Comprehensively Analyzing the Impact of Cyberattacks on Power Grids

Lennart Bader Martin Serror Olav Lamberts

Ömer Sen Dennis van der Velde Immanuel Hacker

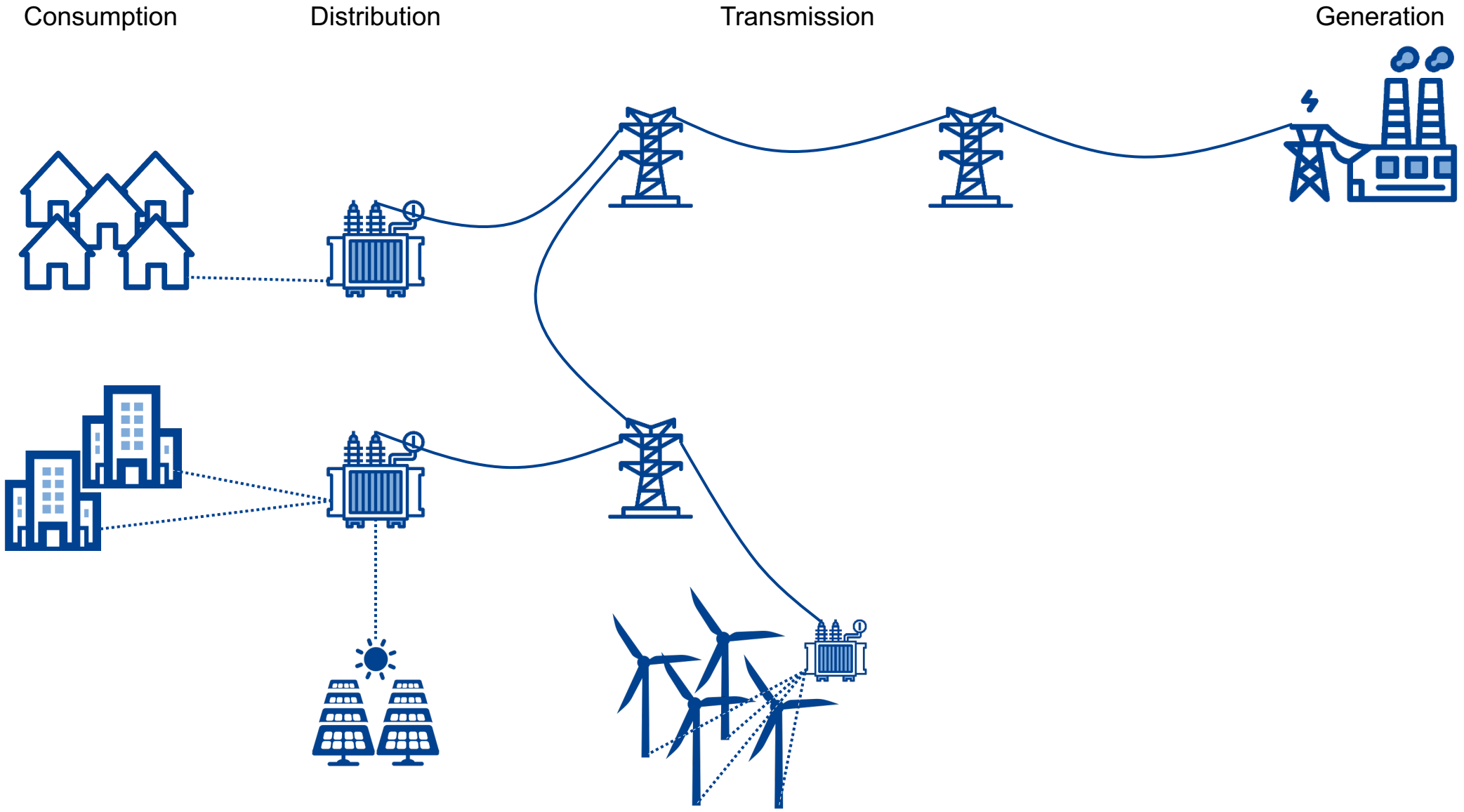
Julian Filter Elmar Padilla Martin Henze

