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

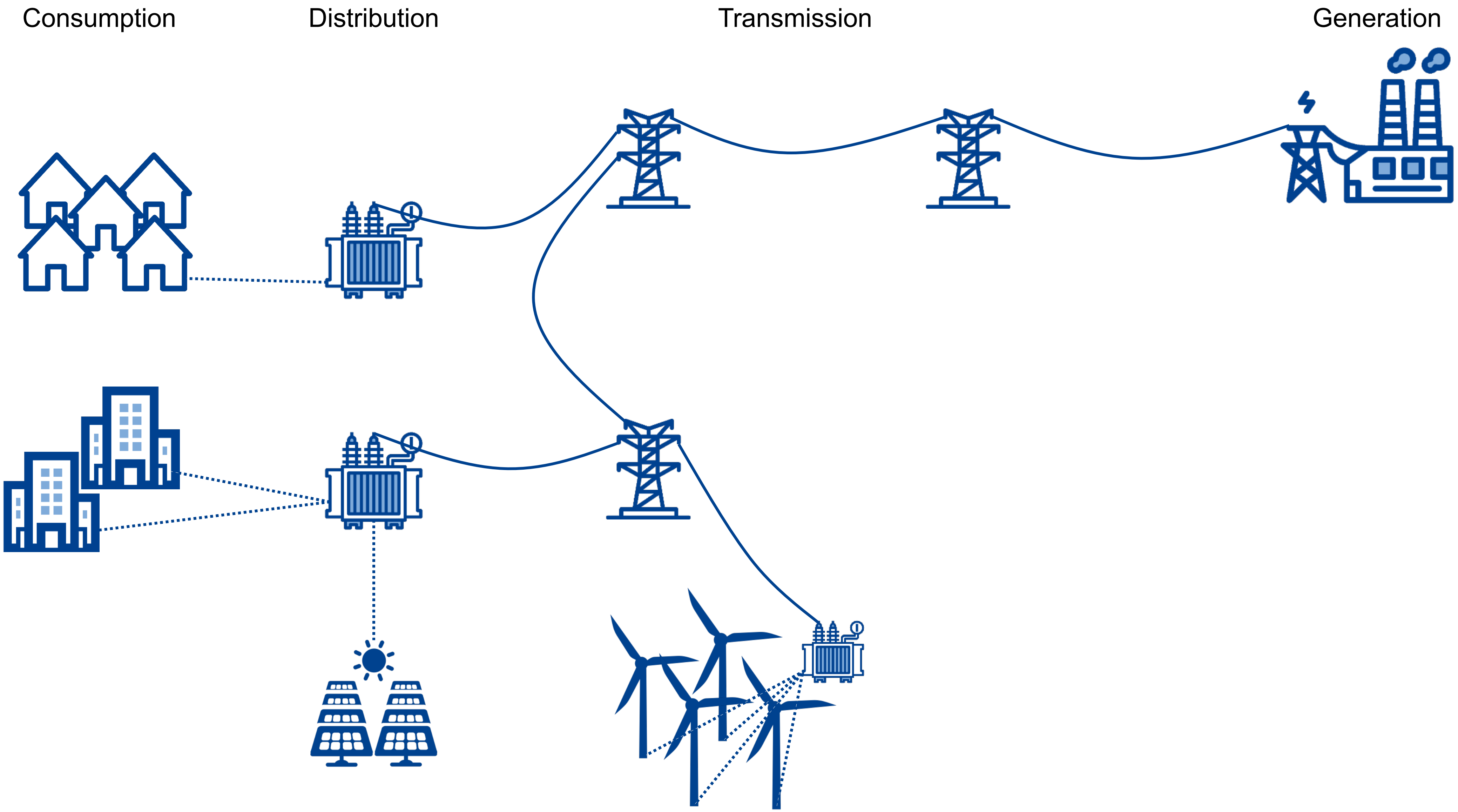
https://github.com/fkie-cad/wattson

Fraunhofer FKIE

