EUTC Cybersecurity Workshop

13 November 2019
EDF Research Centre
Boulevard Gaspard Monge
91120 Palaiseau FRANCE

Final Programme

9:00 Registration & Coffee

9:30 Welcome & Introduction: Julian Stafford EUTC

9:40 Welcome: Vincent Audebert, IoT and Telecom Expert, EDF

9:45 EDF view: Youssef Laarouchi, PM Cybersecurity Research Group EDF

Short overview of importance of cyber security to EDF.

10:00 Previous Incidents and NIS directive - Tania Wallis Glasgow University

Brief outline of cyber incidents including Ukraine. Experiences with implementing the NIS Directive including efforts by OES to manage supply chains in different sectors. NISD and Supply Chains

10:30 Edge Compute Erez Koren Director of Business Development RAD

The IoT revolution enables automation and monitoring of sensors and systems like never before. It affects the traditional utilities and industry verticals by enabling new and advanced applications. While the allure of application agility, intuitive HMI and analytics is irresistible, it also poses a serious gap for traditional infrastructure in terms of security, ROI and data usability.

Edge Computing-enabled platforms allows higher security for new infrastructures, at the same time seamlessly bridging such gaps

10:55 Introduction of E-Sim technology – Marco Bijvelds Kore Wireless

Connectivity is a prerequisite for all IoT applications and many applications rely on cellular connectivity. Traditional cellular connectivity solutions have inherent disadvantages that increase the cost related to connectivity significantly over the lifetime of an IoT device. eSIM addresses these concerns through remote provisioning of the SIM. Secure transfer of both data and SIM profiles is imperative to make this new technology viable for mission critical IoT applications.

11:20 Morning Coffee Break

11:55 Managing Supply Chain Risk Holly Grace Williams, Secarma Ltd

Overview of Secarma's expertise and experience of dealing with cyber security protection, best practise and associated trends.

12:35 Impact of increasing cyber security requirements on bandwidth in the access layer - Kinan Ghanem (Power Networks Demonstration Centre)

The cybersecurity requirements of smart grids place increasingly significant requirements for data throughput in all levels of the network. In this session, Kinan Ghanem will present current progress in a research project that examines how to handle this 'order-of-magnitude' increase in security communications throughput.

13:00 Lunch

14:00 Securing legacy devices in modern networks – Patrick Conway (Virtual Access)

Even with the latest core technology and sophisticated detection capabilities, there remains a significant deployed asset base of older heavy electrical plant and RTUs that present a challenging vulnerability.

14:30 Security by design, the vision of industrial technology provider – Maciej Goraj (Siemens)

Proper cybersecurity approach shall start at the equipment and software vendor itself. "Security by design" measures include end-to-end approach in vulnerability handling and disclosure process. IEC 62443 certification process guarantees own "Secure Product Development Lifecycle". To ensure comprehensive protection of industrial plants and electrical substations from internal and external cyber-attacks, all levels must be protected simultaneously – ranging from the plant management level to the field level and from access control to copy protection. The "defense in depth" concept according to standards such as ISA99 or IEC 62443 is a cybersecurity framework that includes cyber risk assessment, implementation, management and maintenance phases.

15:00 Afternoon Coffee Break

15:30 Network Synchronisation - Christian Farrow (Chronos)

The increasing importance of reliable, highly accurate time synchronisation in smart grids requires uninterruptable access to reliable time signals even in the event of failure or spoofing of one or more reference sources. Modern grids require reliable time services to operate. This session will explore the criticality of synchronisation and solutions to ensure a trusted source is always available.

16:00 Satellite connectivity - Kay Barber (Satellite Insight)

Satellite communications provide an increasingly attractive option for connectivity. The introduction of low earth orbit constellations may be an option for low-latency services such as teleprotection. Can satellite connectivity provider a similar level of cybersecurity to terrestrial systems?

16:25 Panel session

16:55 Closing Comments: Julian Stafford, Director, EUTC

17:15 Drinks reception

Thank you to our Silver Level Partner