Security classes, relevance for cloud services

Josef Noll, (on behalf of the SCOTT team)

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

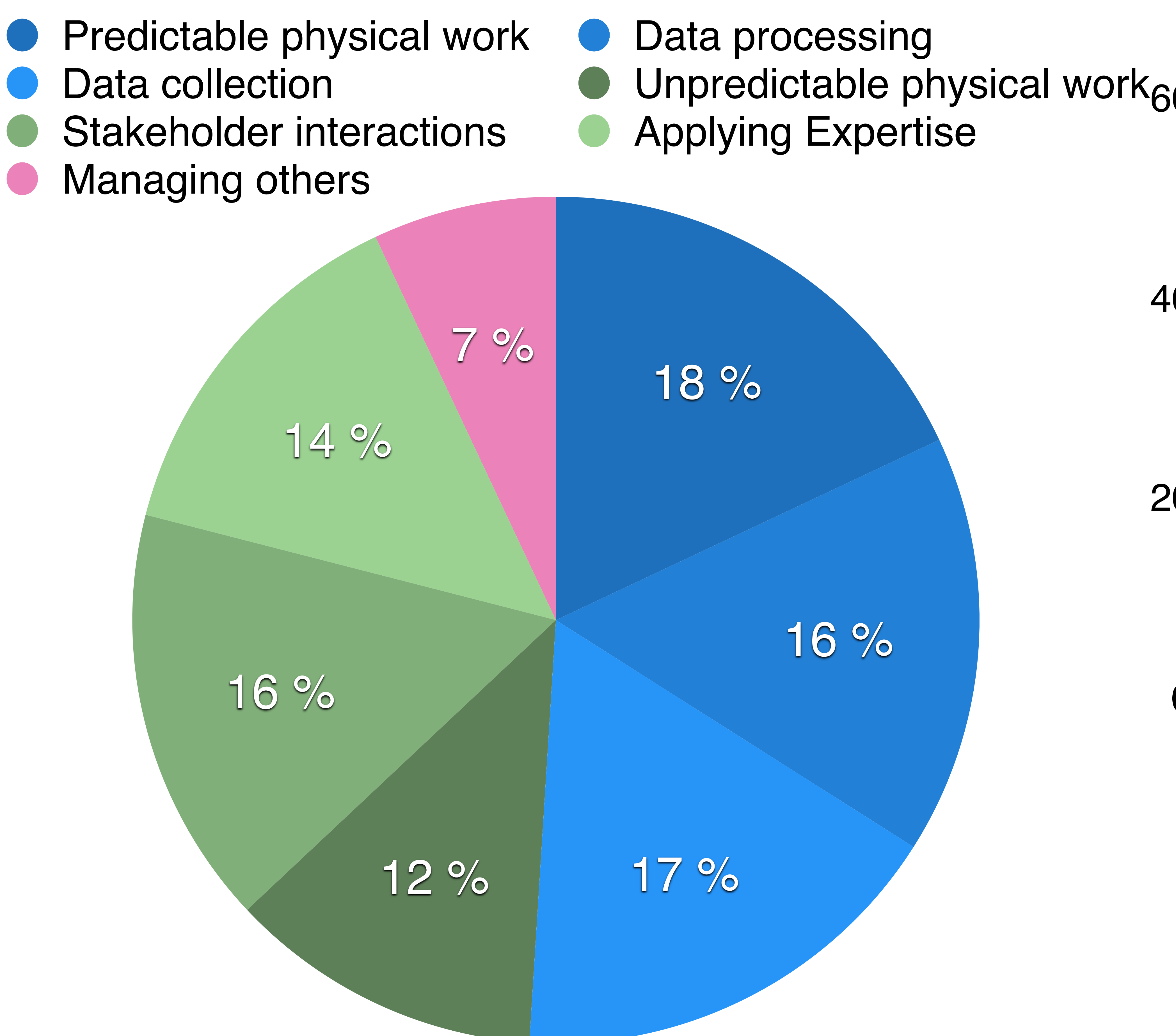
Secure COnnected Trustable Things key message

IoT is the game changer and driver for digitalisation, and SCOTT contributes through:

- **Answer the IoT need for a new and more advanced security paradigm through security classes**
- **Create a Convincing privacy assessment through privacy labelling**
- **Establish a clear link between security and safety**