SPICe RWTH AACHEN UNIVERSITY

lennart.bader@fkie.fraunhofer.de

Digitized Power Grids are Vulnerable



Consumption

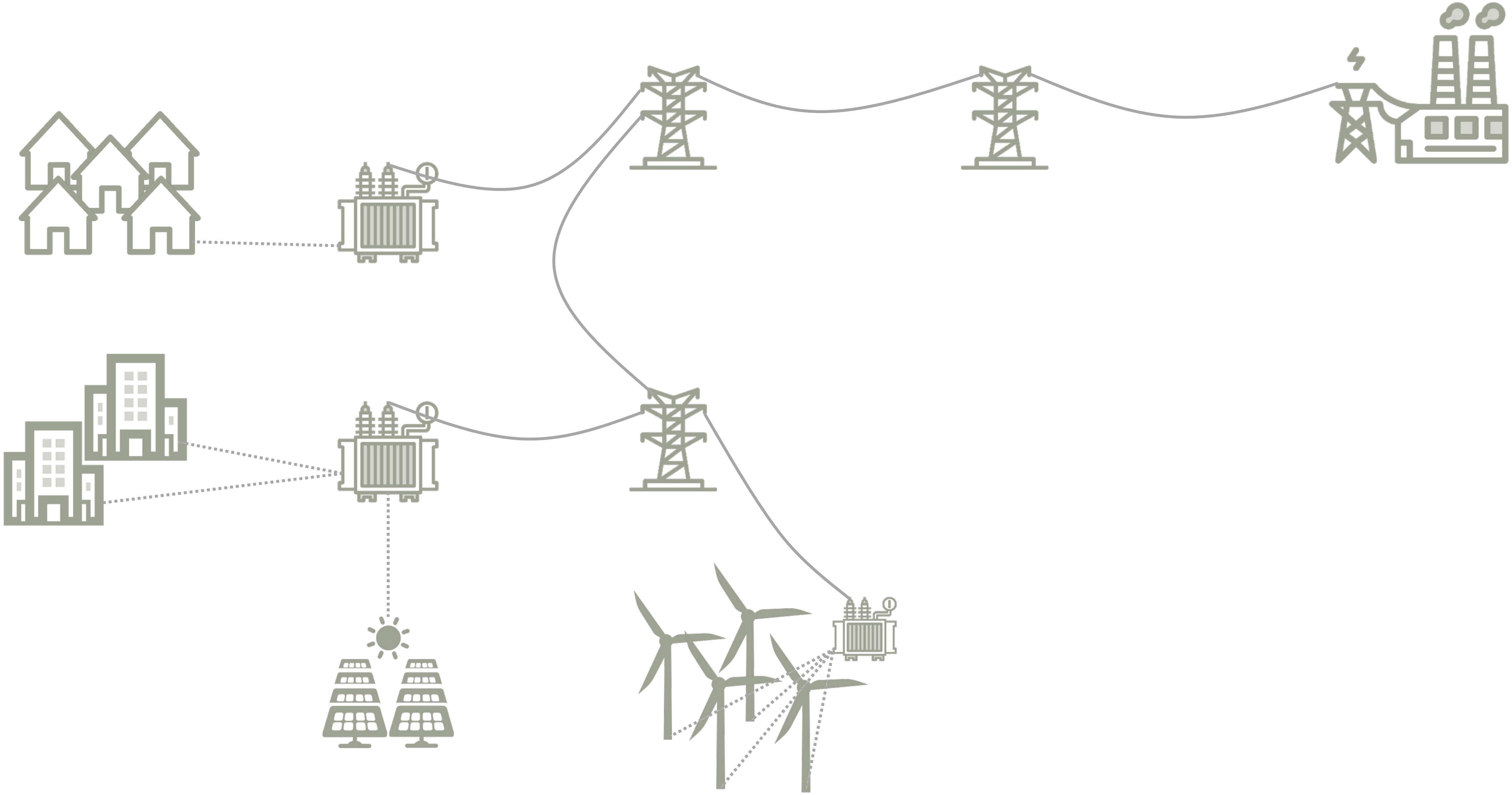
