Cybersecurity
Lessons learned from the energy sector

Trusted partner for your Digital Journey

Atos

Summary

1 Reach a safe harbour

Challenges and opportunities

- **Interoperability**
  - Communication interface
  - Device interoperability
- **Open Standards**
  - Common and Open APIs
  - Odontology and semantics
- **Domain cross-fertilisation**
  - Data layers (collect, store, manage)
  - "Smarter" devices
- **Cybersecurity**
  - Security & Privacy
  - Multi-platforms
  - Multi-devices
- **Blow-out solutions**
  - Digitalization
  - Business opportunities

2 Obtaining knowledge

Project performed

- **OPENNODE (Open Architecture for Secondary Nodes of the Electricity SmartGrid)**

  OpenNode focuses on the research and development of an open Secondary Substation Node (SSN), which is seen as an essential control component of the future smart distribution grid, a middleware to couple the SSN operation with the utility systems for grid and utility operation and a modular communication architecture based on standardized communication protocols.

  ATOS' I+D include prototypes of the **Middleware** and the **Virtual SSN** developed with the collaboration of Atos Word Grid.

  http://opennode.atosresearch.eu

Project performed

- **e-DASH (Electricity Demand and Supply Harmonizing for EVs)**
  Harmonization of electricity demand in Smart Grids for sustainable integration of electric vehicles. This is addressed by an intelligent charging system supported with near real-time exchange of charge related data between EVs and the grid.
  ATOS' I+D include prototypes of the **Brokering services** between **BPRs**, fleet managers and charging points.
  http://edash.eu

Project on-going

- **SHAR-Q (Storage capacity over virtual neighbourhoods of energy ecosystems)**
  The SHAR-Q project aims to establish an interoperability network that connects the capacities of the neighbour hooding and wide regional Renewable Energy Sources (RES) and Electrical Energy Storages (EES) ecosystems into a collaboration framework that mitigates the requirement on the overall EES capacities thanks to the shared capacities among the participating actors.
  ATOS' I+D include **interoperability** and data collection in **heterogeneous environments**.
  http://www.sharqproject.eu

Project on-going

- **inteGRIDy (integrated Smart GRID Cross-Functional Solutions for Optimized Synergetic Energy Distribution, Utilization & Storage Technologies)**
  inteGRIDy aims at integrating **cutting-edge technologies**, solutions and mechanisms in a scalable Cross-Functional Platform of replicable solutions. This platform connects existing energy networks to diverse stakeholders, with enhanced observability of both generation and consumption profiles.
  ATOS' I+D objective include fostering coordination of distributed energy resources within a continuously increased **share of renewable energy**.
  http://www.integridy.eu

3 Unexpected discoveries?

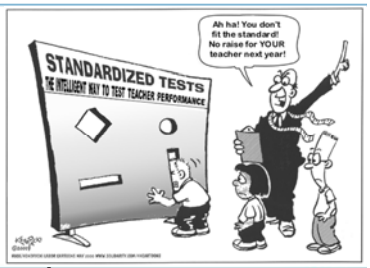
Interoperability aspects

- Even manufacturers distribute devices (meters, sensors, concentrators, etc.) using standards and protocols, those are limited by:
  - **Manufacturer's understanding** regarding how to implement the standard or protocol
  - Devices should be **capable to manage various communication channels** (e.g. Wi-Fi, Zigbee, LAN, etc.) implying additional efforts from manufacturers
  - Devices should be **capable to be integrated within heterogenous platforms** or systems (e.g. SCADA, AMM, FIWARE, etc.)
  - Furthermore…

Source: https://www.cartoonstock.com/directory/s/standardized.asp

Standardization aspect

- Europe has many key players in standardization[1]:
  - European Standardisation Organisations are recognised by Regulation (EU) No 1025/2012
  - CEN, CENELEC, ETSI
- Each focused on specific aspects of standardization and supported by working groups
- **European Standards are voluntary**[2]



