

Move securely within the cyberworld

ISED 04/05/2018

# Standardising the un-standardisable (or how to agree on the IoT)

**Dr. Jean Lancrenon**  
**Dr. Carlo Harpes**

itrust consulting s.à r.l.  
55, rue Gabriel Lippmann  
L-6947 Niederanven

Tel: +352 26 176 212 6  
Fax: +352 26 710 978  
Web: [www.itrust.lu](http://www.itrust.lu)

- itrust consulting** An SME from Luxembourg specialising in Information Security Systems, with four business lines

- Audit and hacking
- Consulting, innovation, sourcing
- Research and development
- Training and awareness



- Skills and products** brought collectively by all 20 employees

- Organisational and technical audits: ISMS, Archiving, BCP/DRP Management, Data protection
- Penetration testing: Vulnerability scans and assessment, Black-and-white-box penetrations tests, Social engineering, Certification and accreditation Audits
- Malware.lu CERT
- Consulting Risk management: TRICK Service, DPIA, risks assessment on PKI and e-money, ISMS documentation, implementation
- Licencing: Software checker, AVCaesar
- Research and & Development: H2020, National
- Standardisation



## H2020 project ending this year, Topic foritrust :

- IoT Payments and blockchain
- Privacy
- Pseudonymisation

## Other topics:

- Use case in 3 different areas:  
BXL, Lyon, Helsinki
- ...



**bloTope** BUILDING AN IoT OPEN INNOVATION ECOSYSTEM FOR CONNECTED SMART OBJECTS

Home Overview News Articles Forum Open Call 2 Results Promotional Consortium Members Photos Contact

IoT-EPI

[Twitter](#) [LinkedIn](#) [Facebook](#) [Pinterest](#) [Like 1](#)

### The bloTope Project

The Internet of Things (IoT) brings opportunities to create new services and products, reducing costs for societies, and changing how services are sold and consumed. A critical obstacle to further IoT innovation is the "vertical silos" that shape today's IoT landscape. These silos impede the creation of cross-industry, cross-platform and cross-organisational services due to their lack of interoperability and openness.

The bloTope project lays the foundation for creating open innovation ecosystems by providing a platform that enables companies to easily create new IoT systems and to rapidly harness available information using advanced Systems-of-Systems (SoS) capabilities for Connected Smart Objects – *with minimal investment*.

### Project Partners

- Aalto University
- uni.lu UNIVERSITÉ DU LUXEMBOURG
- CEPEL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE MONTRÉAL
- Fraunhofer IAS
- BIBA
- CSIRO
- THE Open GROUP
- BMBF
- eccenca command your data!
- OpenDataSoft
- Cityzen Data
- HOLONIX PROJECT CONNECTED OBJECTS
- itrust consulting

### IoT-EPI on Twitter

The bloTope project is one of several projects that comprise the IoT European Platform Initiative (IoT-EPI) under the European Union's Horizon 2020 Programme. Follow the latest activities of the IoT-EPI cluster on Twitter at @IoT-EPI.

Tweets by @IoT\_EPI

IoT-EPI Retweeted

**DunavNET** @DunavNET

Our #IrrigNET solution as Promising practice on e-agriculture FAO Forum - 2gether 4 Strong Digital Agriculture, 18-20 April 2018 in Sofia, Bulgaria. Meet us there! #UNFAO @FAOKnowledge fao.org/europevents/...

Emoted View on Twitter

### Latest site updates

**Abdelhak BOULALAM** liked **Scott Hansen's** photo

Nov 6, 2017

**Scott Hansen's** article was featured

Comments: 0

Tags: conference, interview, lyon

### News

**bloTope at W3C Web Conference in Lyon 23-27 April**

Posted by **Scott Hansen** on May 3, 2018 at 12:10am



The bloTope project was active in presenting the project and new technologies at the **Web Conference** held in Lyon on 23-27 April as part of the series of conferences organised by the World Wide Web Consortium. This series aims to provide the world a premier forum for discussion and debate about the evolution of...

