NexTech 2023 & NetWare 2023

Theme
Security Of Electric Grids

CONTRIBUTORS

PORTO
September 2023

Moderator

Prof. Dr. Dirceu Cavendish, Kyushu Institute of Technology, Japan

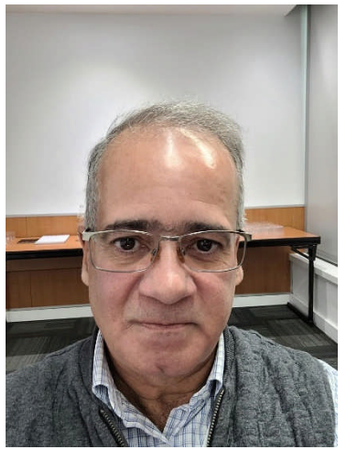
Panelists

Dr. Tiago Espinha Gasiba, SiemensAG, Germany
Prof. Dr. Hajime Shimada, Nagoya University, Japan
Dr. Ing. Eric Veith, Carl von Ossietzky University Oldenburg, Germany

Prof. Dr. Michael Massoth, Hochschule Darmstadt - University of Applied Sciences, Germany

Chair Position

PORTO
September 2023



→ Smart grid evolution opens up new threats

→ Advanced Grid monitoring requires new security protocols

→Energy consumption management demands authentication and secure data gathering

→EV consumers need new travel/commuting planning tools

Panelist Position

Porto
Sept 2023

Eric MSP Veith
UOL

- **Inherent complexity of CPES world-wide makes them brittle:**
  - New threats from the climate catastrophe
  - At the same time, ever-more efficient operation of grids necessary: ICT + AI/ML
  - IoT delivers a load of controllable devices to the grid, critical in mass
    - most are controlled from a white-label cloud solution of the same provider!
  - Resilience is an accepted concept
  - However, situational awareness low due to complexity, “old guard” is leaving, newcomes don’t know the power grids they operate inside-out
- **Proposal: Advanced Learning Systems for Highly-Automated, Resilient Grid Control**
  - CPES research must leave simple AI application domains (e.g., DRL)
  - Advanced architectures necessary: Learn from/incorporate domain knowledge (e.g., safe DRL, offline learning)
  - Adapt on the fly (e.g., continual learning)
  - More cross-over/multi-disciplinary research needed – CPES research is approx. 5 years behind AI research, AI research does not know/accept peculiarities of CPES operation!

Panelist Position

Porto
Sept 2023

Hajime Shimada
Nagoya Univ

- **Work at Univ.: ITC networking team, research/edu. at Grad. Sch. of Informatics**
  - Working at management and development side of Univ. IT Center.
    - Campus wide Networking, WLAN infrastructure (including eduroam)
    - Campus wide Network security (UTM, mail gateway, client tracing)
  - Promoting researches with (Grad.) Sch. of Informatics students.
    - Network management: Malicious traffic detection, automated ACL generation, counter APT operation
    - Counter cyber attacks: malware detection/classification, detecting attack to machine learning systems, constructing security knowledge
  - Educating security intrinsic information literacy and information security

- **Work at Japanese society: Academy (IPSJ, IEICE), Local Cyber Security Community**
  - Committee of SIG-CSEC(Computer Security) and SIG-IOT(Internet and Operating Technology)
  - Committee of cyber-security side conferences.
  - Committee of Local Cyber Security Community

Panelist Position

Porto
Sept 2023

- **Chubu Cyber Security Community (CCSC)**
  - Type of companies: Electronic grid, Gas provider, Train/Airport/Highway operation manager, Finance system manager, (University), (Police).
  - Organized to perform information exchanges for counter cyber attacks.
- **Current hot topic on CCSC**
  - How can we work when we suffered Ransomware attacks?
  - On July 2023, Nagoya Port container import/export registration system stops 2.5 days due to Ransomware and many trailers hung up. (fortunately, successfully recovered with backup)