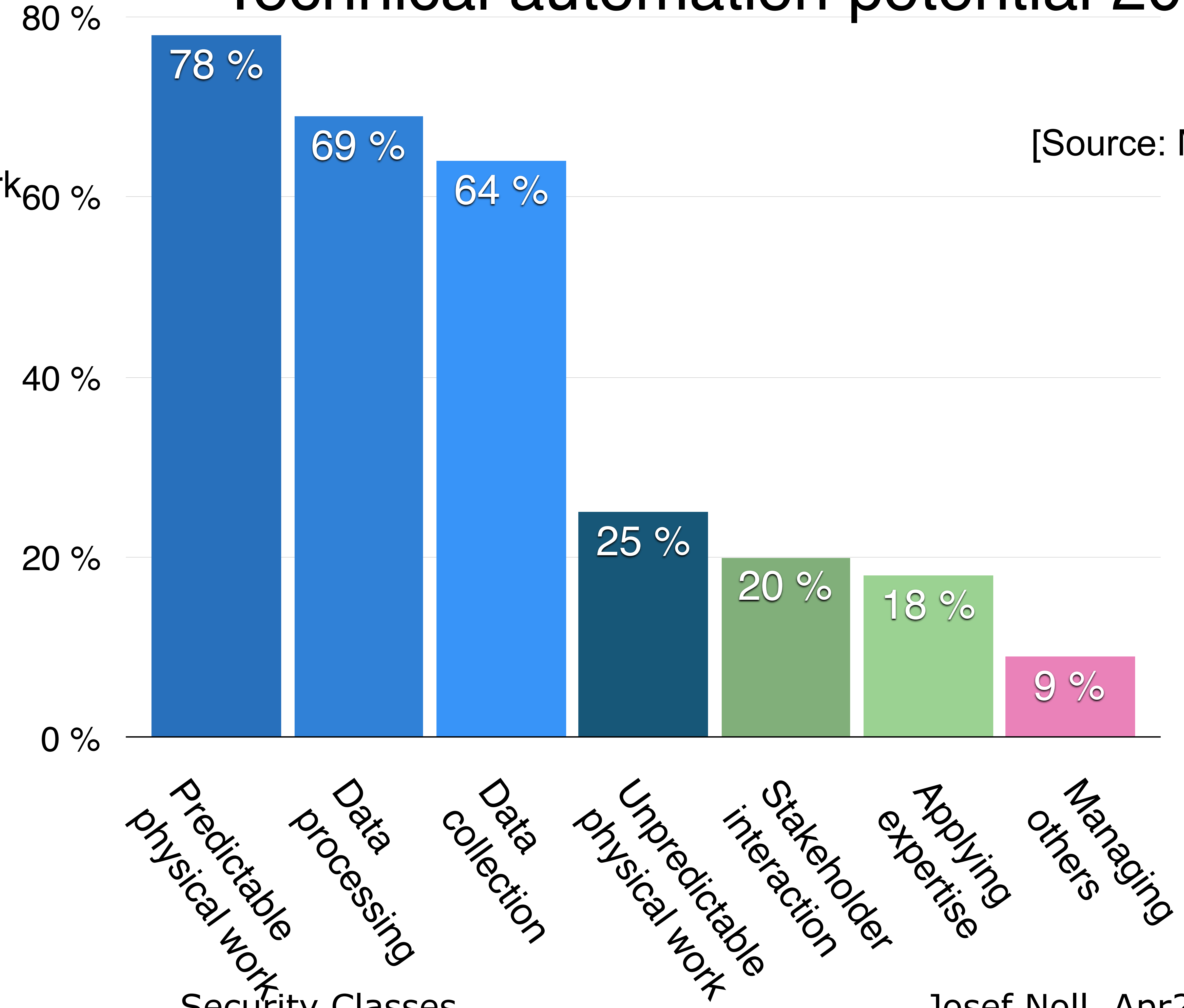
The challenge from automation

USA work force time spent [%]



Technical automation potential 2016 [%]

[Source: McKinsey, 2016]

