Cyber-Security by Application of Secure Hardware Architectures

GFEDCBAZY

20. DWT – Marineworkshop, Linstow, September 24 – 26 2018

What do secure hardware-architectures need?	Triple separation!
What needs to be separated?	- programs from data to be processed - program interfaces from data interfaces - program related tasks from system related tasks (software loading from system operations)
Additional requirements?	- Categorization of all software (data and program) - Independent memory units for each data category
Any benefits Besides higher Cyber-security?	- Full SW-quality- and -configuration-sovereignty - No work required after hacker attacks - No need for Anti-Virus-Software and the like, resulting in longer lifetime and saved license fees - Spectre and Meltdown do not cause any harm. - Technical Basics for new devices