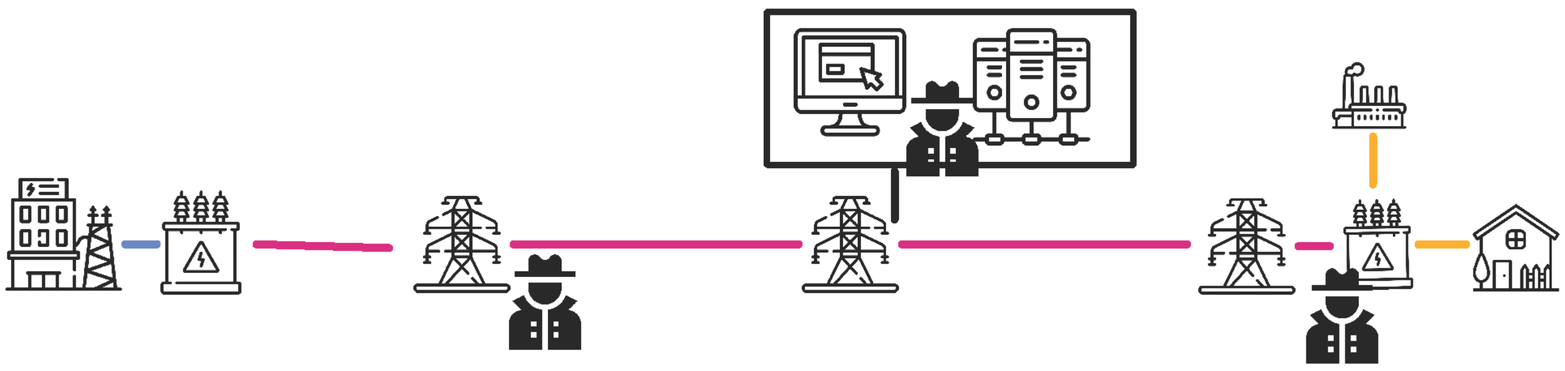
Smart Grids, Smarter Attacks

Can we secure the backbone of our energy future before it is too late?

Verena Menzel* (v.m.menzel@utwente.nl), Johann L. Hurink*, Anne Remke*†
* EEMCS-MOR (**The Energy Group**), University of Twente, The Netherlands
† Safety-critical systems group, University of Münster, Germany

Are our innovations in energy advancing security, or unknowingly exposing the grid to even greater cyber threats?