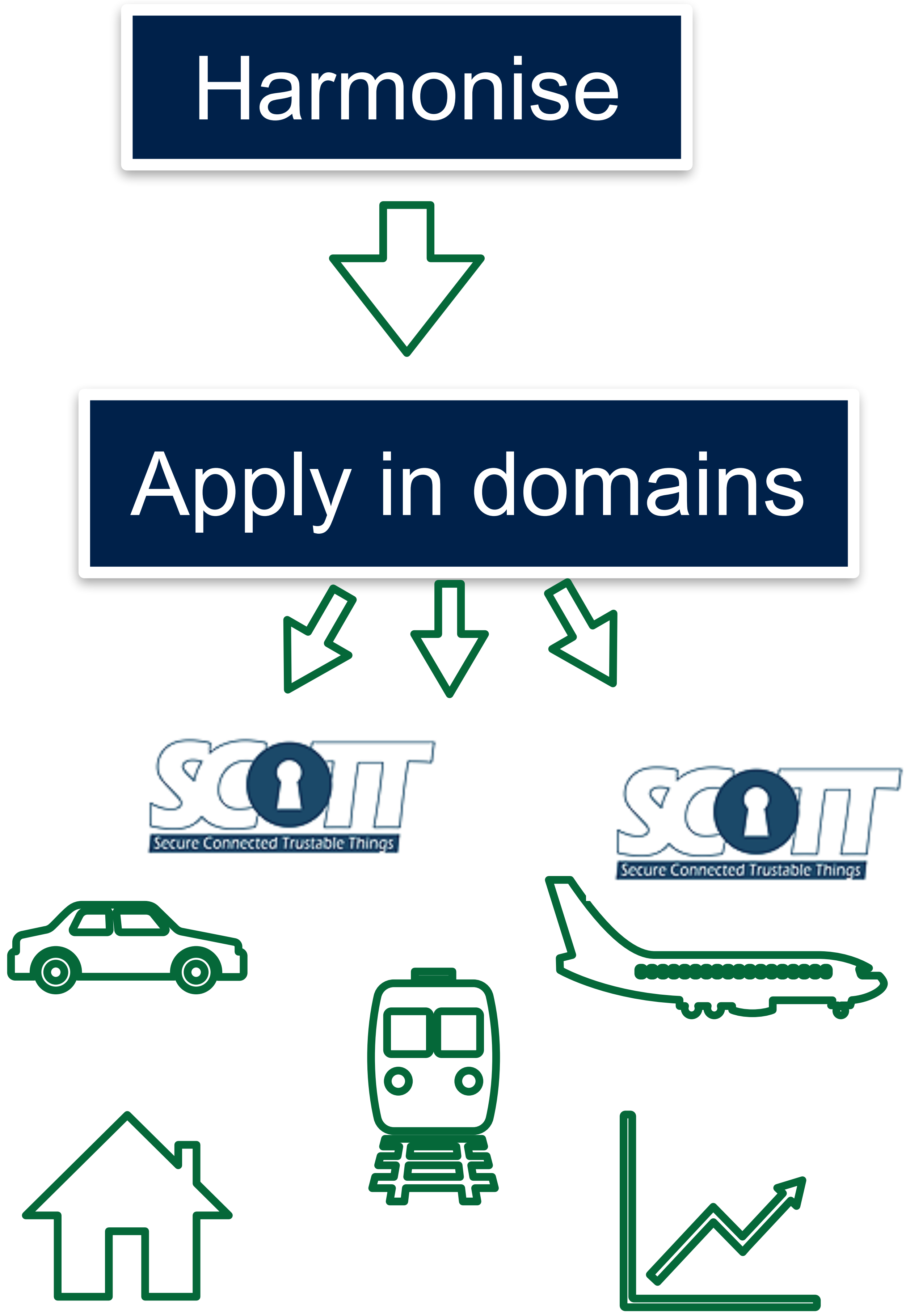


Security Classes

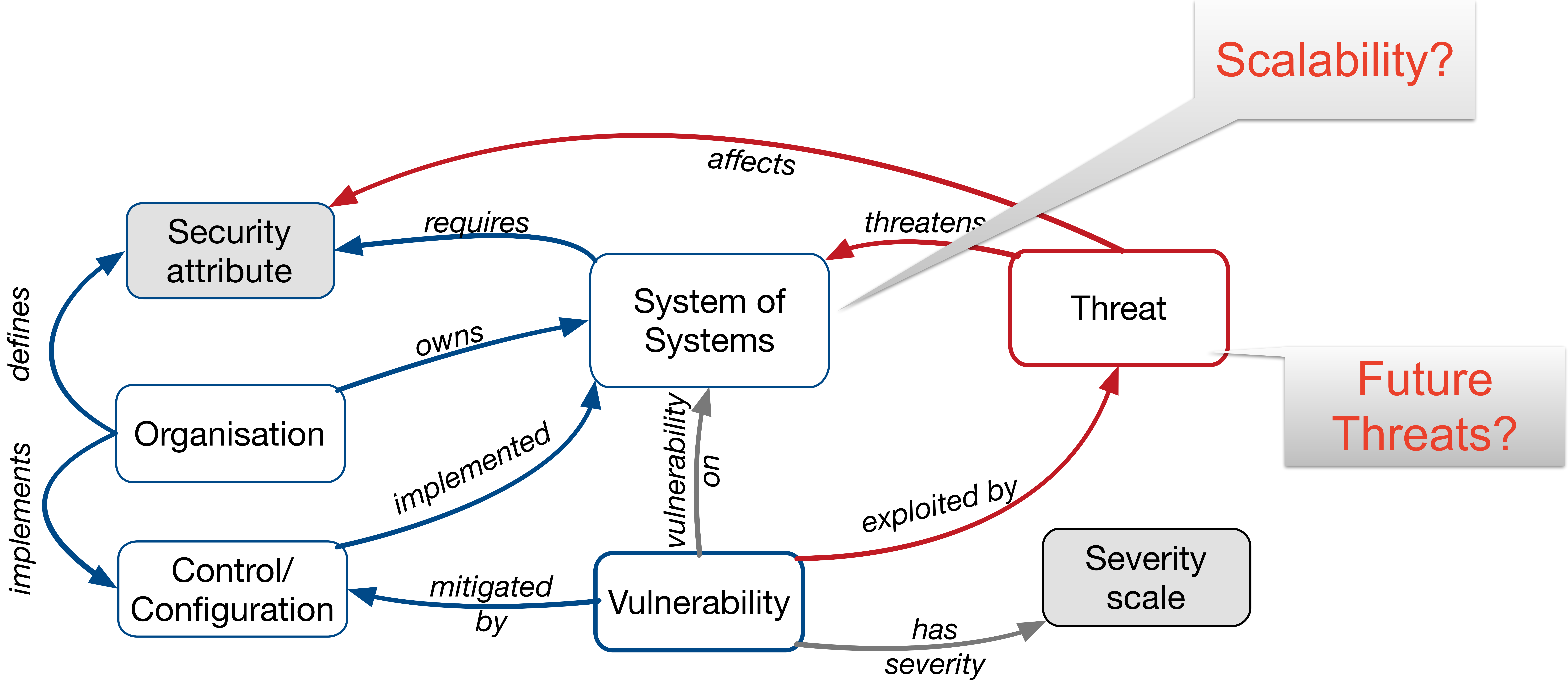
IoT concerns regarding advanced security paradigm