Read more...

## Internet of Things ....

- *A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies* ITU- T Y.2060, ISO 38505
- *A cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making” – ENISA*

Stemming from the definition is the fact that **information** lies at the **heart of IoT**, feeding into a continuous cycle of sensing, decision making, and actions

## ...is composed of:

- Devices (smart cameras, smart watches, smart tractors, smart <insert favorite object here>...)
- Protocols (CoAP, MQTT, HTTP, Bluetooth, WiFi, LoRa, Zigbee, Z-Wave, 3G, 4G, 5G, RFID...)
- Software-and-firmware (TinyOS,...)
- Services
- Other derived concepts: edge networks, fog computing

## ...crosses the fields of:

- Health, Agriculture, Mobility, Smart cities, Smart homes, Industry 4.0, etc...

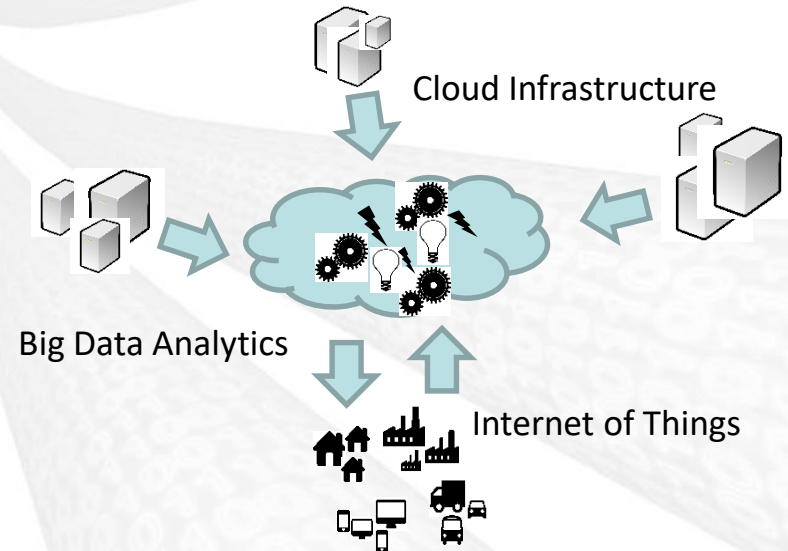
## ...is a nightmare for:

- **Security specialists** (Botnets, UPnP, Telnet...)
- **Standardisation organisms**

- One of the three main technologies under scrutiny in **Digital Trust for Smart ICT:**



- **IoT:** provider of enormous quantities of data, actuation on environment
- **Big Data:** from (among other sources) the IoT, requires analysis
- **Cloud computing:** computing as a utility, elasticity, infrastructure





- ISO/IEC JTC 1/SC 41
- Industrial Internet Consortium (IIC)
- Alliance for IoT Initiative (AIOTI)
- ITU-T Study Group 17
- ISO IEC SC27 WG4 (to create 27030)
- ENISA

## Standardisation efforts,

- very recent in IoT, date back to 2015,
- generally under construction
- at several working groups on it in ISO/IEC (which need to stay aligned and avoid overlap)

## IoT in **general** extensively (in intensely) examined by

- **ISO/IEC JTC 001 SC 41 IoT and related technologies**
  - a) IoT **Architecture**
  - b) Generic characteristics, concepts, a technology-neutral reference point
  - c) Used to build coherent standards upon, and as a reference for any IoT system architecture
- **IoT Interoperability**
  - a) Between entities **within** an IoT system and **between** IoT systems
  - b) Along 5 facets: transport, syntax, semantics, behaviour, and policy
  - c) Others...
- **SG8 on trustworthiness (a bit of IoT security too):**
  - Investigate standards on **security, privacy, safety, resilience and reliability**
  - Make IoT more **verifiable**