Sources:
Figure: https://www.pinterest.com/pin/289567451022227627/
[1] https://ec.europa.eu/growth/single-market/european-standards/key-p
[2] https://www.cen.eu/you/EuropeanStandardization/Pages/default.aspx

Standardization aspect

- Continuous **evolution** and enhancement of standards and impact on interoperability
  - existing vs. new devices, systems, solutions
- Continuous evolution to "**smart**" devices
  - new functionalities

Source: https://xkcd.com/927/

Platform owners aspect

- **(Business / Research / etc.)** Solutions are based on platforms or systems
  - Motivated on own data management needs
  - No solution to interoperate with external devices
  - Internal vs. external world
    - **Hybrid clouds**?

Source: https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwi11bXrg7XdAhURK1AKHfb7C3wQjRx6BAgBEAU&url=https://rampages.us/egglestonep/2014/10/18/23/&psig=AOvVaw2czhFLcl2Co-Zj5eGZ_VVC&ust=1536826728082169

Cybersecurity aspects

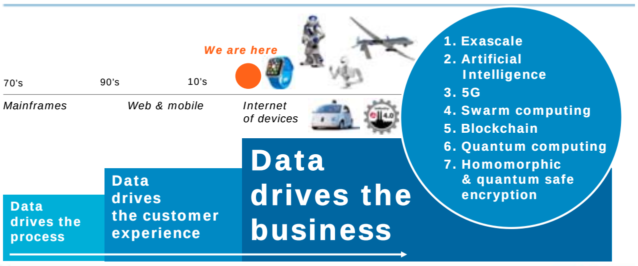
Understood as "**the protection of internet-connected systems, including hardware, software and data, from cyberattacks** [1]"

- Encryption of:
  - **Communication channels (IoT)**
  - **Data and Commands**
- Platform identity
  - **Local / remote location of devices / platforms**
  - **Internal or external to premises or infrastructure**
  - **Users authentication**

Figure: https://pixabay.com/en/hacking-cybercrime-cybersecurity-3112539/
[1] https://searchsecurity.techtarget.com/definition/cybersecurity

4 Data-Driven technologies for Digital disruption

7 data-driven technological breakthroughs will mark the 3rd digital wave



Source: ATOS' corporate presentation

Data driven based on standardization?

- Standardization efforts has started **(150?) years ago** [1] and continues
  - Interoperability with "**old**" but **full functional** devices
- Manufacturers provide guidelines to manage devices including
  - **communication channels**
  - **security and privacy capabilities**
  - **data standards and protocols**
- Data driven Business must have **reliable data** sources
  - **Interoperability** is the key
  - **High connectivity** supports interoperability
- and **cybersecurity**?

[1] https://en.wikipedia.org/wiki/Standardization

Digital Disruption

Business Models – through new sources of business value and partnership, driven by data and connectivity

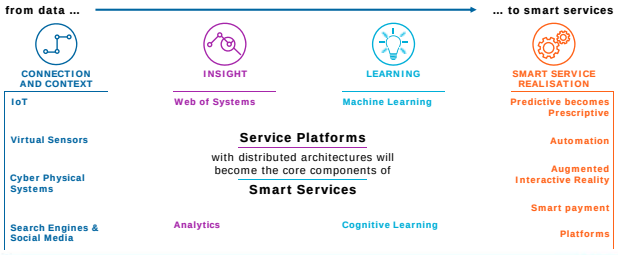
Ways of Working – resulting from changes in business processes and the very nature of work

Disruptive Technologies – the developments that bring revolutionary changes to the "art of the possible" not just evolution

Evolving Challenges – familiar challenges that need to be addressed with different perspectives as a result of the emergence of new influences