- **Traditional threat-based modelling is not appropriate**
  - *Handles only known threats*
  - *Does not address life-time of an IoT system (typical 10-15 years)*

Steps



Traditional: Threat-based approach



[source: http://securityontology.sba-research.org/]

IoT threats

SCOTT Secure Connected Trustable Things

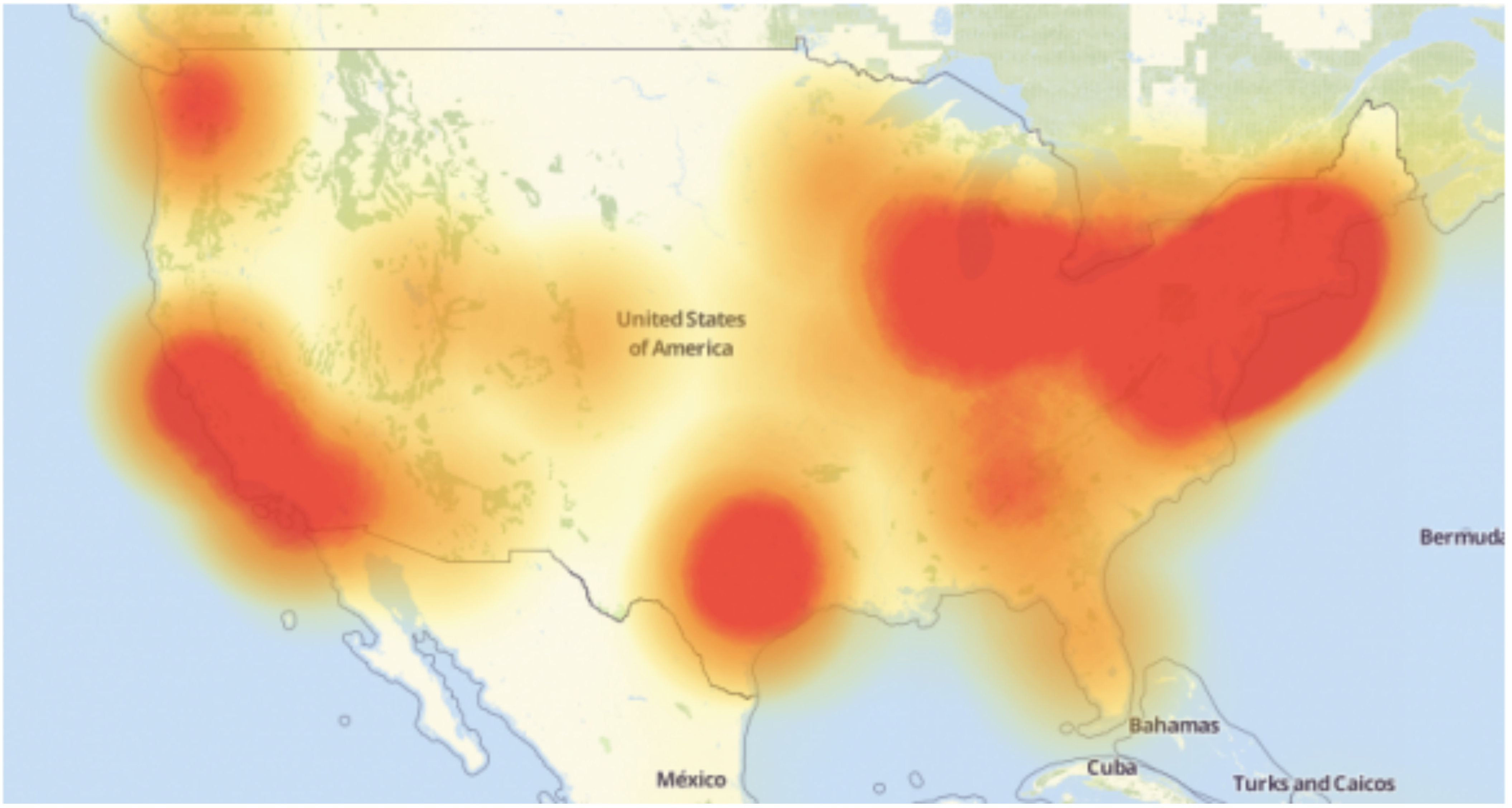
- First massive attack from IoT devices
  - *16Oct2016 IoT botnet attack on Dyn*
  - *Camera (CCTV), video recorder, TV,…*
  - *1.2 Gbps Denial-of-Service attack*