## ISO recent standard related to IoT :

- ISO 19079:2016(en) **Intelligent transport systems** — Communications access for land mobiles (CALM) — 6LoWPAN networking
- ISO 19731:2017(en) **Digital analytics** and web analyses for purposes of market, opinion and social research — Vocabulary and service requirements
- ISO/IEC 38505-1:2017(en) Information technology — **Governance of IT** — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data
- ISO/IEC TR 29181-9:2017(en) Information technology — **Future Network** — Problem statement and requirements — Part 9: Networking of everything
- ISO/IEC TR 22417:2017(en) Internet of things (IoT) **use cases**
- ISO/IEC 29341-....:2017(en) Information technology — **UPnP** Device Architecture — ...

## Semantic models

- O-DF, O-MI



## Information technology — Internet of Things (IoT) :

- ISO/IEC CD 20924, Definition and vocabulary
- ISO/IEC CD 30141, Reference Architecture (IoT RA)
- ISO/IEC AWI 21823-1, Interoperability for IoT systems -- Part 1: Framework
- ISO/IEC NP 21823-3, Interoperability for IoT Systems - Part 3: Semantic interoperability
- ISO/IEC PDTR 22417, Use cases
- ISO/IEC JTC 1/SC 27 N 17773, Guidelines for security and privacy in Internet of Things (IoT)

-> still quite embryonic

## Information technology – Security techniques (always applicable)

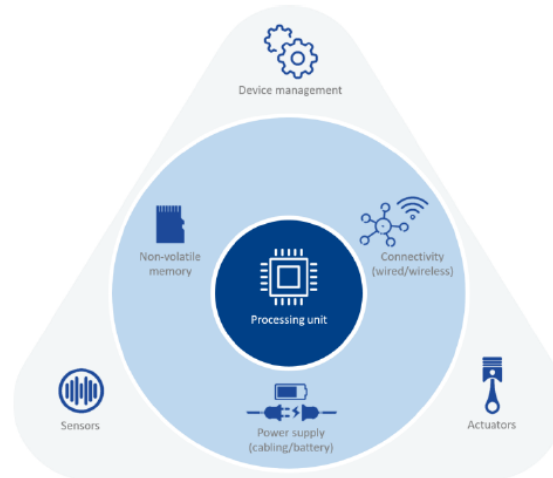
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27552, Enhancement to ISO/IEC 27001 for privacy management — Requirements



## Content:

- The IoT Paradigma
- Threats and risk analysis
- Security measures and good practices
- Gaps and high-level recommendations to improve IoT cybersecurity