Distribution

Transmission

Generation

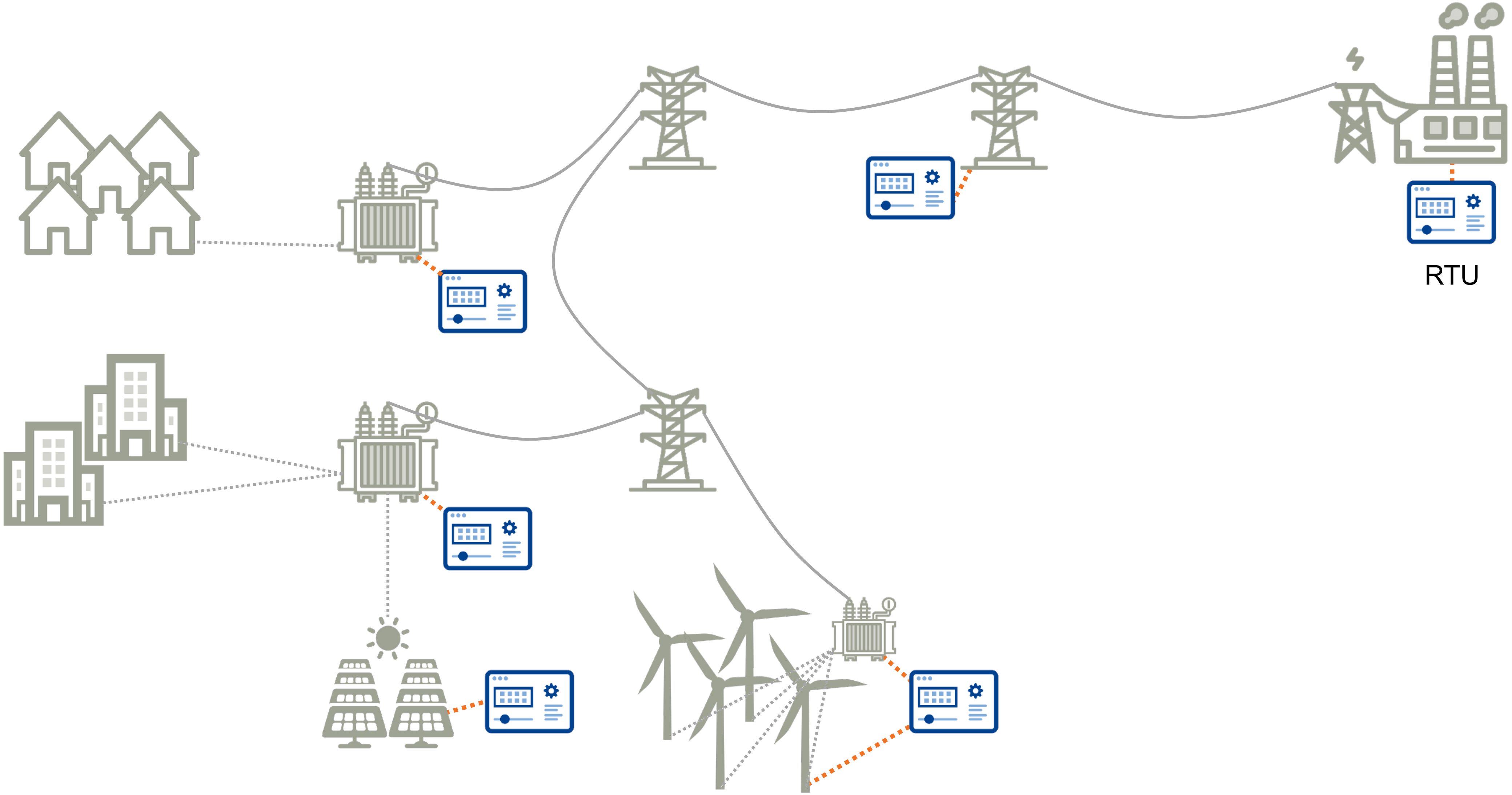
This graphic uses resources from flaticon.com

