An Ecosystem Vision of Security and Data Protection for the Internet of Thing

Antonio Kung (Trialog), Ahmed Amokrane (CoESSI), **Hocine Ameur (CoESSI),** Hervé Daussin (CoESSI), Olivier Genest (Trialog)

IOT Systems can involve Complex Ecosystems

End-user

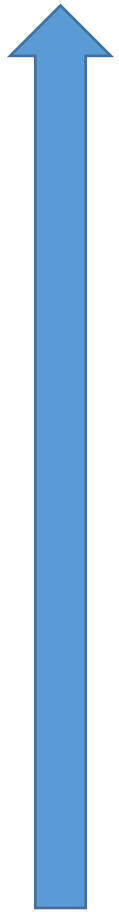
Policy Maker

Application Manager

Operator

Integrator

Supplier



Example of Security and Privacy Roles

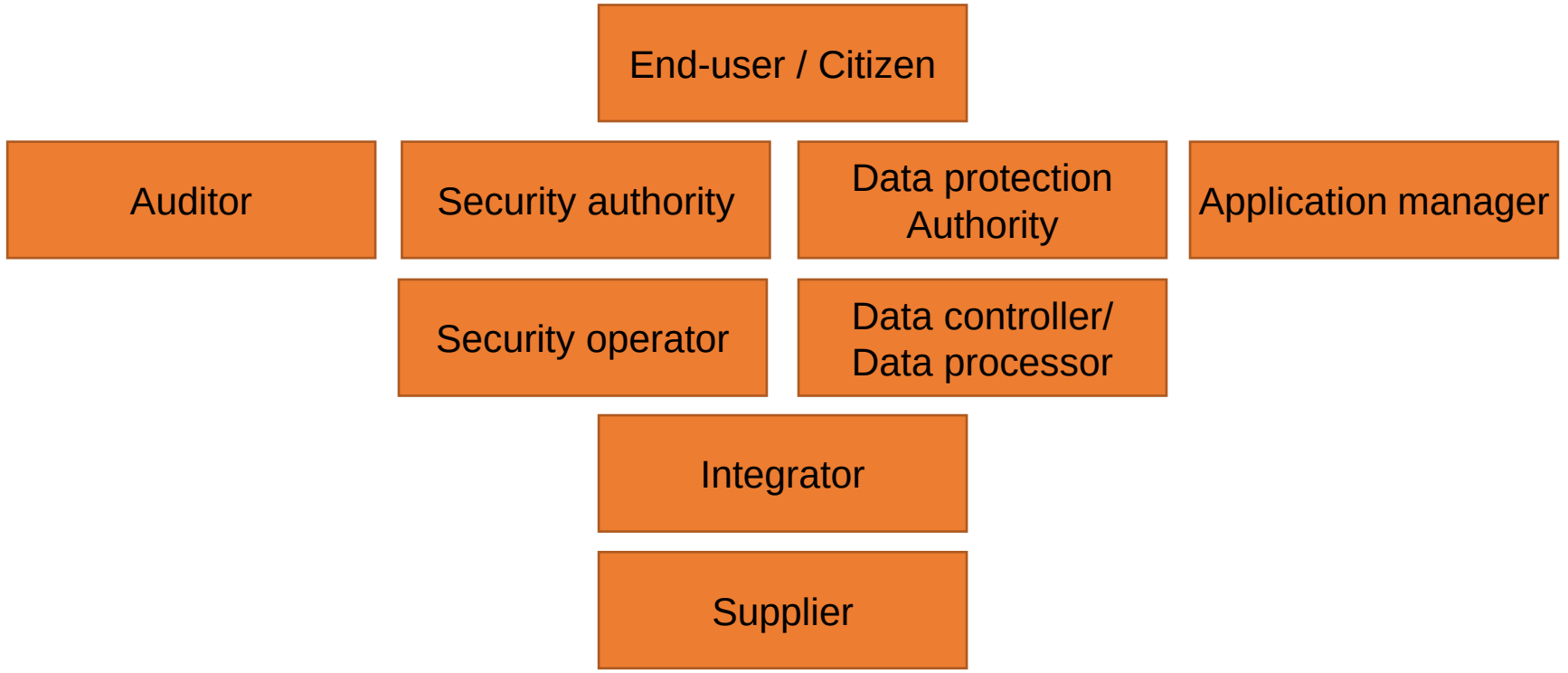
Requirements and Management of security and privacy concerns