Industries of CCSC members

Trailers hung up due to system failure with Ransomware

Panelist Position

Porto
Sept 2023

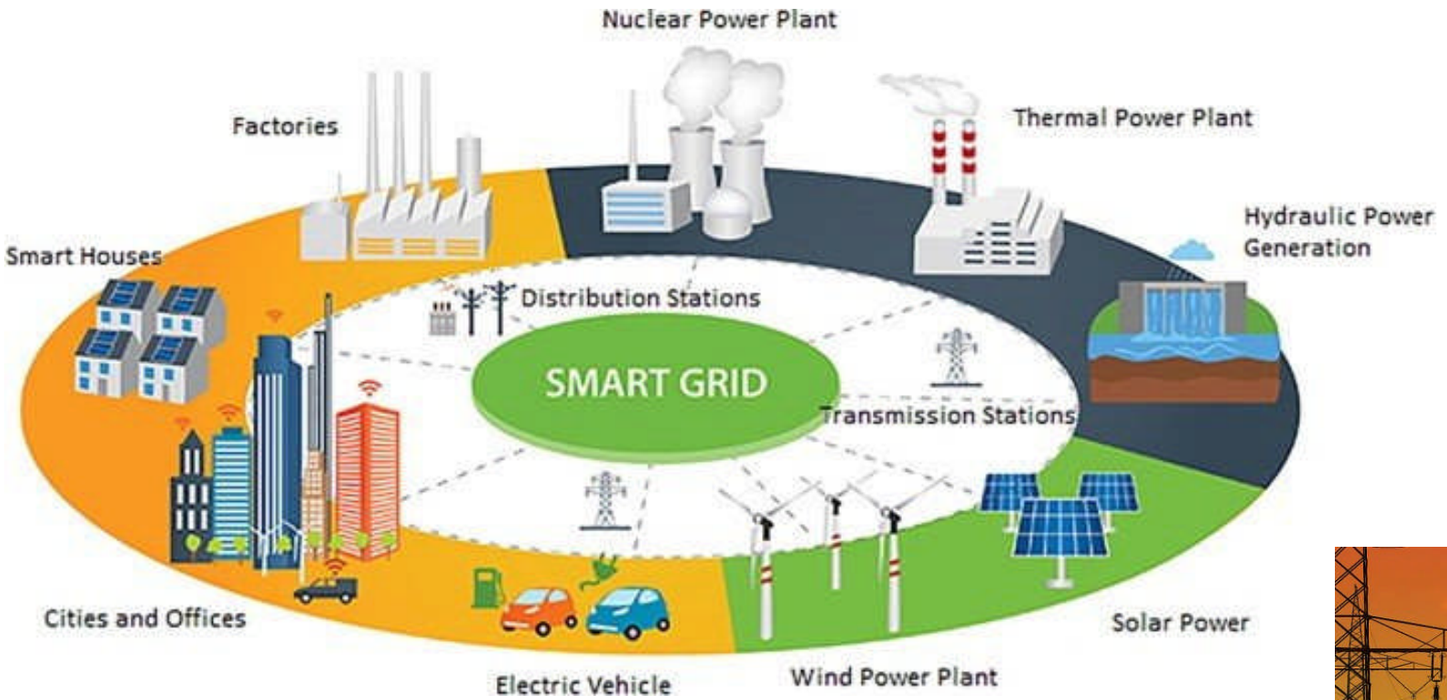
Tiago Gasiba
Siemens AG

- **Cyber-Attacks vs Need for a Holistic View and the Human Factor**
  Cybersecurity incidents, specially in critical infrastructures and supply chains, are evermore important; Proliferation of readily available tools, such as those that enable everyone to perform advanced attacks on systems and networks, leads to the need to have a holistic cybersecurity approach and the need to systematically address “low-hanging fruits”; however, most of the incidents find their cause in the human factor! We need to use automation, but acknowledge its inherent limitations

- **Need for CyberSecurity Education**
  Many problems in cybersecurity are of the category “non-decidable”, e.g., no Turing-complete machine exists that can decide the absence of certain vulnerabilities. *There are inherent technological limitations to cybersecurity automation. At the end, humans will have to make final decisions.* The future of cybersecurity might be dependent on well-designed *decision-support systems* with good heuristics; there is the danger that automation tries to “take over”; Furthermore, trust plays a central role in cybersecurity – we still have not really solved the problem of “root trust” – while automation and AI will put this to the test, a good solution is awareness – perception, protection and behavior!