- How?
- All using Linux BusyBox for authentication
  - *admin - admin, root - root, admin - 1111…*
  - *simple "test" was enough to convert IoTs into botnet*

21 OCT 16 **Hacked Cameras, DVRs Powered Today's Massive Internet Outage** 16Oct

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

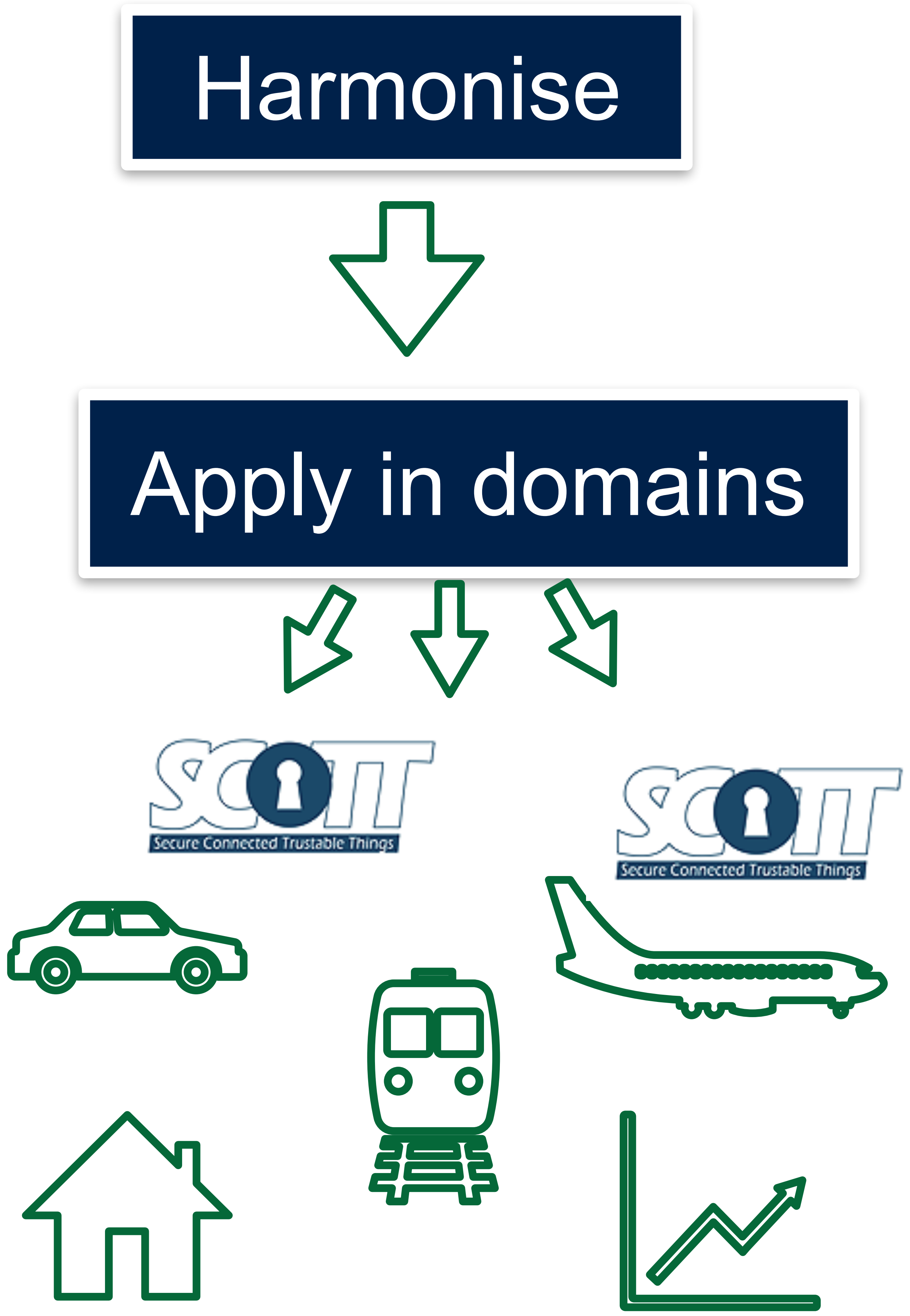
Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



[Source: https://krebsonsecurity.com/2016

IoT concerns regarding advanced security paradigm

Steps



- **Answer the IoT need for a new and more advanced security paradigm**
  - *How to measure security of (complex) IoT systems, how to incorporate security it into designs, how to have a clear (understandable to end-users) security level assessment*
  - *Address cybersecurity through proactive safeguard*