Evidence of compliance
Lifecycle management
Assurance

Risk assessment, Controls identification
Integration of security and privacy capabilities
Assurance at integration level

Supplying security and privacy capabilities
Assurance at supply level

A SECURITY AND PRIVACY VIEWPOINT



Requirements and Management of security and privacy concerns

Evidence of compliance
Lifecycle management
Assurance

Risk assessment, Controls identification
Integration of security and privacy capabilities
Assurance at integration level

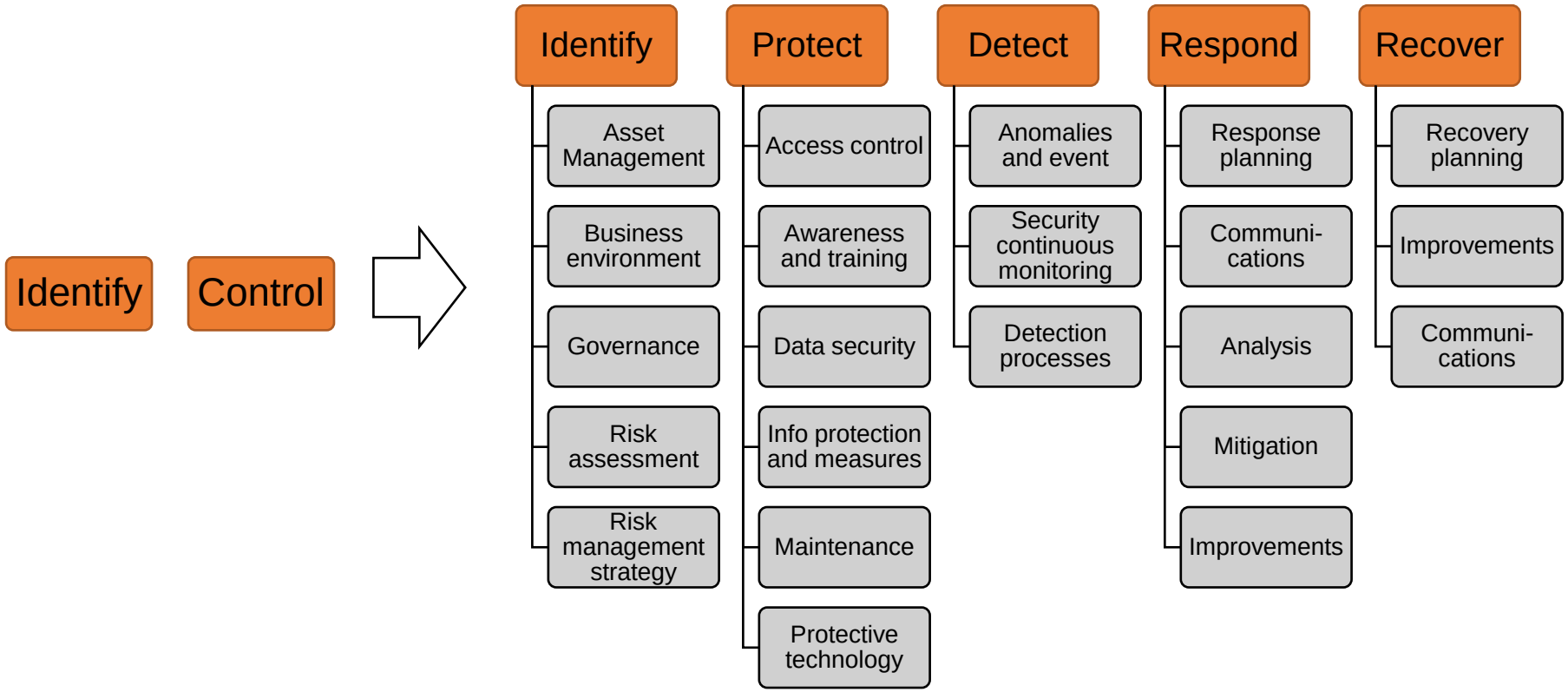
Supplying security and privacy capabilities
Assurance at supply level