Source: ATOS' corporate presentation
Atos

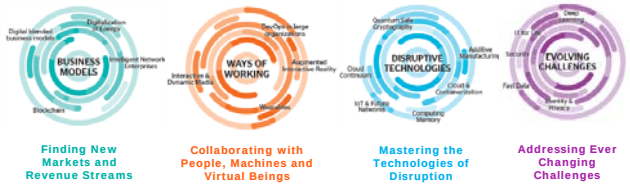
The emergence of smart services



Source: ATOS' corporate presentation
Atos

4 sources of digital disruption

19 evolving and emerging technologies



Finding New Markets and Revenue Streams

Collaborating with People, Machines and Virtual Beings

Mastering the Technologies of Disruption

Addressing Ever Changing Challenges

Source: ATOS' corporate presentation
Atos

Cybersecurity

- **Data management**
  - Collection
  - Transmission
  - Storage
- **Devices and Infrastructure protection**
  - **Devices** identification and authentication
  - Users management (**inside threats**)
  - Platforms and devices risk management

The **cybersecurity** is a critical aspect that MUST be embedded

Cybersecurity is not a **static solution**, initial protection must be enhanced for the whole device life

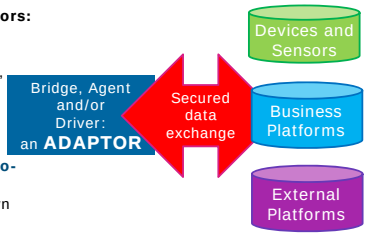
In **R&I** cybersecurity is not critical aspect during the design – it's a **limitation**

Atos

5 Ambition and Approach

Device oriented adaptors

- **Common concepts for Adaptors:**
  - An adaptor has **many functionalities** (e.g. identification, data collection, commands, transformation, security)
    - A functionality is based on **many services**
    - A service uses many **micro-services**
    - Each adaptor can have own **semantic/ontology**
  - **Reusable, reliable, resilient**

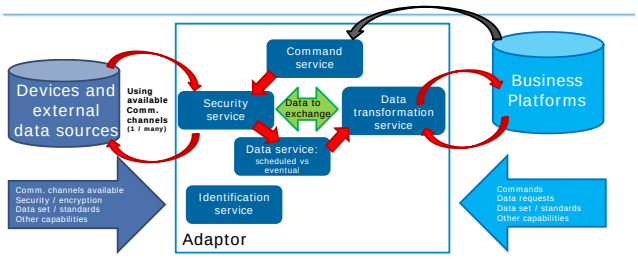


Atos

Device Oriented adaptors

- **Device-oriented Adaptors** means that an adaptor is only operable for a specific device and based on the **manufacturer model, year and functionality** provided; consequently, an adaptor is like a driver or bridge that allows an OS manages the device related to the driver
- Adaptors aims are:
  - **Secure communication**
  - **Collect Data** in a secure manner
  - **Transform Data** before deliver
- Services and micro-services can be re-used or enhanced for other adaptors (**and distributed in a digital market place**)
- **Open** source, **open** standards

Adaptors as bridges for interoperability



Adaptor's services

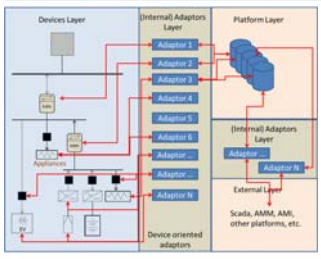
- **Identification service**: obtains information provided by manufacturers (Model, S/N, Year, etc.) used to identify the device and communication channels available and create "drivers" for data and command services
- **Data service**: request and collect data per time slot. Once device delivers the data, it is send to the transformation service
- **Command service**: Device with bi-directional capabilities use it to send commands from the control centre (e.g. SCADA) to the device and validate its execution and results, e.g. specific data requested, firmware updates, etc.
- **Transformation service**: platform oriented service to convert device´s data set to the data structure used by the platform and vice-versa
- **…**