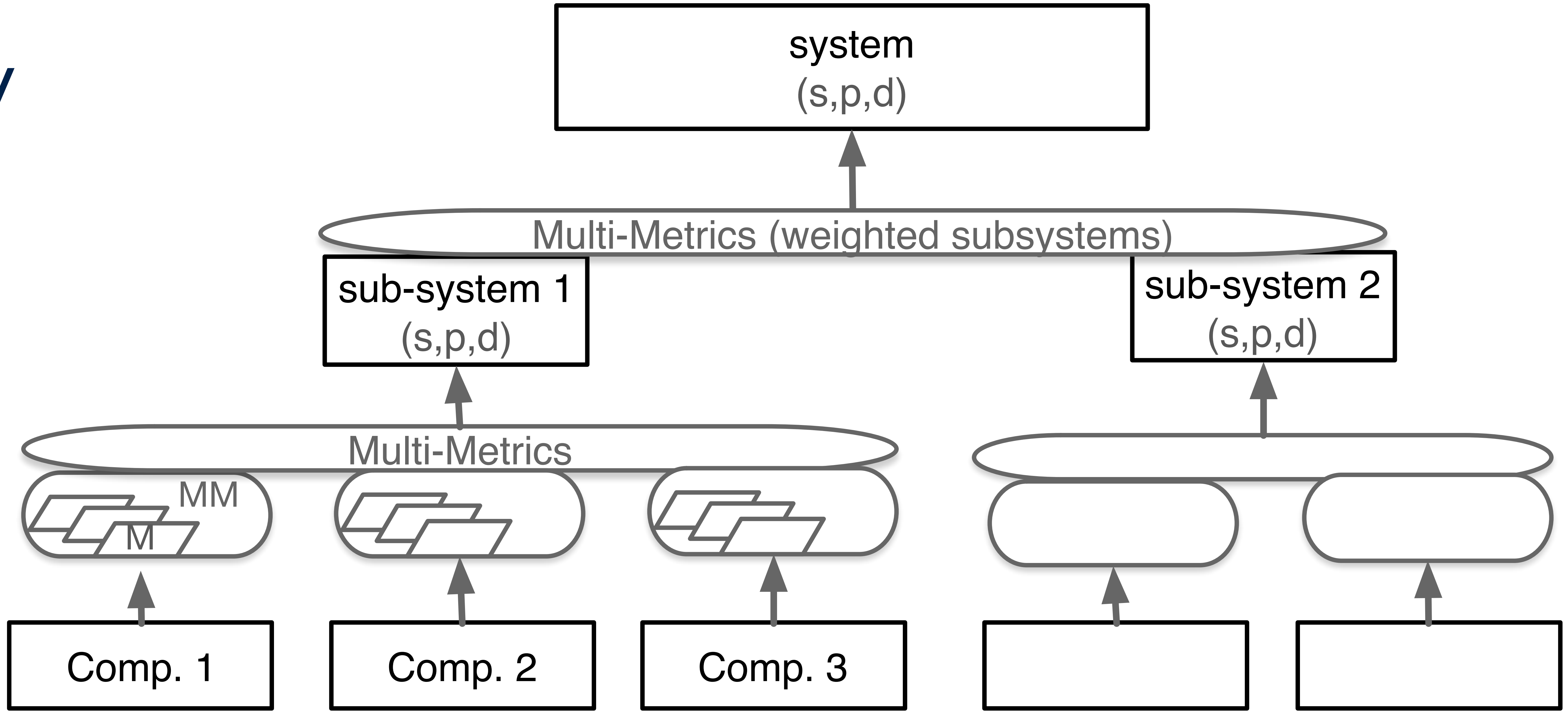
- **Main outcomes**
  - *Measurable security of (complex) IoT systems,*
  - *Security classes, defined through*
  - *Goal: Design paradigm for IoT systems*

- **Today: Impact of IoT/autonomous processes/ CPS/… on Cloud Certification - *discussion***

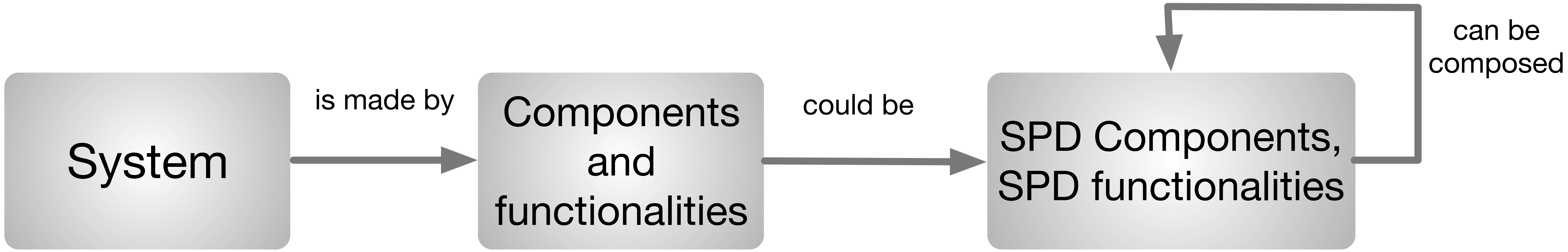
Measurable Security in IoT systems
- applicable for the cloud?

