Day	27.02.2019
Time	16:00 - 16:30
Session/Workshop	Session 5.4
Title	OP-TEE – A Intro to a Trusted Execution Environment
Description	The security of Embedded Systems has become a key concern, especially when hacked or tampered systems create safety issues and can harm people. In order to make an embedded system secure, CPU vendors like ARM offer the TrustZone technology. On top of this ARM TrustZone technology sits OP-TEE, an open source Trusted Execution Environment. OP-TEE allows the CPU to switch to a trusted OS where only trusted Applications can run. As OP-TEE is authenticated by the device at boot up, many security related features can be encapsulated in OP-TEE so the RichOS never sees or access security related data.This offers trusted applications access to memory regions and chip functions which non secure applications can not. The context switch happens over a OP-TEE linux driver which can make a call to the OP-TEE OS. This communication is monitored by the ARM Trustzone Secure Monitor. The benefit of OP-TEE running on a Xilinx Zynq Ultrascale+ MPSoC, beside of the key benefits for use in industrial and automotive systems, are the build in special functions offered by the device itself like AES and RSA encryption, SHA3, PUF (Physical Unclonable Function) and unique Programmable Logic functions. Our presentation starts with introducing OP-TEE, which problems it solves, why customers would use it. Furthermore will this presentation show the joint work between Xilinx and MLE to optimize and made work on OP-TEE on ZU+ MPSoC devices and show how to implement OP-TEE on a Xilinx Zynq Ultrascale+ MPSoC.
Speaker 1	Andreas Schuler, Missing Link Electronics Andreas Schuler holds a Bachelor of Engineering degree in Industrial Electronics and is Director Applications at Missing Link Electronics where he coordinates joint work of Xilinx and MLE. His field of operation reaches over Artitecture design, Image processing, Security, Neural Networks to product development.