Panelist Position

Porto
Sept 2023

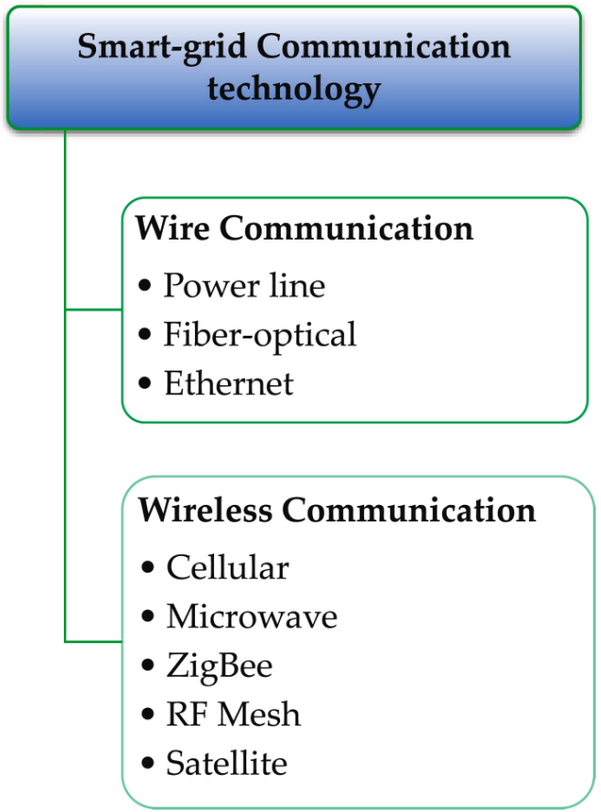


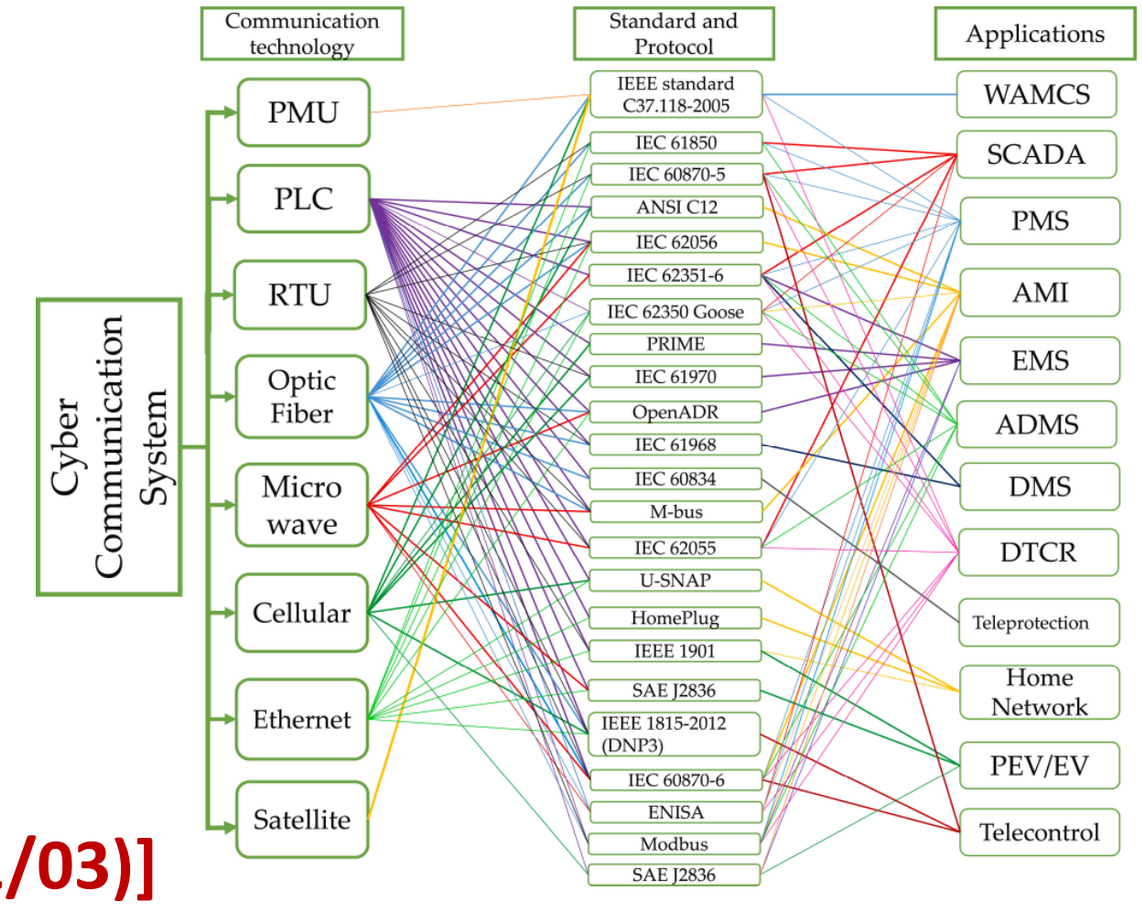
Prof. Dr. Michael Massoth,
Germany

Panel #3 Theme:

Security of Electric Grids

Smart Grid Communication Technologies





[Adapted from (Jha et al., 2021/03)]

Panelist Position

Porto
Sept 2023

Smart grid systems have become so complex that we are likely to see many successful attacks and acts of sabotage against them in the near future.

A major current weakness is that many operators invest only in technical defenses (such as firewalls), but not enough in staff training.

There is also a lack of contingency/emergency plans in the event of an attack, as well as a lack of proven system recovery plans/tests/training.

Prof. Dr. Michael Massoth,
Germany