EXAMPLE OF HEALTH MONITORING SYSTEM

Stakeholder	Example of stakeholders	Example of security related activity
End-user	User of health monitoring system	Relies on a 24x7 system
Auditor	Security conformance auditor	Verifies that hospital information system and health sensor communication systems conform with security requirements
Security authority	National security center	Carries out **audit** of security related activities
Application manager	City security officer	Manages security breach
Security operator	Hospital	Monitors systems against cyberattacks
Integrator	Integrator of hospital information system	Carries out security risk analysis Implement security capabilities
Supplier	Health sensor communicating with information system	Provides a secure channel capability.

Stakeholder	Example of stakeholder	Example of privacy related activity
End-user	User of health monitoring system	Provides consent Complains to the city data protection officer in case of privacy breach
Auditor	Privacy conformance auditor	Verifies that hospital information system, health sensor communication systems and associated operating procedures comply with GDPR [6]
Data protection authority	National data protection authority	Provides recommendations to city data protection officer and hospital manager. Carries out **audit** of privacy related activities. Interacts with city data protection officer in case of privacy breach
Application manager	City data protection officer	Manages citizen requests for privacy information. Manages privacy breach
Data controller/ Data processor	Hospital	Maintains a registry of personal data processing, and a secure log of access
Integrator	Integrator of hospital information system	Carries out privacy impact assessment Implement data protection capabilities
Supplier	Health sensor communicating with information system	Provides a user control capability

IMPACT ON LIFECYCLE (SECURITY)

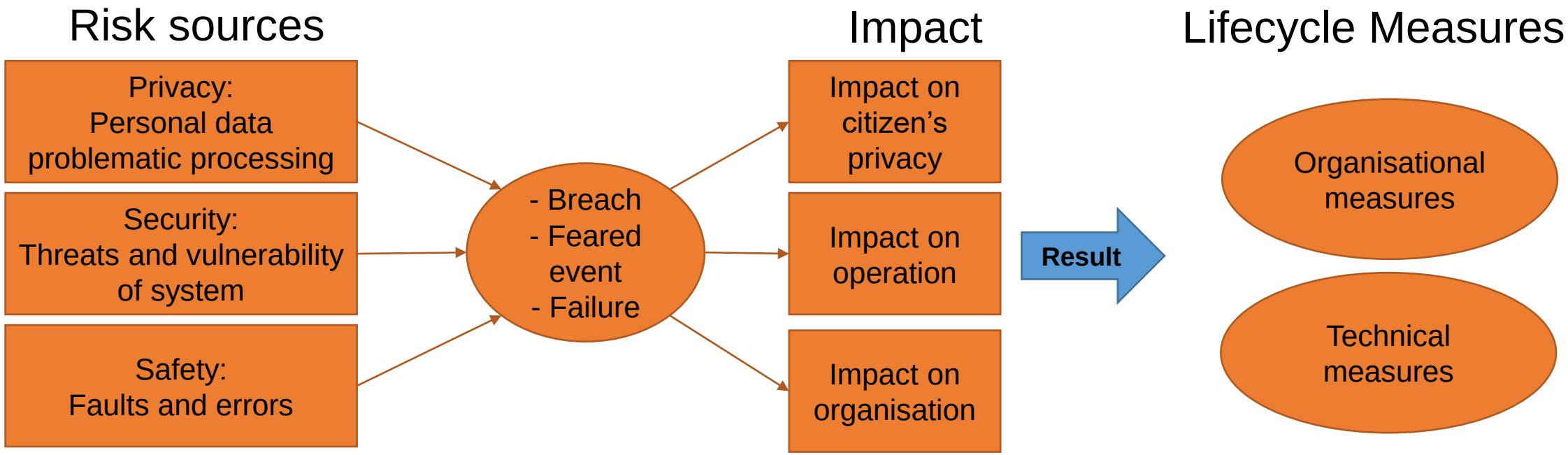


NIST Cybersecurity Framework – Towards ISO/IEC standards (JTC1/SC27)

