Network Monitoring of Industrial Control Systems: state of affairs

Sandro Etalle (TU/e)

Summary: Despite the recent notable advances in the field of security for OT, industrial Control Systems (ICS) are still not resilient against cyberattacks as they should and could be. In particular, network monitoring of large OT systems is still very hard. This is due to the fact that ICS network traffic is deeply context dependent: systems that behave very similarly on the outside, may look completely different when one investigates their network behavior. In the DEPICT project the University of California Santa Cruz and the University of Eindhoven have joined forces to combine their expertise in different approaches (e.g. quantitative and qualitative ones) of network monitoring for ICS. Goal is to improve the situational awareness, and ultimately, ICS security. In this talk we present some of the latest updates and challenges in the field.