Digitalization brings “Smartness” into Products

- We see a strong digitalization trend both for
  - “Thing-like” *tangible* products(*)
    (autonomous cars, robotics, home appliances, …)
  - “Service-like” *intangible* products(*)
    (insurance, banking, public administration, …)

- Digitalization gives products a certain “smartness”: increasingly autonomous, self-improving interaction with their environment for the benefit of the user
  - Intuition: A “smart” product behaves like a personal assistant.

- Smartness requires interaction and work-split with others in the environment.

(*) Product = anything a *supplier* offers to a *customer* (paid or free of charge)
Security Standards for a Secure Products Manufacturer

“Smart” Products cross-cut the IT Verticals

- Development
- Engineering IT
- Corporate IT
- Backend / “the cloud”
- Manufacturing IT
- Initial Individualization

“Smart” Product
A few Things **could** go wrong with “Smart” Products

What “could go wrong” is what may happen to a product:
- with **uncertainty**, and,
- with **negative impact** for at least one product stakeholder

Intentional acts on stored or processed data

Potential harm for life and limb

Disclosure / Abuse of personal data

Interdependencies between Safety, Security and Privacy increase.
Security Standards for a Secure Products Manufacturer

Increasingly many Things do go wrong with “Smart” Products

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

... and quite some more


https://www.hackread.com
Security Standards for a Secure Products Manufacturer

Underlying Problem: Trustworthiness Assurance

Objective: Customers entrust products with potentially critical missions and potentially sensitive data.

Challenges

- **As a customer**, how can I assess the trustworthiness of a certain product?
  - remedy information asymmetry and take a risk-based decision.

- **As a supplier**, how can I make sure (assure) that
  - my product is **sufficiently trustworthy** (make sure I do it right)?
    - state-of-the-art systems engineering, and risk management over the entire product lifecycle (esp. incident response)
  - my product is **perceived** as sufficiently trustworthy (make sure I sell it right)?
    - explain how you address the customer’s security needs in a way the customer understands.
Towards Doing it right: Risk Management Standards

- On a generic, sector-agnostic level, sufficiently many appropriate international standards exist (e.g., ISO 31000).

- Sectors often require adaptations of generic standards to their specific environments.
  - Examples: ISO 27005, IEC 62443

- If sector-specific standards are created, they shall be inherited from the same (at least as as few different as possible) generic standards.

- The bottleneck is often not the availability of appropriate standards, but the ability to use them.

Appropriate Risk Management requires both Methods and Competence to use them.
Security Standards for a Secure Products Manufacturer
Towards Selling it right: Talk about the Good you do

▶ After you’ve done it right, talk about how you address the customers’ (and other stakeholders’) needs…

▶ … in a way the stakeholders understand and value

▶ may be a data sheet with security features
▶ may be a recognized label or certificate
▶ may be a “don’t worry, we’ve got it covered” feel-good message
▶ … or other (combinations of) measures that serve the purpose

The appropriate way of communicating security properties varies greatly among domains.
Security Standards for a Secure Products Manufacturer
Regional and Global Developments

- A global company prefers global standards.

- But: People are different, and so are the markets.

- Regional and national standards are unavoidable, but shall be harmonized as much as possible.
Security Standards for a Secure Products Manufacturer

Conclusion

- “Smart” products are dragging other IT verticals (corporate, manufacturing, engineering) into the product world.

- Product trustworthiness assurance primarily requires systems engineering and risk management.

- What is perceived as a trustworthy product and how to assure this trustworthiness differs greatly among verticals, market segments, and stakeholders.

- Solutions have to be appropriate for their context as well as harmonized across contexts.
THANK YOU