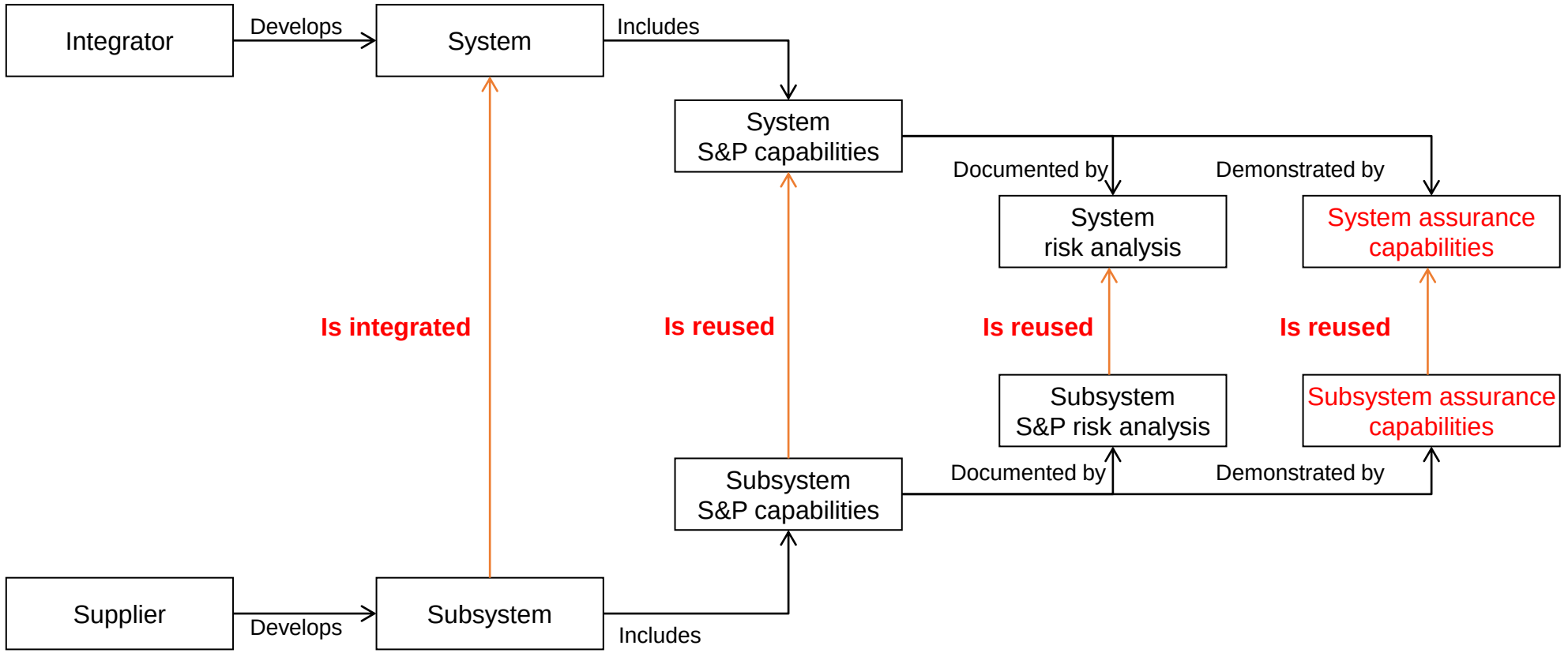
IMPACT ON LIFECYCLE (PRIVACY)

Types of processes	Selected system life cycle processes ISO/IEC 15288 (JTC1/SC7)	Privacy engineering processes ISO/IEC 27550 (JTC1/SC27)
Agreement processes	Acquisition process Supply process	Supply chain involving personal information
Organizational project-enabling processes	Human resources management process	Privacy engineering human resource management
	Knowledge management process	Privacy engineering knowledge management
Technical management process	Risk management process	Privacy risk management
Technical processes	Stakeholder needs and requirements process	Stakeholders' privacy expectations
	System requirements definition process	Privacy principles operationalisation
	Architecture definition process	Impact of privacy concerns on architecture
	Design definition	Impact of privacy concerns on design