https://github.com/fkie-cad/wattson

Fraunhofer FKIE SPICe RWTH AACHEN UNIVERSITY

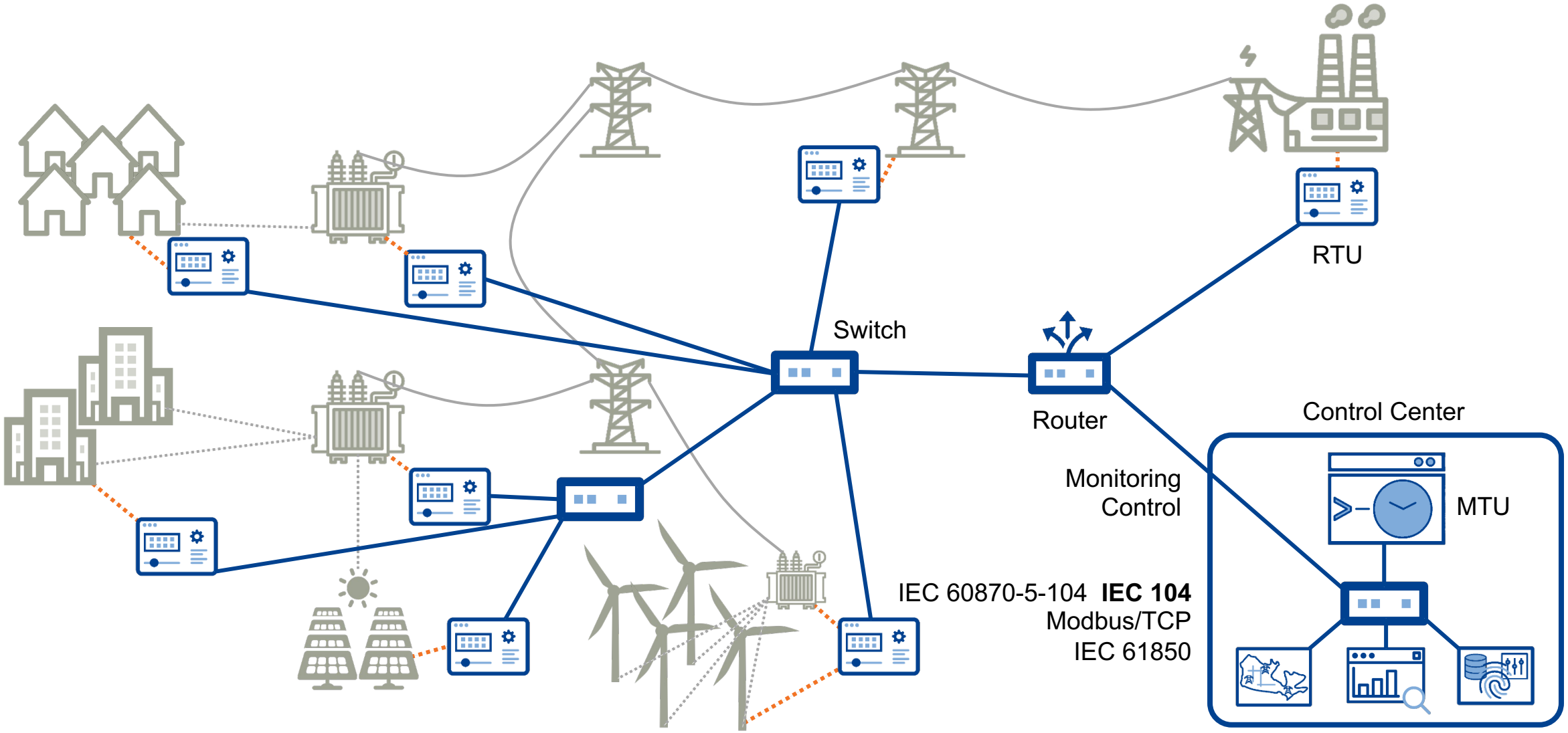
lennart.bader@fkie.fraunhofer.de

Digitized Power Grids are Vulnerable



This graphic uses resources from flaticon.com
Lennart Bader
lennart.bader@fkie.fraunhofer.de

Digitized Power Grids are Vulnerable



This graphic uses resources from flaticon.com
Lennart Bader
lennart.bader@fkie.fraunhofer.de