Example: Measurable Security

- From people defined security classes
- To automated security decisions
  - *through metrics assessment*



- based on
  - *security, privacy and dependability (SPD) functionalities*



SPD$_{Goal}$ versus System-SPD$_{Level}$

- Application-based security goals
- Automated assessment

- Visualisation of “operating envelopes”
  - *Security good enough?*
  - *Too high Security*

- Critical component/sub-system assessment

Table 1 SPD$_{Goal}$ of e

Use Case	Security	Privacy
Billing	90	80
Home Control	90	80
Alarm	60	40

Table 9 Selected configuration SPD level for each use case

Use case	SPD$_{Goal}$	Configuration	SPD level	SPD vs SPD$_{Goal}$
Billing	(90,80,40)	10	(67,61,47)	(🔴,🟡,🟢)
Home Control	(90,80,60)	10	(67,61,47)	(🔴,🟡,🟡)
Alarm	(60,40,80)	6	(31,33,63)	(🔴,🟡,🟡)

Security in IoT
- postulation of Security Classes, based on “exposure” and “impact”

Security Classes and System design

- Security Classes in IoT
  - *Consequence*
  - *Exposure*
- Consequence
  - *as in risk map*
- Exposure
  - *Physical exposure*
    - people, building, physical ports,…
  - *IT exposure*
    - ports, firewall, connectivity
- Used to assess the security class of Syste[illegible]ns and components

New postulate of security class

Consequence

5	Class 5	Class 5	Clas[illegible]	Class 5
4	Class 4	Cl[illegible]	[illegible]	Class 5
3	Class[illegible]	[illegible]	[illegible]s 4	Class 4
2	Class [illegible]	[illegible]ass 3	Class 3	Class 3
1	Class 1	Class 1	Class 2	Class 2
Impact/Exposure	1	2	3	4+