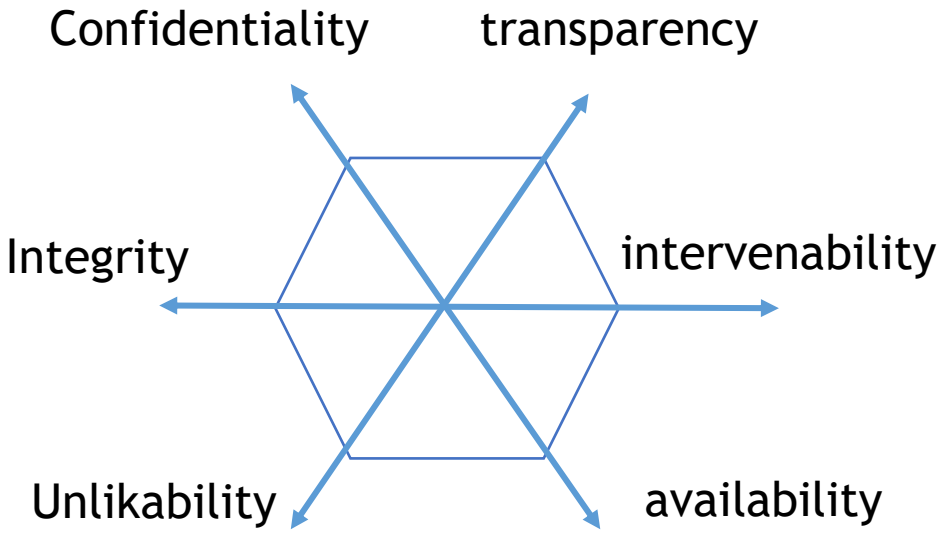
INTEGRATION OF RISK ANALYSIS

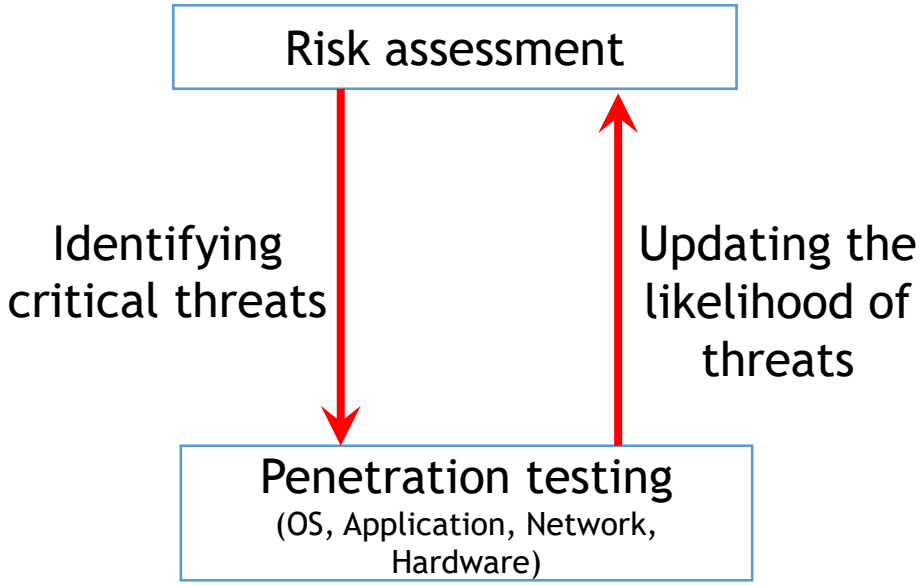


INTEGRATION OF SECURITY AND PRIVACY CAPABILITIES



THE IMPACT ON ASSURANCE AND THE NEED FOR PENETRATION TESTS





- Provides the means to measure the **impact of an attack**
- Provides some **level of evidence** that the system is properly protected
- The measurement can be in terms of properties