Vulnerabilities and Common Attacks

Compelling target
- Critical infrastructure
- Physical consequences

Physical access
- Unmanned facilities
- Geographic scale
- Multiple actors

Limited security
- Encryption, authentication
- Network segmentation

- **Multiple attack types in related work**
  - Demand manipulation
  - Denial of service
  - Control command issuance
- **Isolated evaluations**
  - Mostly focus on one attack type / class
  - Mostly considering only one domain (power grid *or* network)

	Attack Type	ICT	Power Grid
Phys.	Device Disconnect		[36], [91]
	Demand Manipulation		[37], [90] [89], [103]
Syn.	Denial-of-Service	[3], [13], [66] [108], **[92]**	**[92]**, [2], [30] [33], [56], [109]
	Replay	[51], [62], [107]	[39], [109], [112]
Sem.		[79]	[2], [39], [99]
	False Data Injection	[13], [43], [45] [44], [51], [102]	[2], [19], [56], [77] [17], [47], [61], [111] [24], [41], [54], [85]

Sophisticated cross-domain evaluations of effects of cyberattacks missing

Lennart Bader
lennart.bader@fkie.fraunhofer.de

Methods for Realistic Cross-Domain Evaluations of Cyberattacks

The real power grid

\+ Maximum realism

\- **Risky**
\- Expensive
\- **Infeasible**

Laboratory setups

\+ **Great realism**
\+ Real devices

\- Limited scalability
\- Inflexible topologies
\- Costly

Simulations

\+ Good realism
\+ Scenarios **flexibility**
\+ **Scalability**

\- Realism depends on model
\- Abstraction

Existing simulation environments

- Often specific focus / use case
  - No **real network traffic**
  - Insufficient **accuracy** (for one domain)
  - Limited **scalability**
- Usage of proprietary hard- or software
  - Limited **availability**

