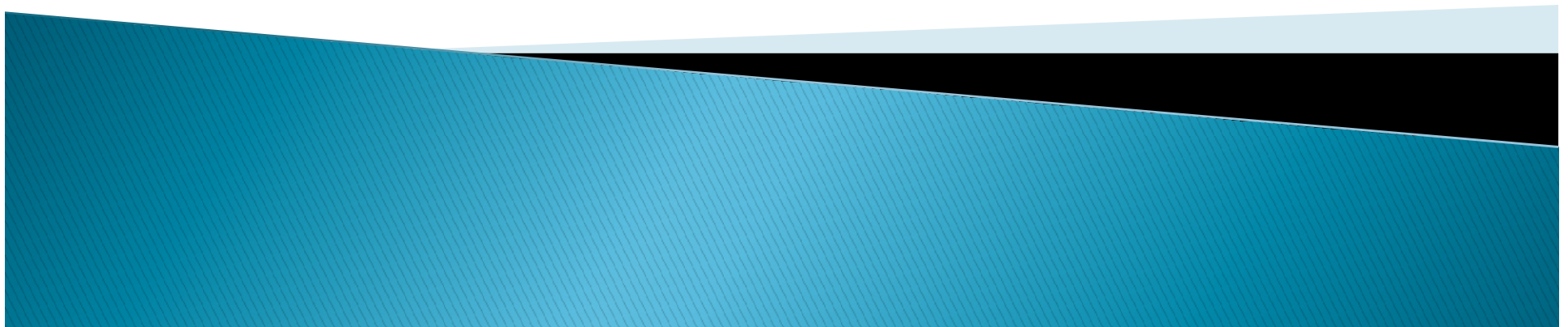


Modelling in Security by Design

Group 2 – Contrary position



Security by Design – Advantages

- ▶ Reduced risk of security gaps and vulnerabilities in hardware and software.
- ▶ less likely to be the victim of an attack or other security threat.
- ▶ higher quality and robustness of the products.
- ▶ Greater customer confidence in the products provided.
- ▶ less cost to eliminate vulnerabilities and security gaps.
- ▶ reduced liability risk for companies.
- ▶ Avoidance of production downtimes in Industry 4.0.
- ▶ more security in the Internet of Things.

Modelling in Security by Design – Disadvantages

- Cost, time and resource intensive
 - The time needed to create the models can already be put in the development process.
- Requires modelling skills of the development team
 - Teams need to be trained, which takes time and money.
- Dangers of a pre-structured design
 - Can lead to a less flexible development process.
 - Safety concerns overlooked in the model might not be considered in the development process.



Modelling in Security by Design – Disadvantages

- Confusion caused by changing models
 - Changes, especially to complex models, can be overlooked and cause confusion and/or security threats.
- False confidence through models
 - A feeling could be conveyed that everything has been taken into account and considered, so that there is no further questioning of safety aspects.

References:

- ▶ Schmitz, P. (2021) Was is Security by Design. *Security Insider*. Available from: <https://www.security-insider.de/was-ist-security-by-design-a-1071181/> [Accessed 07 June 2022].
- ▶ Graube, M., Hensel, S., Iatrou, C., & Urbas, L. (2017) Information models in OPC UA and their advantages and disadvantages. *IEEE International Conference on Emerging Technologies and Factory Automation*. 1–8. Available from: <https://ieeexplore.ieee.org/abstract/document/8247691> [Accessed 07 June 2022].