THE IMPACT ON ASSURANCE AND THE NEED FOR PENETRATION TESTS

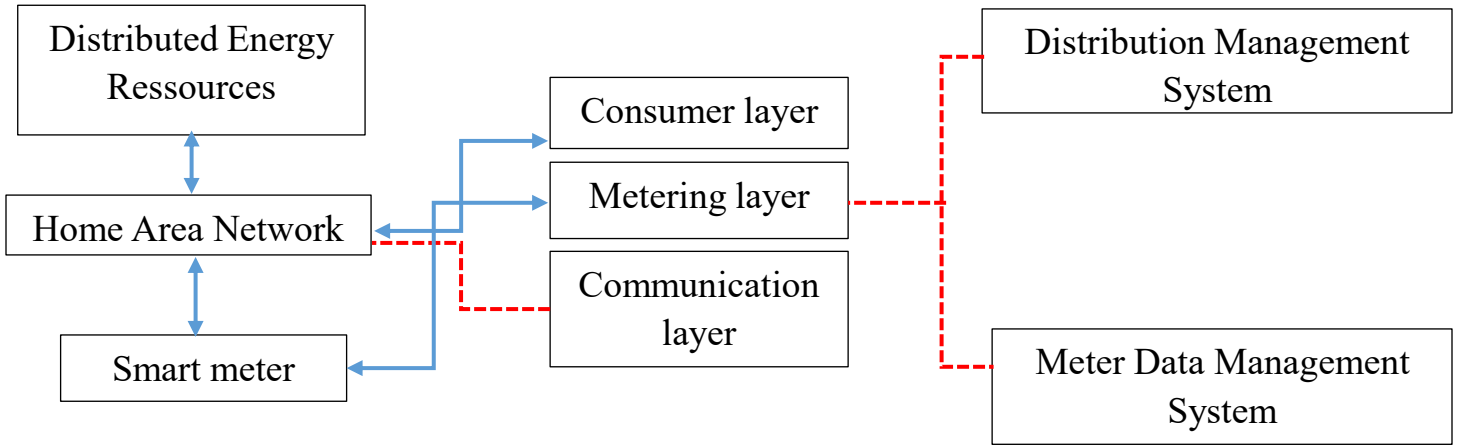
IOT ARCHITECTURE LAYERS

Nodes technology	Access network	Services	Applications
ZigBee 6LoWPAN NFC RFID Bluetooth	LAN WLAN Cellular network	PaaS SaaS IaaS	Transport Production Smart buildings Electric vehicle charging

WHAT NEEDS TO BE TESTED?

- Internet facing **services**
- Web and **administrative interfaces**
- **Cloud** infrastructures
- **Mobile** Applications
- Communication **networks** and wireless communication media
- Communication **APIs** and web services
- **Hardware**
- Device **firmware** and software **updates**

A LARGE SCALE SMART GRID PROJECT

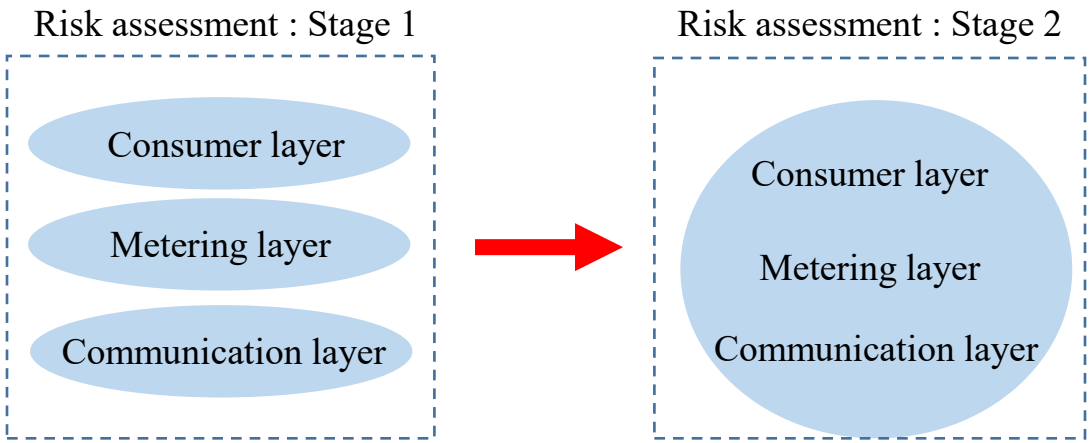


- If one component is compromised, **the whole system can be exposed**
- Can affect the **power utility** network as well as the **end users** (homes/businesses)
- Studying **storage** and **sharing** of users' identifiable information
- Limiting **data collection** of the information

