AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

**Thomas Walloschke**
Chairman
Working Group 11: Smart Manufacturing Industry
Member of AIOTI Steering Board

# IoT International Symposium 2018

## Smart IoT Acceleration Forum, Tokyo
## 9th March 2018

Session3: Smart home in the future –AI speaker, smart home appliance, and smart services bring drastic change in our life

# Future – Business View

- Learning from  Robotics Success Factors  Design and Constitution
- Transfer Insights from Artificial Intelligence to Business

# Issues, Solutions – Social View

- Challenges in the Market and Impact of the EU for Smart Home

# Challenges in the Market and Impact of the EU for Smart Home

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

Horizontally influenced by
IoT Research, Innovation Ecosystems, IoT Standardisation, IoT Policy (GDPR, Cybersecurity Package)

Vertically influenced (excerpt) by
Smart living environment for ageing well, Smart Cities, Smart Mobility, Wearables, Smart Buildings and Architecture

# Influence of upcoming Cybersecurity Packge and General Data Protection Regulation (GDPR)

## Security

- **Security** by design and by default
- **Encryption**
- **Up-to-date** software
- **Strong authentication** settings installed by default

## Privacy

- **GDPR** based user rights

## Safety

- **Product safety legislation** needs to be amended to ensure that the security of all **connected devices** placed in the EU markets do not pose a safety risk for its users.
- The **General Product Safety Directive** as well as product specific safety legislation (Toy safety directive, Low Voltage Directive, Radio Equipment Directive, etc) must be updated to ensure that they are in line with the new '**security for safety**' concept of the general legal framework

http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

# ANEC and BEUC recommendations

• A minimum set of security measures should be obligatory for all connected products as a condition for putting them on the market.
• These requirements should at least include encryption, software updates and strong authentication mechanisms:

It is worth reading this here
Not now!

o All manufacturers and service providers should ensure that the data stored in their services and the data stored by their connected products is encrypted. Manufacturers and service providers shall also ensure that third parties accessing the data keep it properly encrypted. Finally, communications coming in and out of the connected product should be encrypted end-to-end.

O Manufacturers shall make sure that when they first put a product on the market, the software that runs on the product is as secure and up-to-date as it can be. In addition, manufacturers should also be required to ensure that the software is updated during the entire lifecycle of the product whenever this is needed to guarantee that it remains secure

https://www.anec.eu/
http://www.beuc.eu/

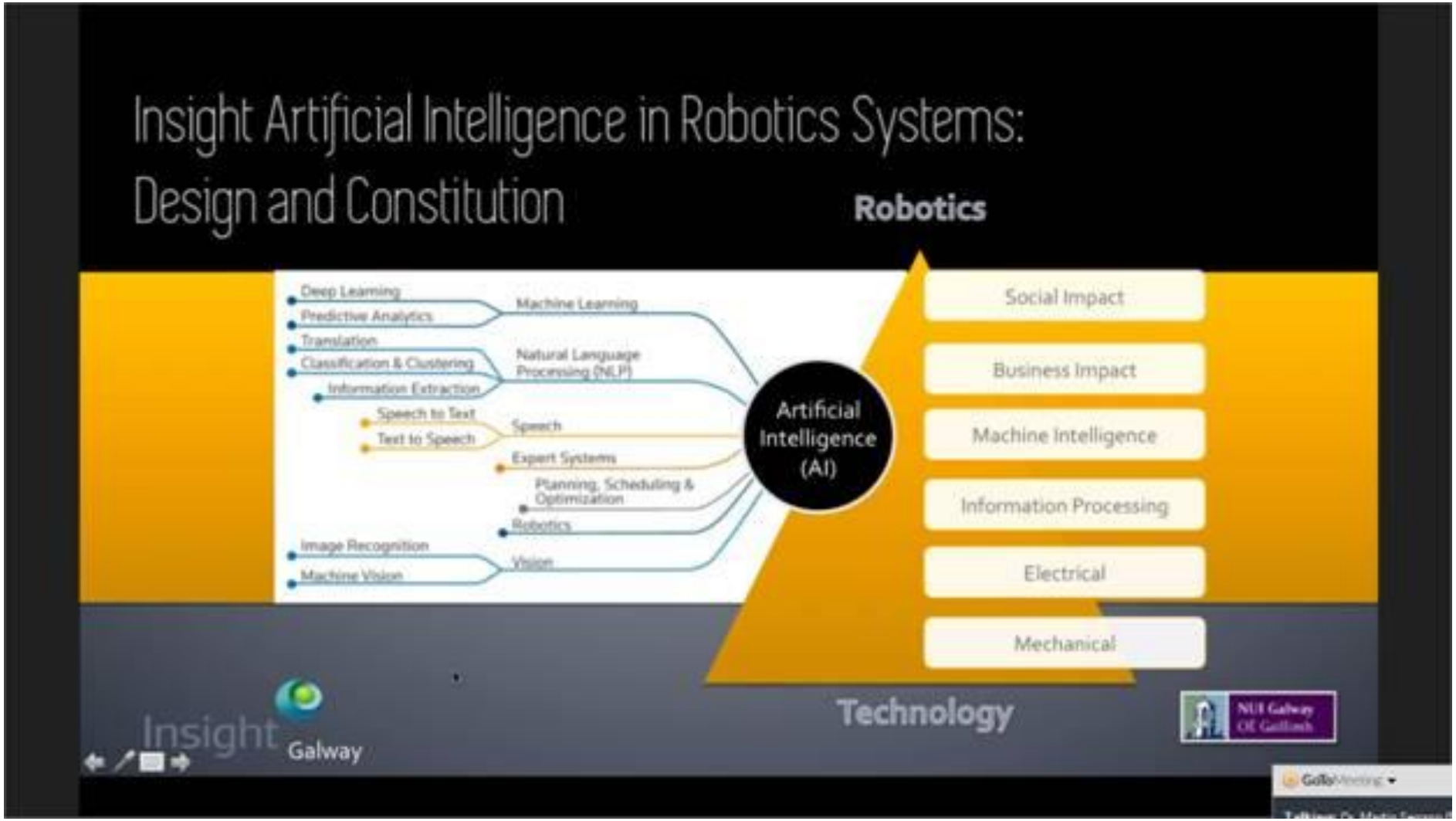
o Connected products and services intended for consumers should by default only accept state of the art security authentication methods. This is for example the case of passwords that contain a certain level of complexity(e.g. numbers, capital letters, etc.) and two-factor authentication systems.