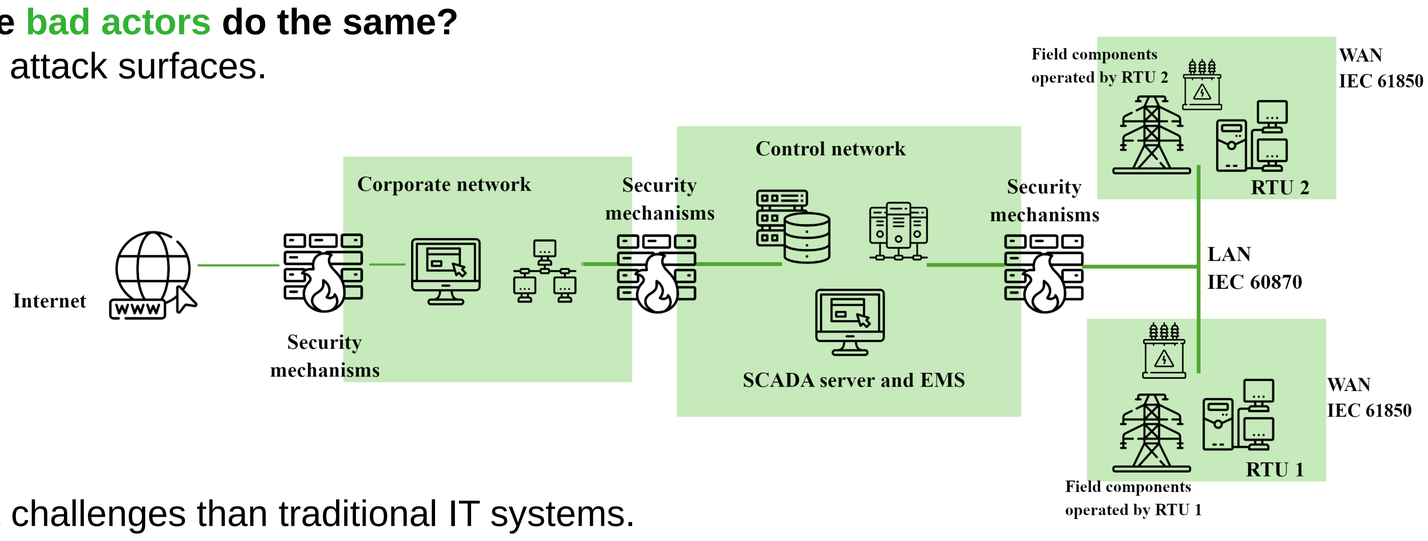


The electricity grid was not built for today's challenges, let alone tomorrow's.
Existing infrastructure was not designed with modern cyber threats in mind.

From a cyber-security perspective, we face a lot of legacy issues that are not solved yet.
Outdated systems (e.g., insecure communication protocols) pose persistent risks.

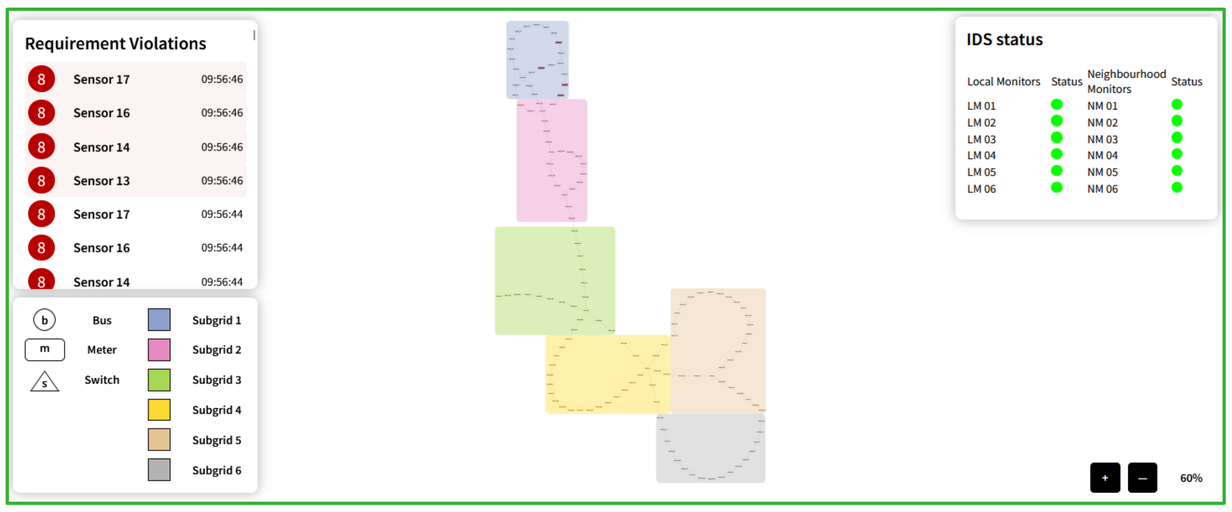
Now, we are adding "smart" technology to an aging grid.
These innovations bring benefits, but also open new vulnerabilities.

If we can access our grid smartly, can't the bad actors do the same?
Increased connectivity means increased attack surfaces.



Standard IT security solutions fall short.
A physically distributed grid has different challenges than traditional IT systems.

Energy and cyber security research must collaborate.
To create a truly secure and future-proof grid, these fields need to work hand-in-hand.



We develop a process-aware decentralized intrusion detection systems combining cyber and physical.
But this is just one layer of the solution and not a one-size-fits-all approach.

Let's power a cleaner, more secure future together.

Achieving this requires bold collaboration, diverse expertise, and layered defense solutions.

Are we ready to rise to the challenge?

Get access to the source code and the papers!

UNIVERSITY OF TWENTE. | Climate Centre

This research is conducted as part of the ISoLATE project (CS.016) funded by the Dutch Research Council (NWO).