A LARGE SCALE SMART GRID PROJECT

- Risk assessment with regard to **data protection**
- Data **anonymization** to guarantee privacy
- Security **integrated into the design** phase of devices and data storage platforms (HSM integrated into concentrators)
- Penetration tests within the **certification process** of components
- **Interoperability** and functional tests to homologate the whole system.

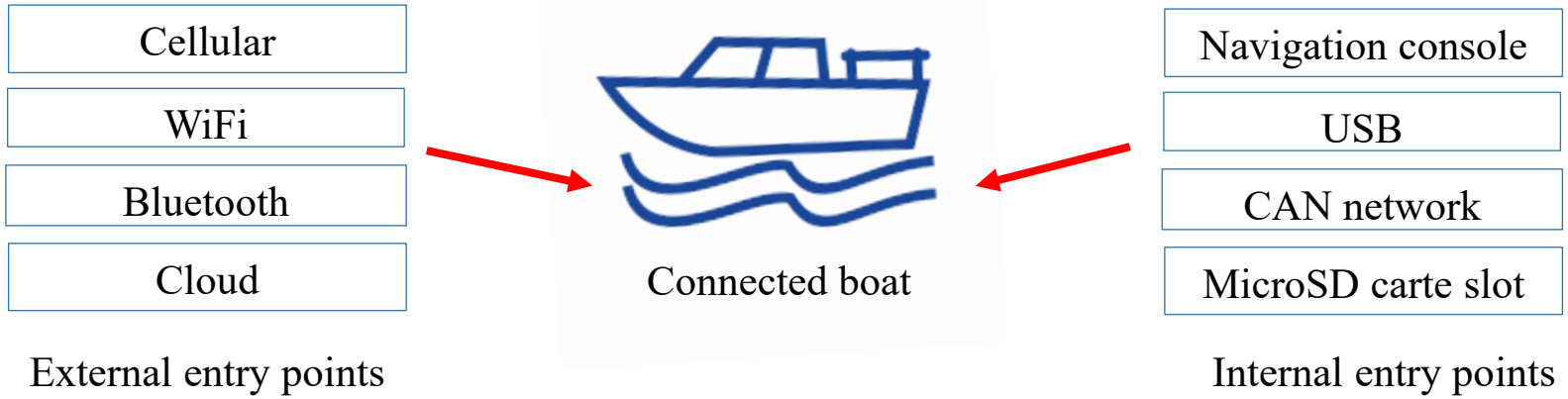
A LARGE SCALE SMART GRID PROJECT



Risk assessment approach for the AMI

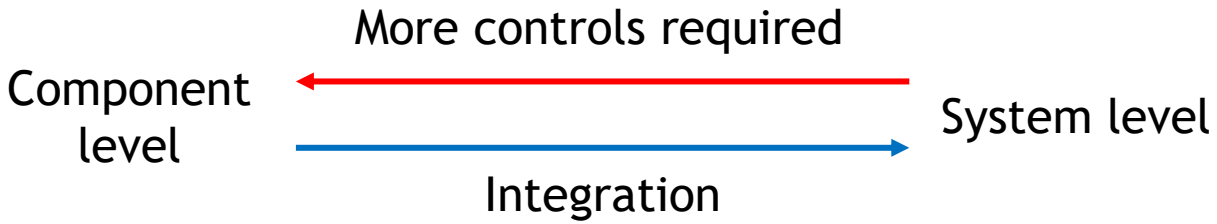
- Privacy is regarded through **the type, scale and content** of the collected data
- The data collected from a smart meter can be used to discern **the behaviour of the end users**