The regulatory framework establishing a minimum set of security requirements shall be regularly reviewed to ensure that the list of security requirements follows the technological evolution.

• The personal data collected through connected devices shall be adequately protected according to the General Data Protection Regulation.

# Learning from Robotics Success Factors Design and Constitution

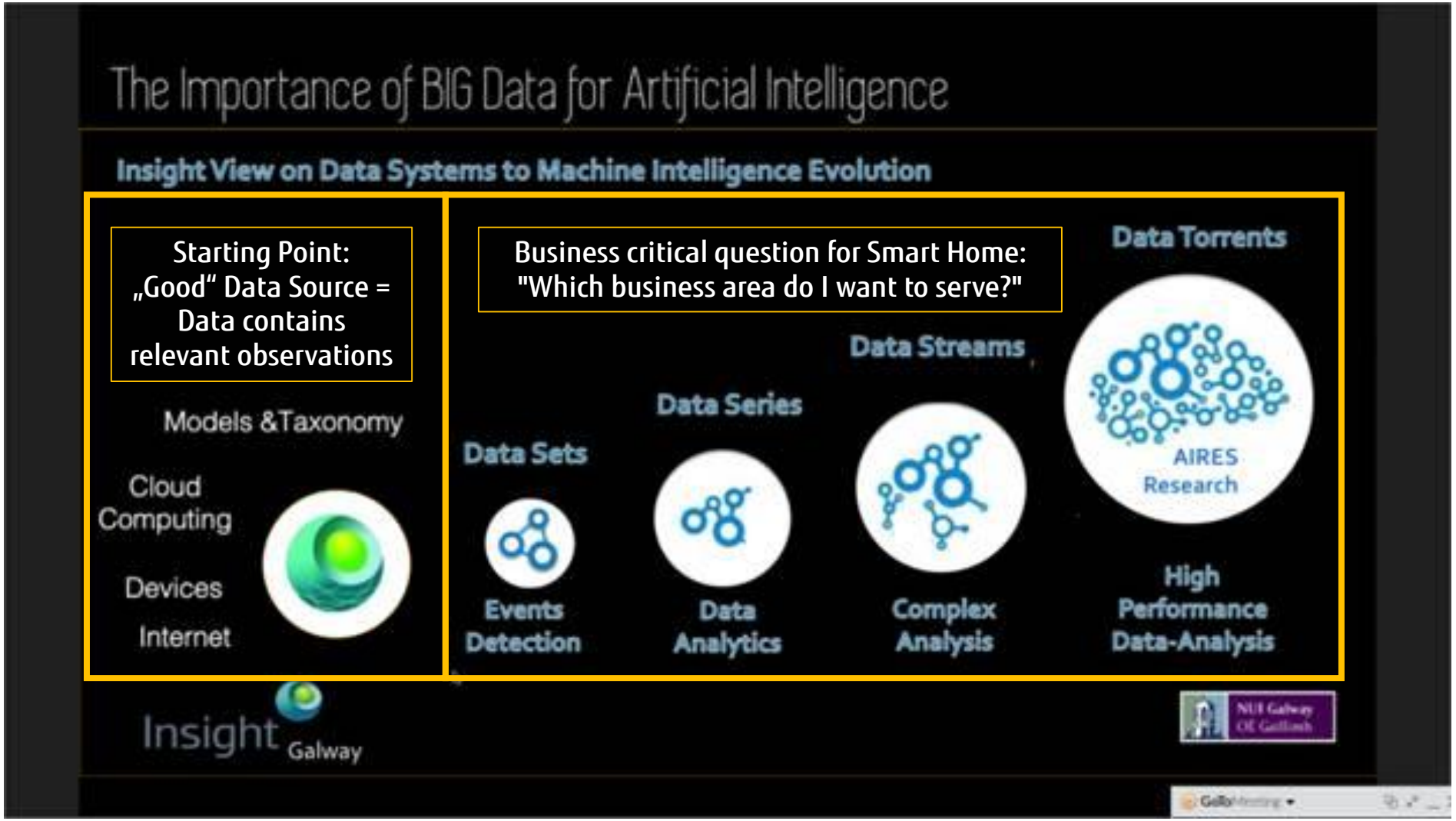
# Transfer of Requirements for Success in Design and Constitution of Robotics to Smart Home Infrastructures




Ref: Insight Centre for Data Analytics, https://www.insight-centre.org/

# Transfer Insights from Artificial Intelligence to Business

# Transfer of Insights of Big Data for Artificial Intelligence as Success Factor of Smart Home Infrastructures




Ref: Insight Centre for Data Analytics, https://www.insight-centre.org/

# Many thanks for your patience
# Q & A to follow

Thomas Walloschke
AIOTI WG11 Chair
thomas.walloschke@ts.fujitsu.com