Digitized Power Grids are Vulnerable



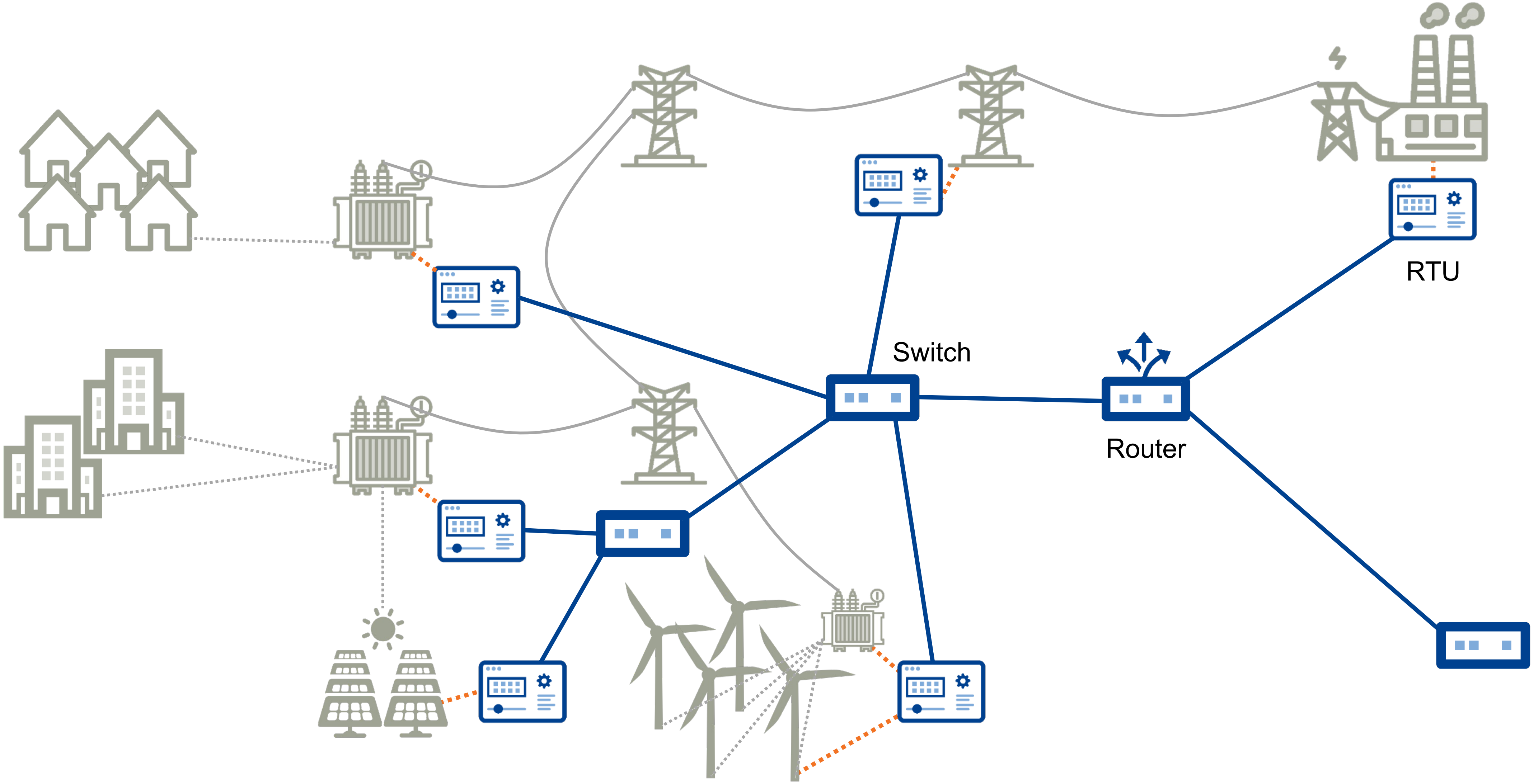
This graphic uses resources from flaticon.com