A CONNECTED YACHT PROJECT



Internal and external entry points of the Yacht

A CONNECTED YACHT PROJECT



- Vulnerabilities of some components are **covered after the integration by other components** (eg. components that use cleartext protocols)
- Some security controls can be identified and should be added at the components level **after the integration** of the whole system

A CONNECTED YACHT PROJECT

Data related to the boat

- Engine **statistics**
- Engine **location**
- Maintenance **history**
- Can be tied to the user as **ownership**

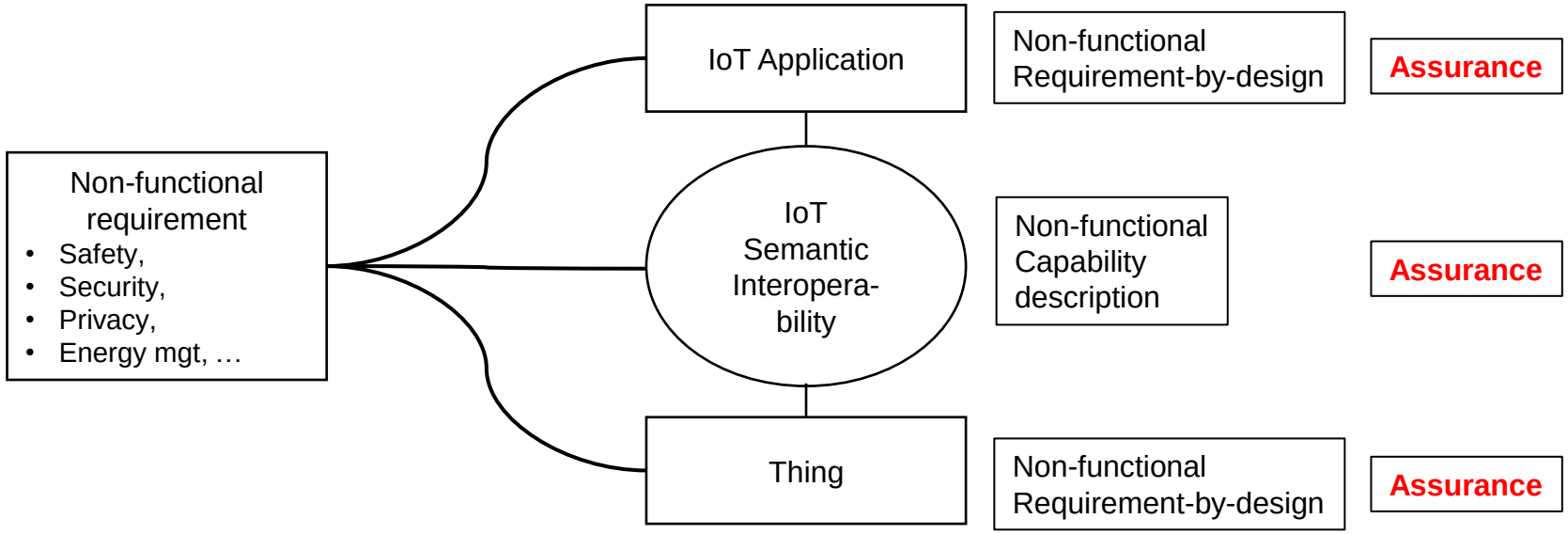
Data related to the user

- Bookmarked **locations**
- **Shared** locations/information with other users
- **Personal** as each user is identified

- The need of data **anonymization**: the data collected by the manufacturers is only related to the boats and no ownership relationship is kept.

CONCLUSION

- Current standardisation work at ISO/IEC (Nov 2017)
  - **Cyber security: new work item** – guidelines for cybersecurity framework
  - **Big data: ISO/IEC 20547-4** -reference architecture – Security and Privacy
  - **IoT: new work item** – security and privacy guidelines for IoT
  - **Smart cities: new work item** – privacy guidelines for smart cities
- Towards interoperability of security and privacy capabilities, including **assurance**



THANKS

Trialog contribution to this paper is based on work carried out in the PRIPARE and Create-IOT support action