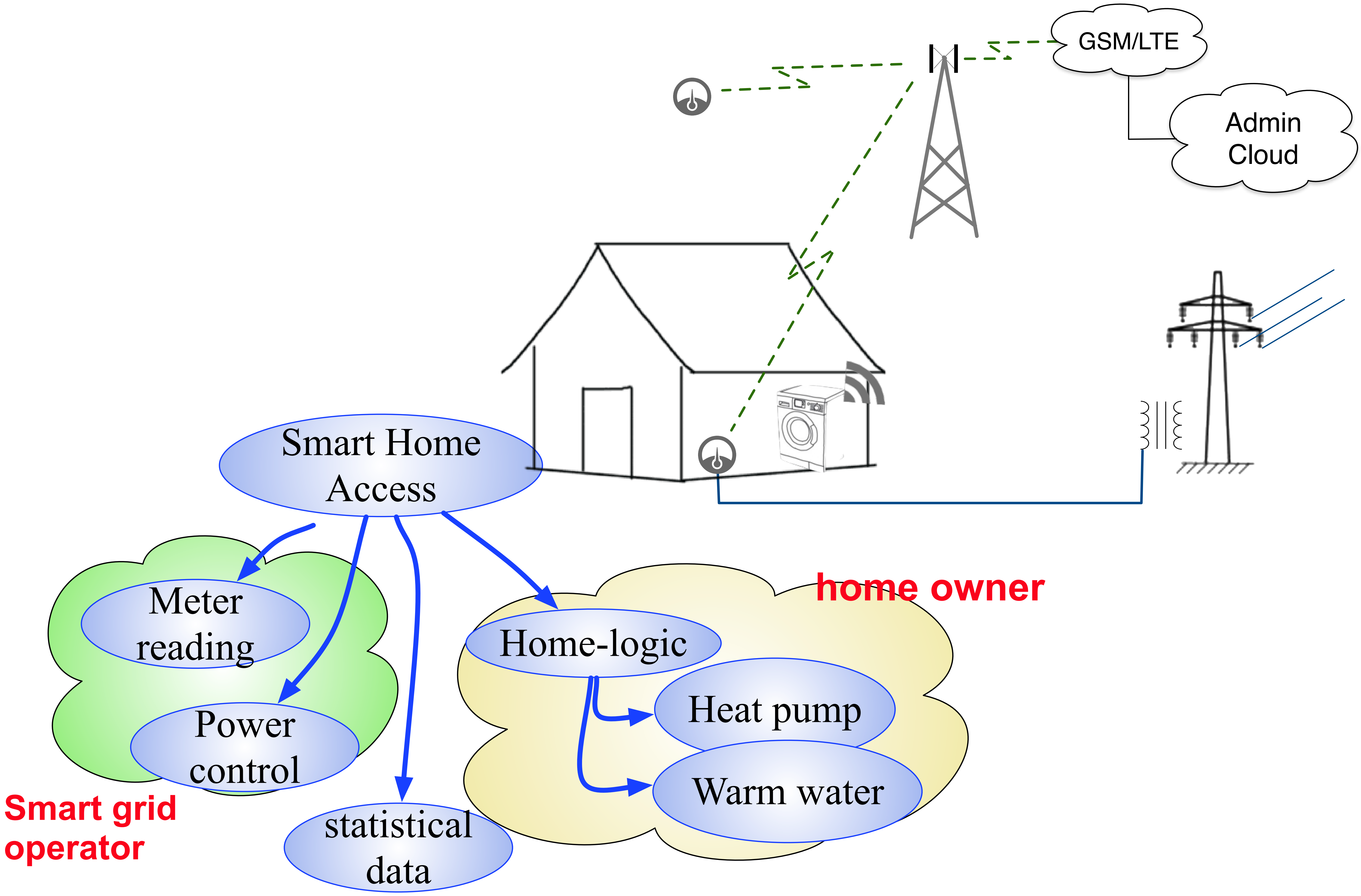
Security Class

Exposure

Increase weak security:
- watchdog
- Attribute based access control (S-ABAC)

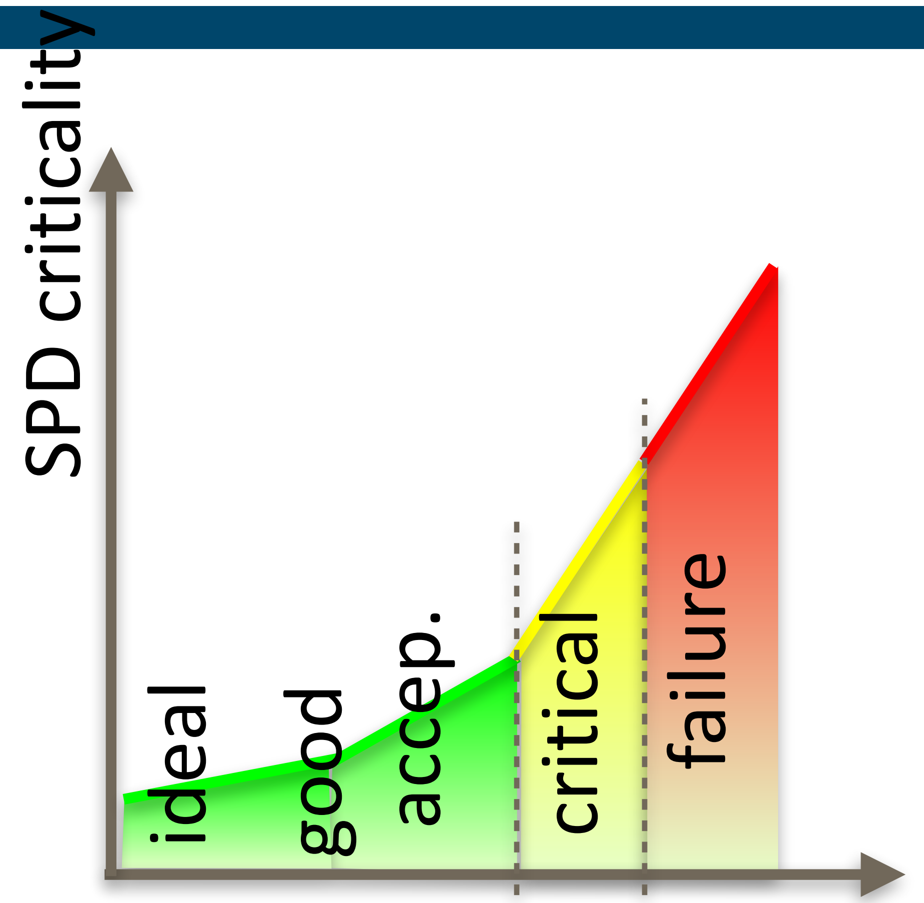
Semantic attribute based access control (S-ABAC)

- Lifting the security class through S-ABAC
- Access to information
  - *who (sensor, person, service)*
  - *what kind of information*
  - *from where*
- Attribute-based access
  - *role (in organisation, home)*
  - *device, network*
  - *security tokens*
- Rules inferring access rights



Attributes: roles, access, device, reputation, behaviour, ...

Conclusions & Discussion



- Things (IoT) are driving the digital societies
- Common challenges
  – *Internet + Semantics + Things = IoT*
  – *Insecure devices*
  – *Measurable Security and Privacy*
  – *Autonomous Decisions*

- IoT Security and privacy
  – *automated privacy/security through Multi-Metrics*
  – *Security classes for design*
  –

Other Topics

Privacy labelling

IoT trust /IOTA.org

Global perspective
UNO SDG 2030