Digitized Power Grids are Vulnerable



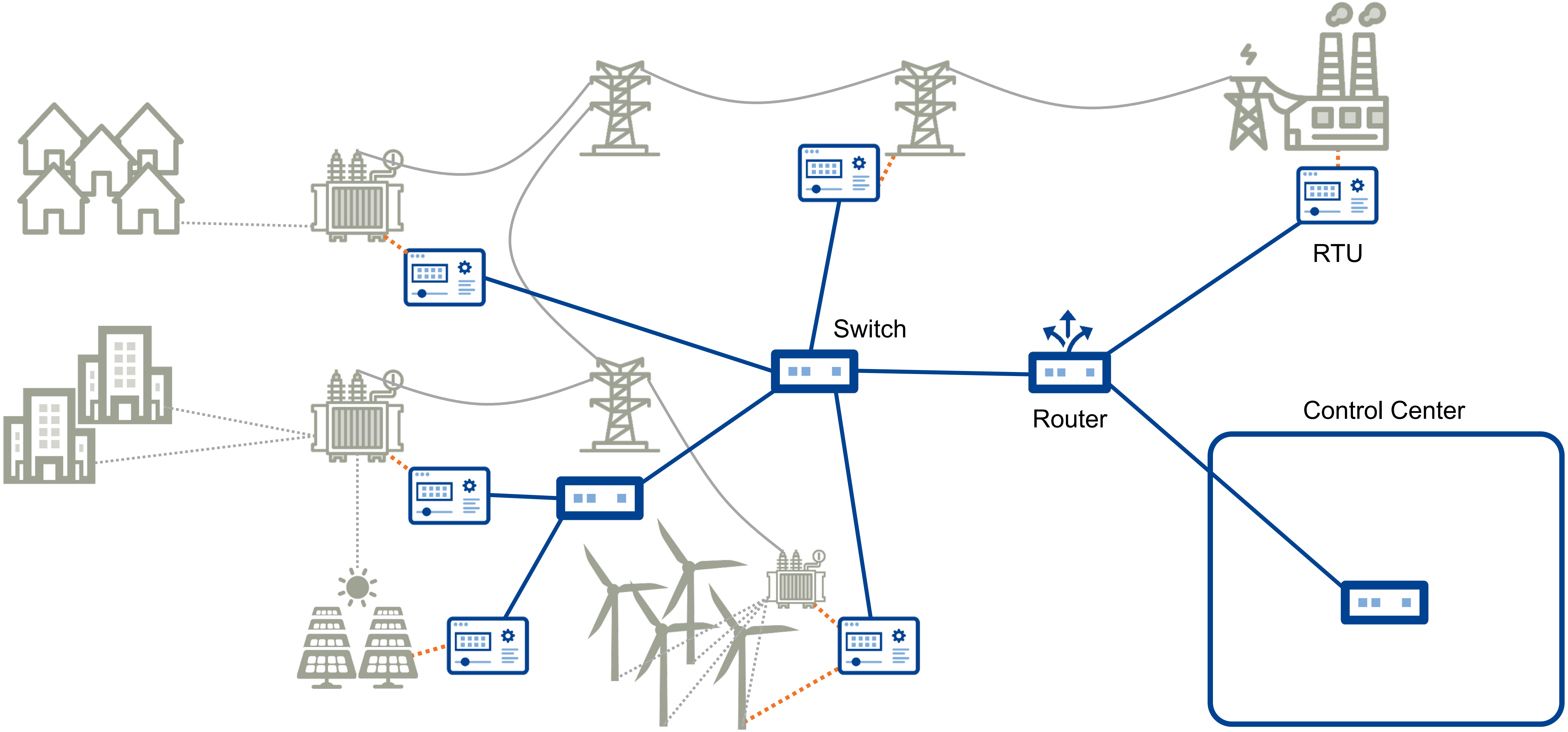
This graphic uses resources from flaticon.com