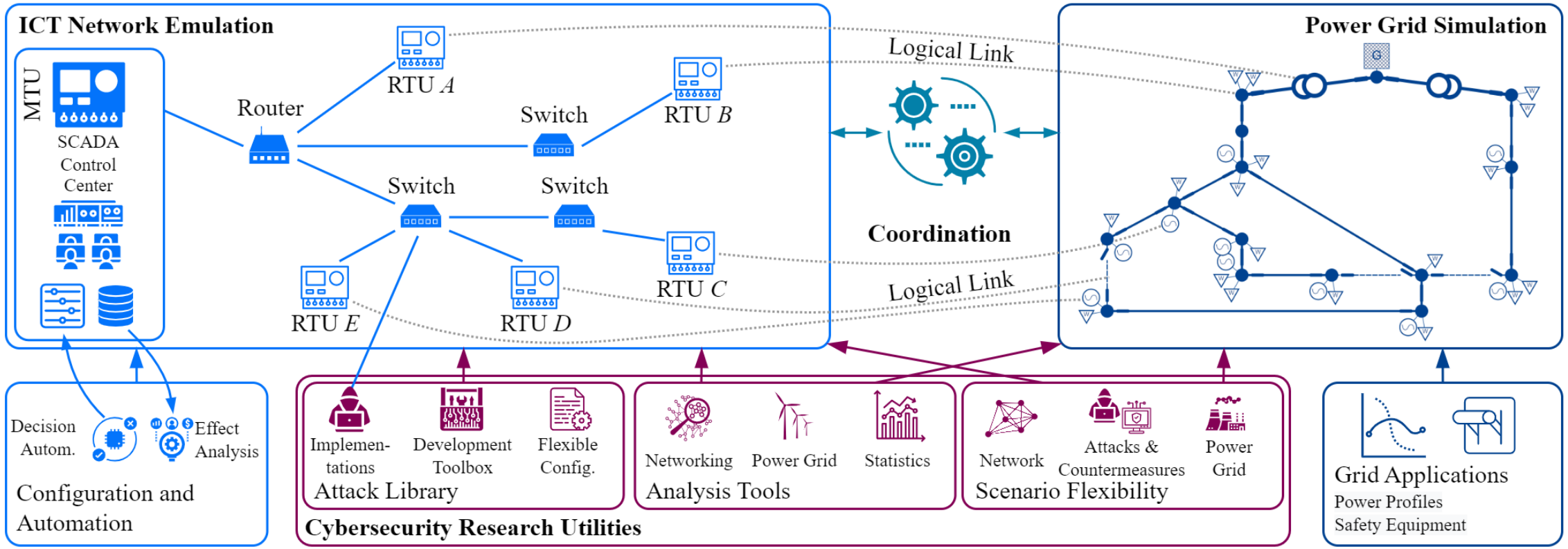
Our proposal

WATTSQN

- Open source
- Co-simulation environment
- Cybersecurity focus

Lennart Bader
lennart.bader@fkie.fraunhofer.de

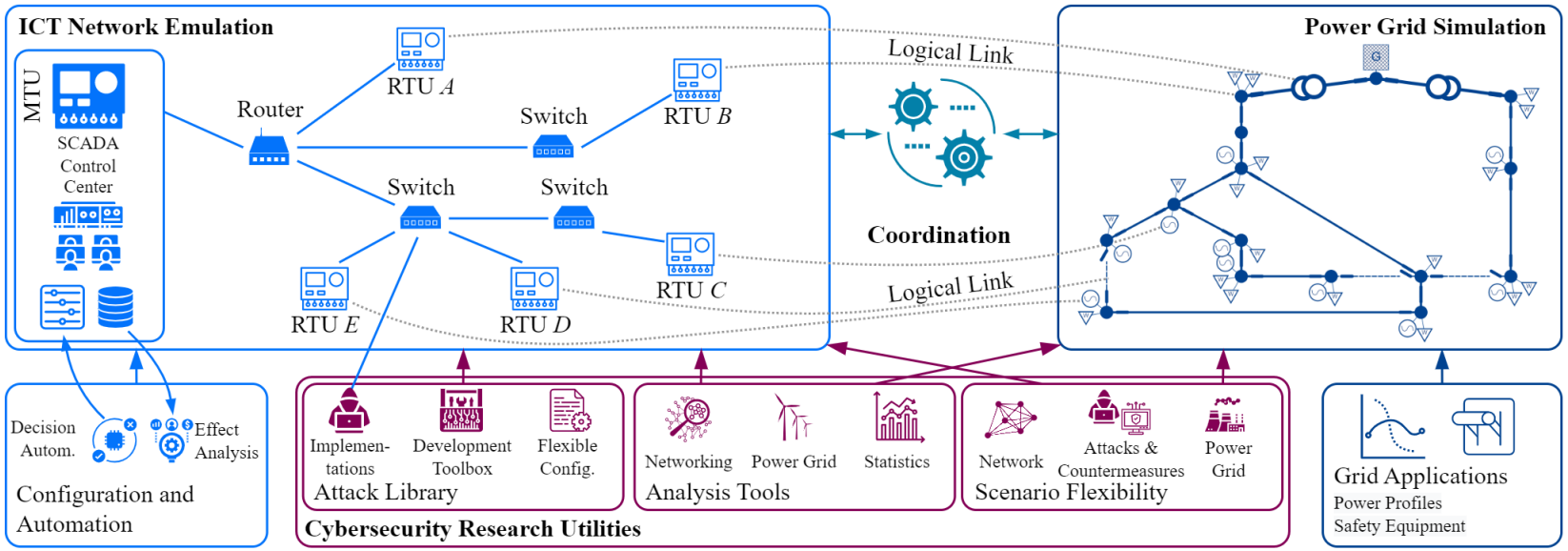
Wattson: A Cybersecurity Research Testbed for Power Grids



- **Network emulation** Containernet-based
  - Realistic network traffic down to Layer 2
- **Power grid simulation** Pandapower-based
  - Static on-demand power flow computation
- **Transparent coordination**
  - Interactions between ICT and grid components
- **Cybersecurity research utilities**
  - Attacks, analyses, configurations

Lennart Bader
lennart.bader@fkie.fraunhofer.de

Wattson: A Cybersecurity Research Testbed for Power Grids



WATTSON is available on GitHub

https://github.com/fkie-cad/wattson

- **Network emulation** Containernet-based
  - Realistic network traffic down to Layer 2
- **Power grid simulation** Pandapower-based
  - Static on-demand power flow computation
- **Transparent coordination**
  - Interactions between ICT and grid components
- **Cybersecurity research utilities**
  - Attacks, analyses, configurations