## The IoT Paradigma

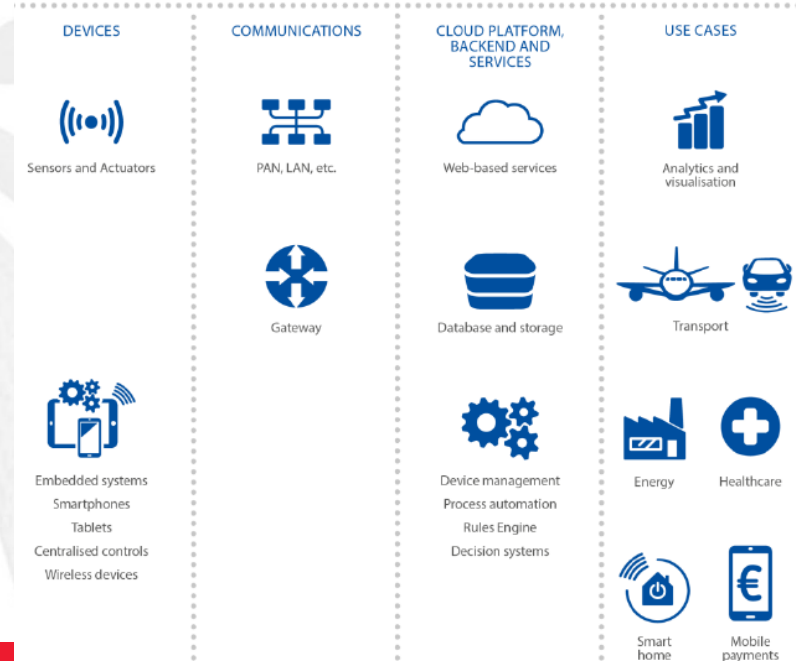


## SECURITY

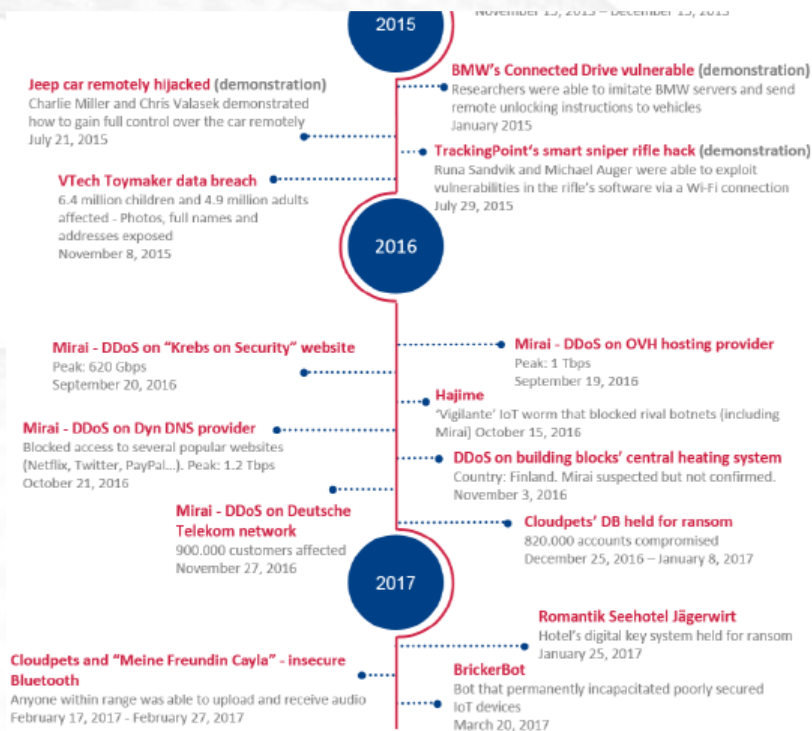
Authentication  
Authorisation  
Access Control  
Availability