(Cyber) security

- **Security service**: when available, manages all operations with devices or platforms. This service ensures reliability by:
  - **Provide additional security** to communication channels (IoT)
  - **Manage** data/command **encryption**
  - **Manage device reliability** (e.g. checksum of firmware for not authorized changes)
  - **Other security measurement** (e.g. identification/authentication)

Source:https://www.istockphoto.com/es/fotos/security?sort=mostpopular&mediatype=photography&phrase=security

Adaptors usability: interoperable



- Any **environment or infrastructure**
  - Water, Energy, Gas, etc.
  - Home, Nano- or Micro-grids
- **Internal / external** interoperability
  - Between platforms or solutions
- Manufacturers can provide enhanced **devices** with **additional** functionalities
  - Basic adaptors can be improved by third parties re-using services and microservices
- Availability of adaptors managed using **digital market places**

6 Digital Market Place

Some Facts

- A key ingredient for improving growth performance of countries is innovation. **Start-ups and Micro, Small and Medium Enterprises** (MSMEs) play an important role in developing and commercializing innovations [1]
- Globally, MSMEs account for 95% of all enterprises and for **two thirds of all formal jobs**. The sector also plays a critical role in the job creation process. Data from the **EU show that 85%** of net employment creation is attributable to MSMEs [1]
- Information and Communications Technology (ICT) – including cloud computing and the rise of software-as-a-service – has reduced the **cost of innovation and market access**, allowing small tech businesses to compete with established industries [1]

[1] https://www.itu.int/dms_pub/itu-s/oth/06/36/S06360000013301PDFE.pdf

Digital Market

- The **Digital Marketplace** is the online platform that all public sector organisations can use to find and buy cloud-based services In the future, it will also become the home for services from other frameworks, including the **Digital** Services framework [1]
- **Digital Single Market**: It's time to make the EU's single market fit for the digital age – tearing down regulatory walls and moving from 28 national markets to a single one. This could contribute €415 billion per year to our economy and create hundreds of thousands of new jobs [2]
  - **Google** Play Store or **Apple** App Store are successful examples of market places for operating systems
- Re-usability of services to create enhanced solutions
- Continuous improvement of Adaptors lead to **near-to-immediately deployment** of standardization results

[1] https://digitalmarketplace.blog.gov.uk/digital-marketplace-strategy-march-2015/
[2] https://ec.europa.eu/commission/priorities/digital-single-market_en

Advantages of Digital Market

- Improves **accessibility of consumers and business** to an unified and common marketplace to marketing ICT solutions and services meanwhile enhance EU's digital world
- Provides the **environment for continuous improvement of technology services** meanwhile it supports infrastructure development.
  - **Skilled computer experts** (e.g. hackers) can uses their technical knowledge to resolve a problem.
  - **Security hackers** can provide innovative solutions for bugs or exploits used to break into computer systems with their technical knowledge.
  - Both **obtain legitimate benefits** from their activities
- Ensures that Europe's **citizens**, **business and employment** take full advantage of digitalisation

Impact on Cybersecurity

- "Closed" adaptors provide enhanced **interoperability with no human interaction**
- **Best-in-class** (and tested) solutions available immediately for any infrastructures
- Assessment y device **certificates**
- **Reusability, Reliability and Resilient**
- **Future** improvement and **evolution**
- Digital Market Place as **testing and security control** environment

Source:https://www.istockphoto.com/es/fotos/security?sort=mostpopular&mediatype=photography&phrase=security

and on Critical Infrastructures

- Speed up **Digital transformation**
- **Openness (SMES, entrepreneurs, developers)**
- **Risk assessment**
  - Infrastructure excellence
  - Standardization (**convergence**)
  - Updates/upgrades
  - Selected platforms
- **Manufacturers** and service **providers**

Source: https://en.wikipedia.org/wiki/Critical_infrastructure#/media/File:Grand_Coulee_Dam_

Trusted partner for your Digital Journey

Atos