

Questions for discussion later:

- Is Agile Certification achievable?
- What is the alternative to product security certification / regulation?