Encryption  
Integrity  
Secure communication  
Non repudiation

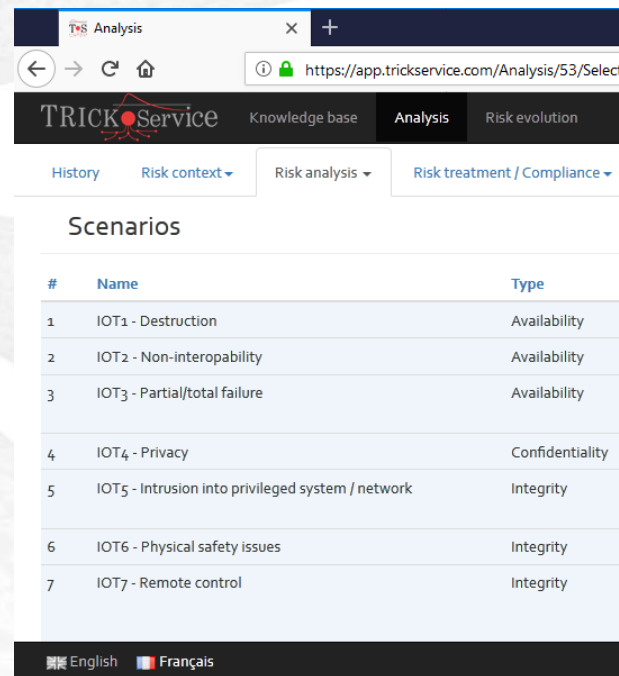


## Threats and risk analysis



## TRICK Service extended by:

- IoT Threat-Vulnerability-Risk brainstorming
- IoT Attack scenarios



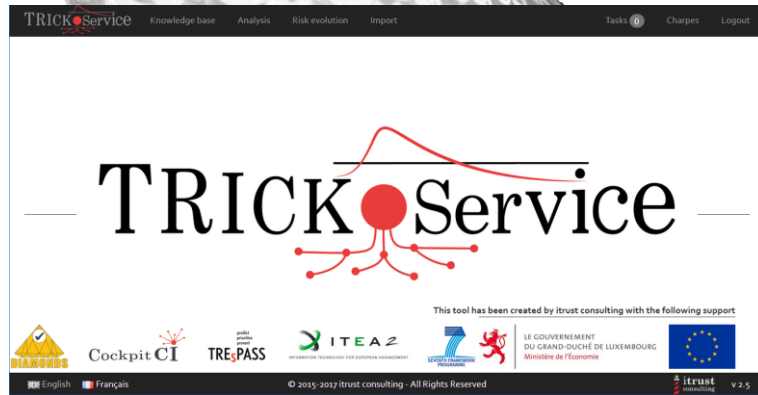
The screenshot shows the TRICK Service web application interface. The browser address bar displays the URL <https://app.trickservice.com/Analysis/53/Select>. The application has a navigation bar with tabs for "Knowledge base", "Analysis" (selected), and "Risk evolution". Below the navigation bar, there are sub-tabs: "History", "Risk context" (selected), "Risk analysis", and "Risk treatment / Compliance". The main content area is titled "Scenarios" and contains a table with 7 rows of IoT attack scenarios.

#	Name	Type
1	IOT1 - Destruction	Availability
2	IOT2 - Non-interoperability	Availability
3	IOT3 - Partial/total failure	Availability
4	IOT4 - Privacy	Confidentiality
5	IOT5 - Intrusion into privileged system / network	Integrity
6	IOT6 - Physical safety issues	Integrity
7	IOT7 - Remote control	Integrity

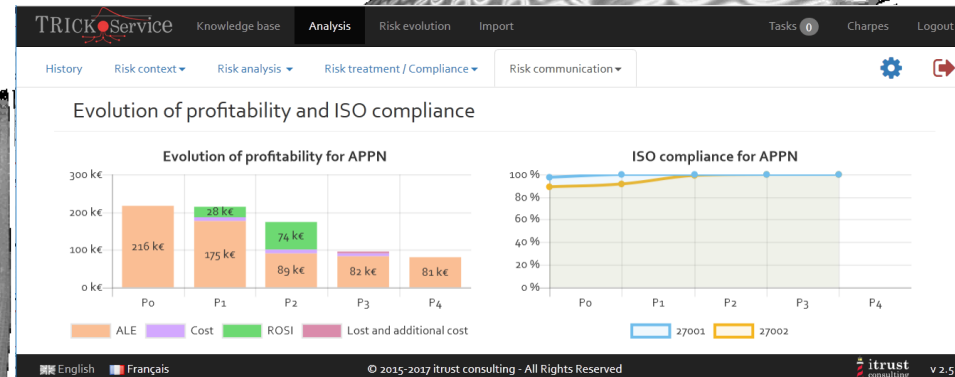
At the bottom of the interface, there are language selection buttons for "English" and "Français".

# TRICK Service

## Tool for Risk management of an ISMS based on a Central Knowledge base



1. Context & assets valuation (cf. 27005, 29134)
2. Gap analysis (27002, 29151, 27552...)
3. Qualitatively assess threats, vulnerabilities, risks;
4. Quantified assessment of impacts and likelihoods;
5. Risk treatment plan, sorted by phases and ROSI;
6. DPIA compliant to GDPR, RAR compliant to CSSF