Digitized Power Grids are Vulnerable



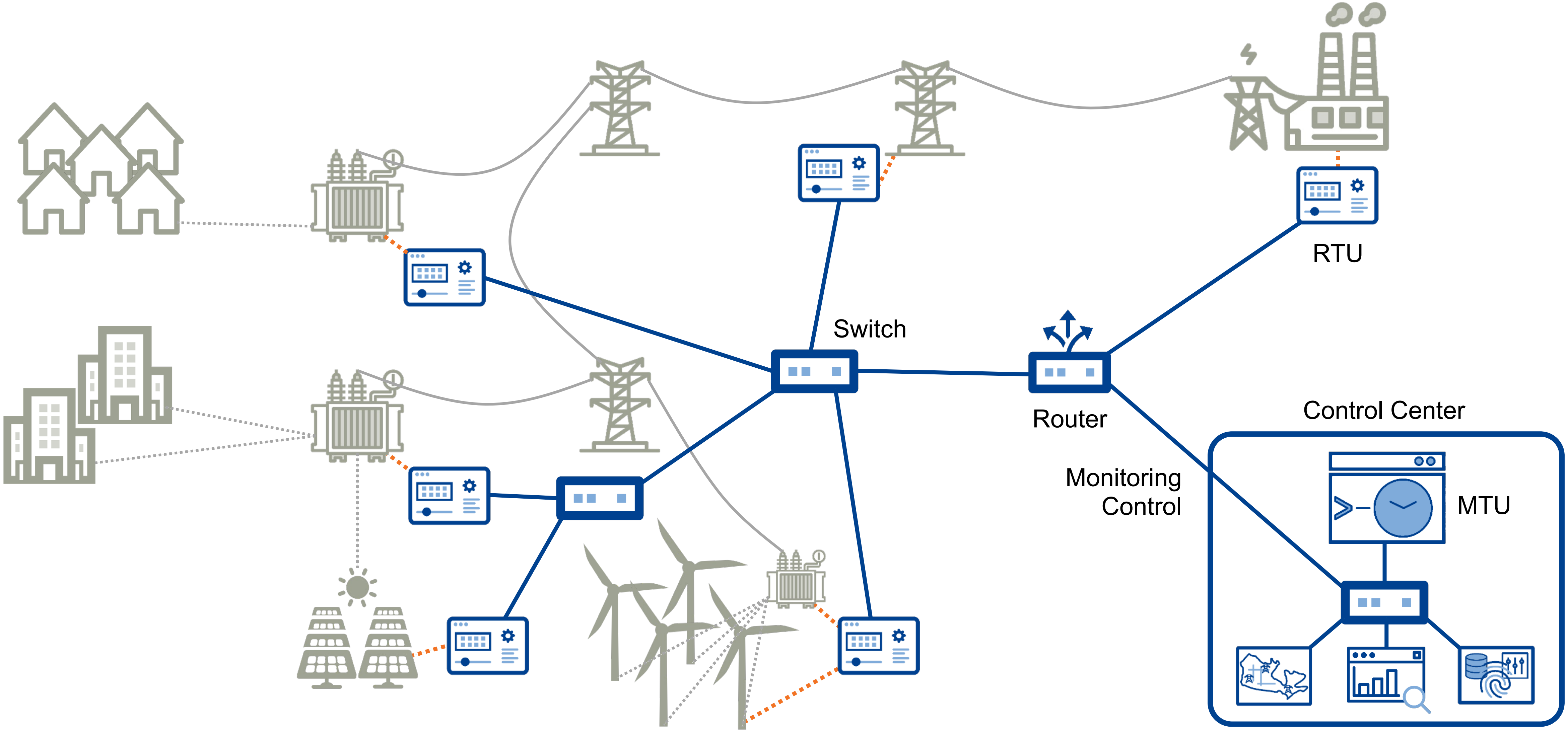
This graphic uses resources from flaticon.com