Lennart Bader
lennart.bader@fkie.fraunhofer.de

Wattson is Accurate and Scalable

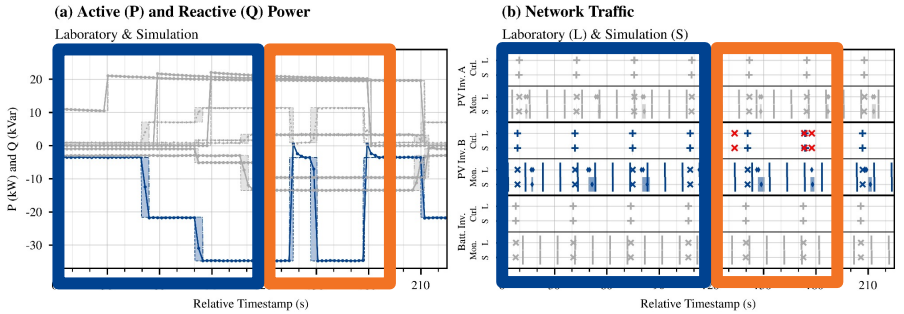
Validation against laboratory grid at RWTH Aachen Univ.

© Martin Braun

Lennart Bader
lennart.bader@fkie.fraunhofer.de

Wattson is Accurate and Scalable

- **Recreate laboratory topology and scenario in Wattson**
  - Normal behavior
  - MitM-based attack
  - Compare laboratory and simulation

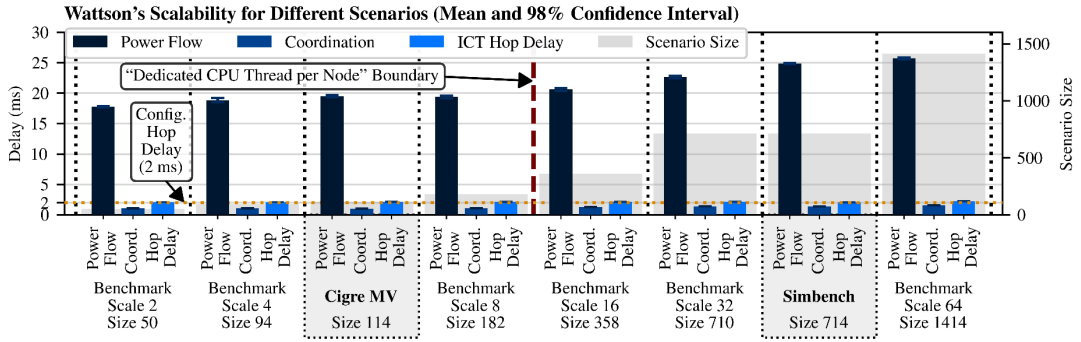


© Martin Braun

Accurately matching behavior under normal and attack conditions

Scalability

- We evaluated Wattson‘s scalability with synthetic and reference power grid topologies
- Suitable **performance** for evaluating cyberattacks
- **Scales** to realistic grid sizes



Lennart Bader
lennart.bader@fkie.fraunhofer.de

Evaluating Cyberattacks against Power Grids with Wattson

Destruction of equipment

Interference with network traffic

Manipulation of application layer traffic

Physical Attack

- Destruction of substation
  - Power grid assets
  - ICT equipment

Flooding

- TCP SYN flooding
- Affects multiple RTUs
- Saturation of network links

Industroyer

- Secondary IEC 104 client
- Issues control commands
- Disconnects large parts of the power grid

ARP Spoofing

- Targeted denial of service
- Interrupt RTU connections
- Loss of visibility
- Loss of controllability

False Data Injection

- MitM-based attack
- Measurements manipulation
- Command injection
- Live and transparent

Lennart Bader
lennart.bader@fkie.fraunhofer.de

Evaluating Cyberattacks against Power Grids with Wattson

Destruction of equipment

Interference with network traffic

Manipulation of application layer traffic

Physical Attack

- Destruction of substation
  - Power grid assets
  - ICT equipment

Flooding

- TCP SYN flooding
- Affects multiple RTUs
- Saturation of network links

Industroyer

- Secondary IEC 104 client
- Issues control commands
- Disconnects large parts of the power grid

ARP Spoofing

- Targeted denial of service
- Interrupt RTU connections
- Loss of visibility
- Loss of controllability