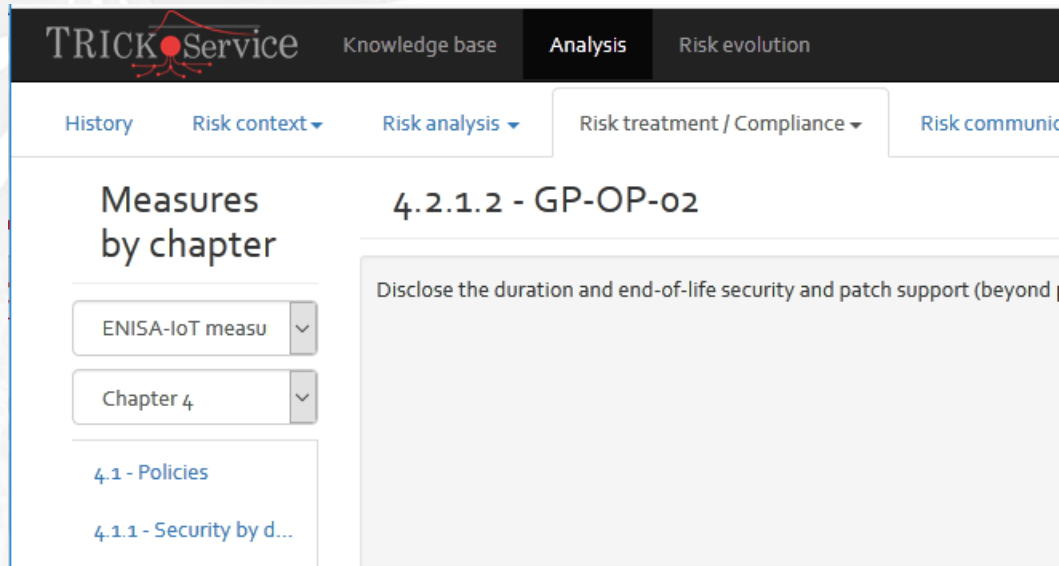


## Security measures and good practices

- a) Policies
- b) Organisational, People and Process measures
- c) Technical Measures

### TRICK Service extended by:

- IoT Security measures  
(to treat risks)



The screenshot shows the TRICK Service web application. The top navigation bar includes 'Knowledge base', 'Analysis', and 'Risk evolution'. Below this, a secondary navigation bar contains 'History', 'Risk context', 'Risk analysis', 'Risk treatment / Compliance', and 'Risk communication'. The main content area is titled 'Measures by chapter' and features two dropdown menus: 'ENISA-IoT measu' and 'Chapter 4'. Below these, a list of measures is displayed, including '4.1 - Policies' and '4.1.1 - Security by d...'. On the right side, a specific measure is highlighted: '4.2.1.2 - GP-OP-02', with a description: 'Disclose the duration and end-of-life security and patch support (beyond...'.

## Gaps:

1. Fragmentation in existing security approaches and regulations
2. Lack of awareness and knowledge
3. Insecure design and/or development
4. Lack of interoperability across different IoT devices, platforms and frameworks
5. Lack of economic incentives
6. Lack of proper product lifecycle management

## High-level recommendations to improve IoT cybersecurity

1. Promote harmonization of IoT security initiatives and regulations
2. Raise awareness for the need for IoT cybersecurity
3. Define secure software/hardware development lifecycle guidelines for IoT
4. Achieve consensus for interoperability across the IoT ecosystem
5. Foster economic and administrative incentives for IoT security
6. Establishment of secure IoT product/service lifecycle management
7. Clarify liability among IoT stakeholders

-> Topics for further research:

... which might be “un-standardisable”, at least difficult to standardise.

To conclude

- IoT is new, with little standardisation
- Technology provider do not wait for standards (facebook & google don't need standards),
- But standards help us to know where to go
- You should use Security by Design, Privacy by Design, Risk Assessment, for IoT
- We tried integrating existing referentials in our tools (TRICK Service)
  - i.e., base our tools on available standards
- We look for opportunities to improve them in further use cases, risk assessments, ...



# Move securely within the cyberworld