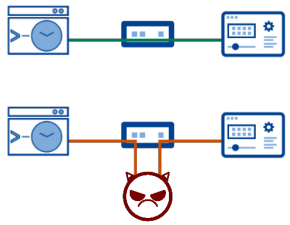
False Data Injection

- MitM-based attack
- Measurements manipulation
- Command injection
- Live and transparent

Lennart Bader
lennart.bader@fkie.fraunhofer.de

False Data Injection Attack: Scenario

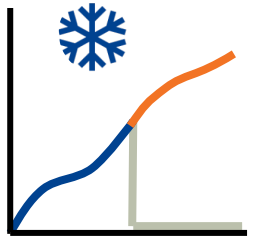
Attack Phases



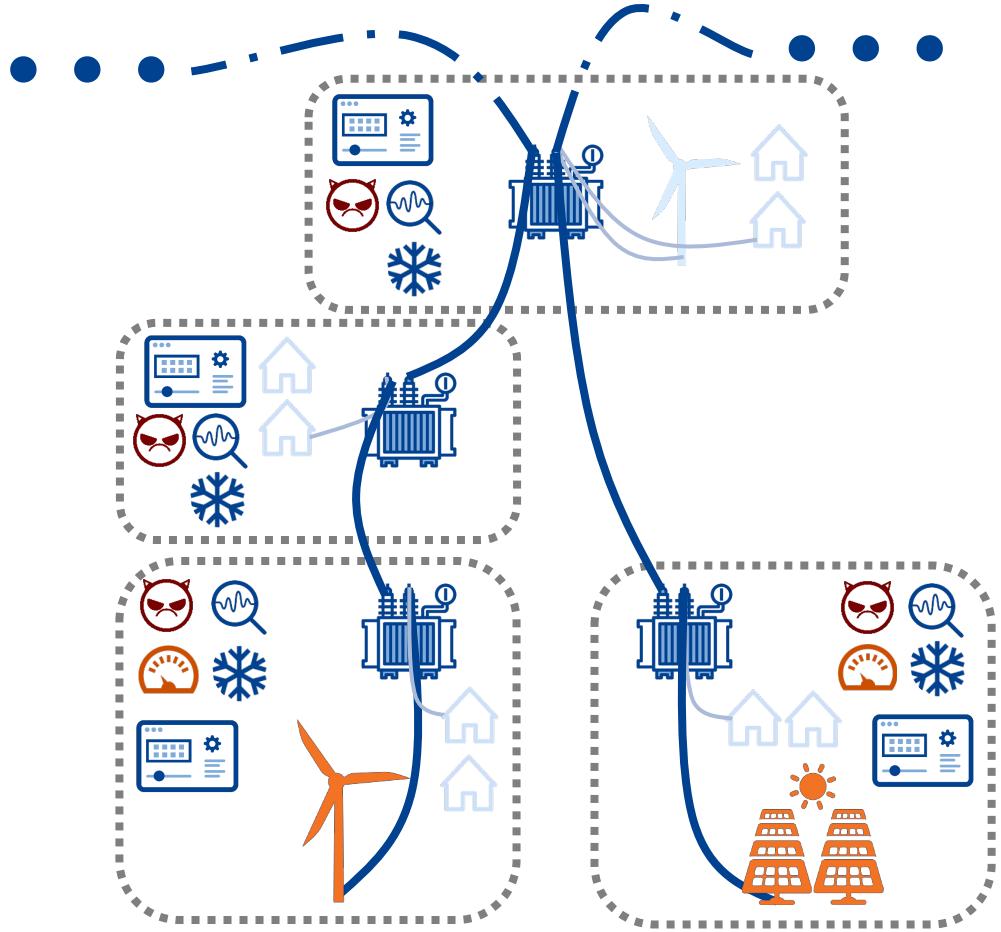
- MitM via ARP spoof
  - Learn SEQ/ACK (TCP) and SSN/RSN (IEC 104)

- Eavesdropping & recording
  - Learn measurement values & store history

- Command Injection
  - Inject control commands into active connection



- Freezing
  - Manipulate measurements to represent former grid state



Simbench semi-urban medium-voltage scenario
~ 110 substations, 119 RTUs
Represents a district

This graphic uses resources from flaticon.com
Lennart Bader
lennart.bader@fkie.fraunhofer.de

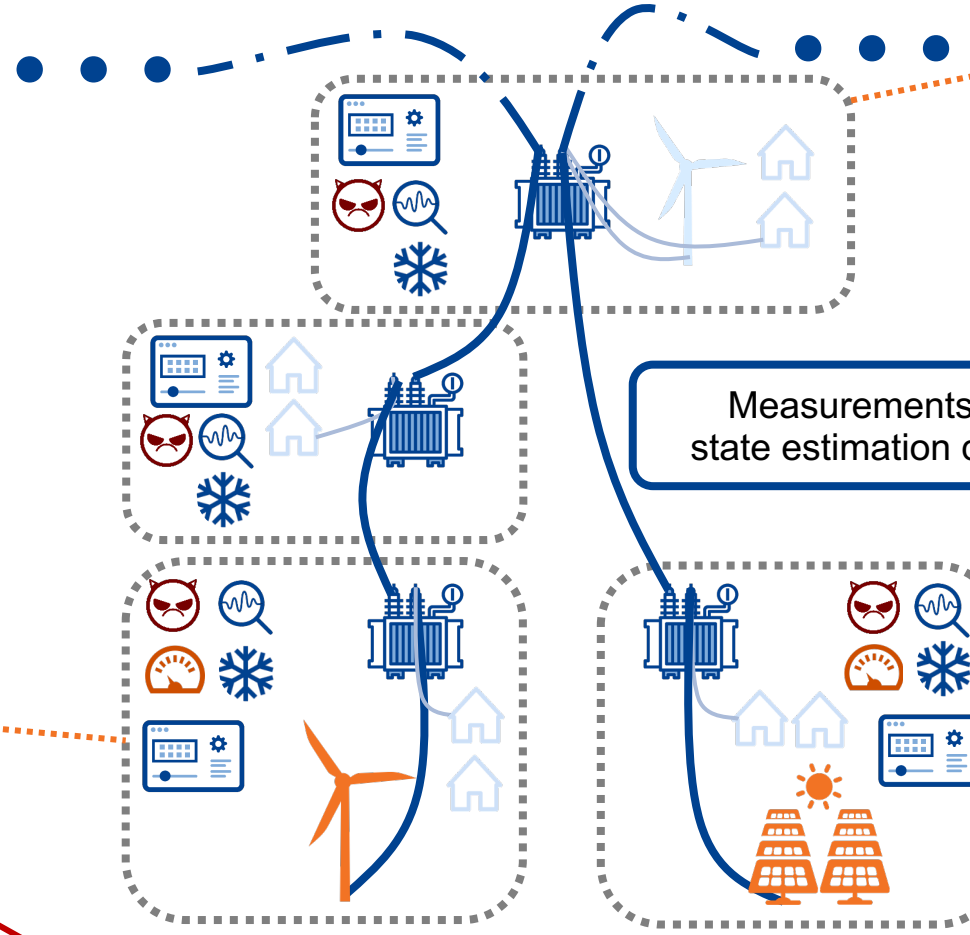
False Data Injection Attack: Evaluation

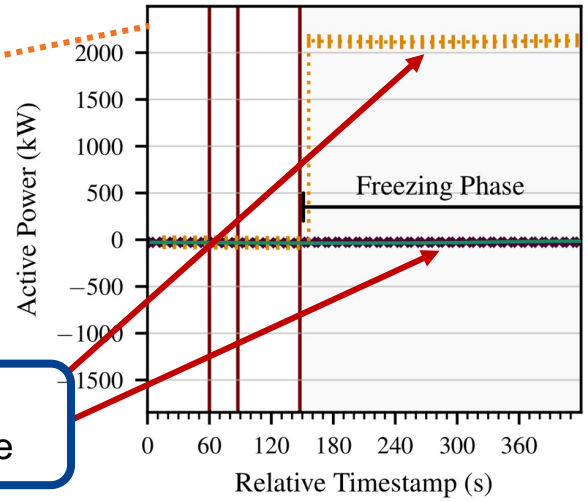
Loss of visibility

Loss of control

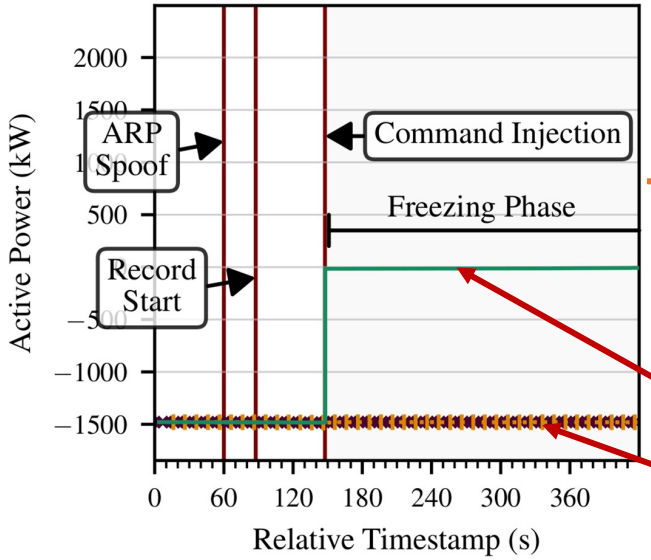
Incorrect conclusions

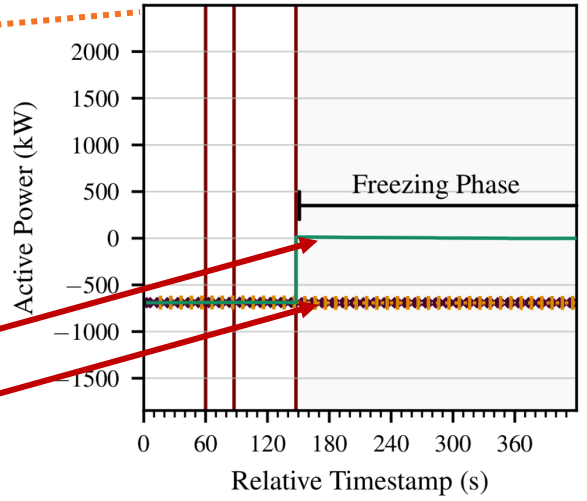
Impaired grid operation





Measurements and state estimation diverge





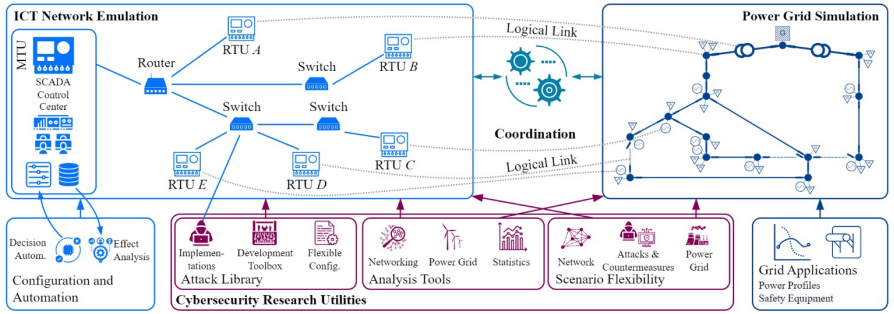
Measurements and state estimation diverge from actual grid state

This graphic uses resources from flaticon.com
Lennart Bader
lennart.bader@fkie.fraunhofer.de

Conclusion

- **Power grids as targets for cyberattacks**
  - Digitized cyber physical system and critical infrastructure
- **Evaluation of attacks and their effects**
  - Co-simulation framework
  - Cybersecurity research focus
  - Evaluated attacks highlight potential vulnerabilities
- **Various applications for Wattson**

WATTSON



Evaluate intrusion detection systems	Analyze preventive countermeasures	Network forensics for energy networks
Attack evaluations	Awareness trainings	Dataset generation

● ● ●

https://github.com/fkie-cad/wattson

Thank you!

Lennart Bader
lennart.bader@fkie.fraunhofer.de

Comprehensively Analyzing the Impact of Cyberattacks on Power Grids

Lennart Bader Martin Serror Olav Lamberts

Ömer Sen Dennis van der Velde Immanuel Hacker

Julian Filter Elmar Padilla Martin Henze

https://github.com/fkie-cad/wattson

Fraunhofer FKIE SPICe RWTH AACHEN UNIVERSITY

lennart.bader@fkie.fraunhofer.de