Digitized Power Grids are Vulnerable



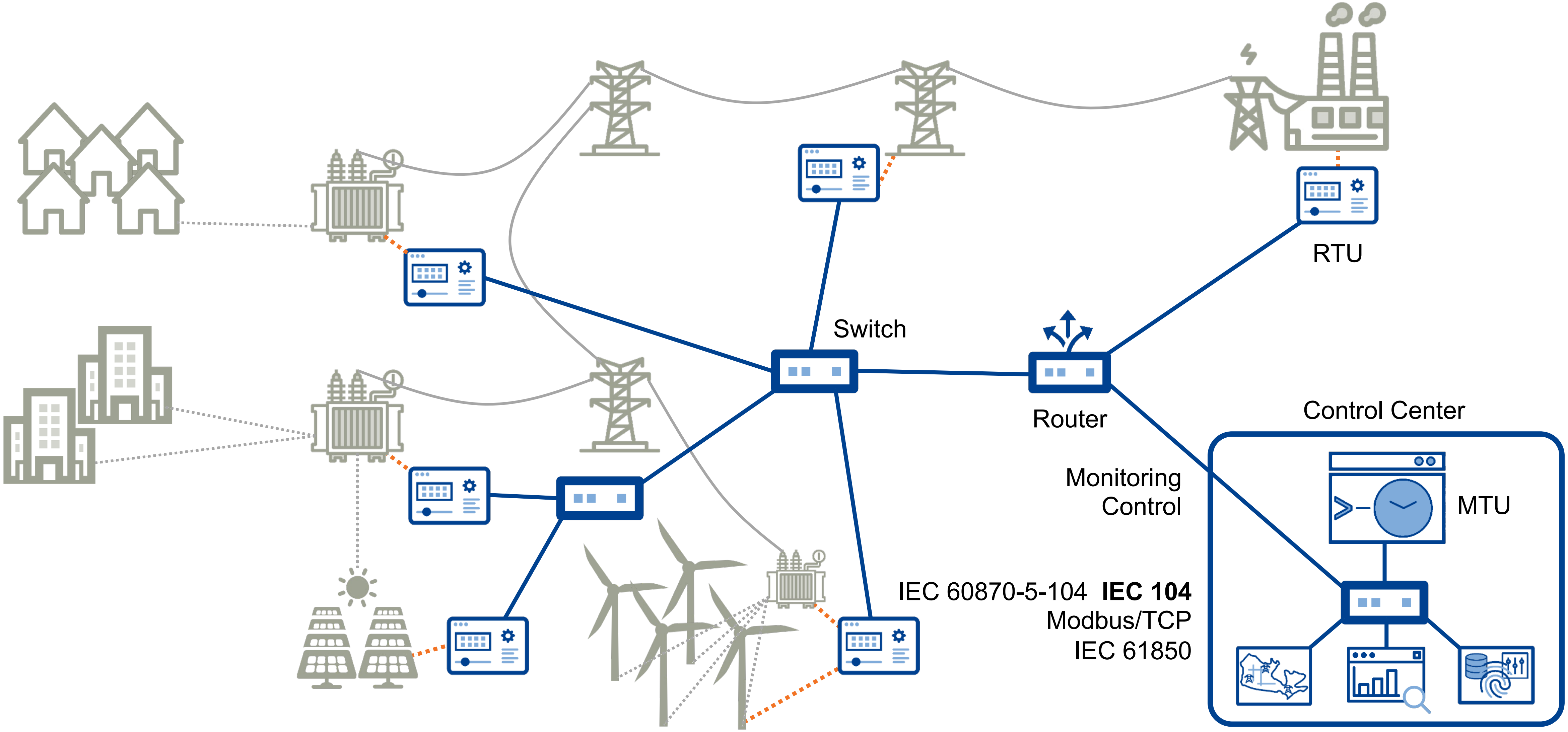
This graphic uses resources from flaticon.com

Digitized Power Grids are Vulnerable



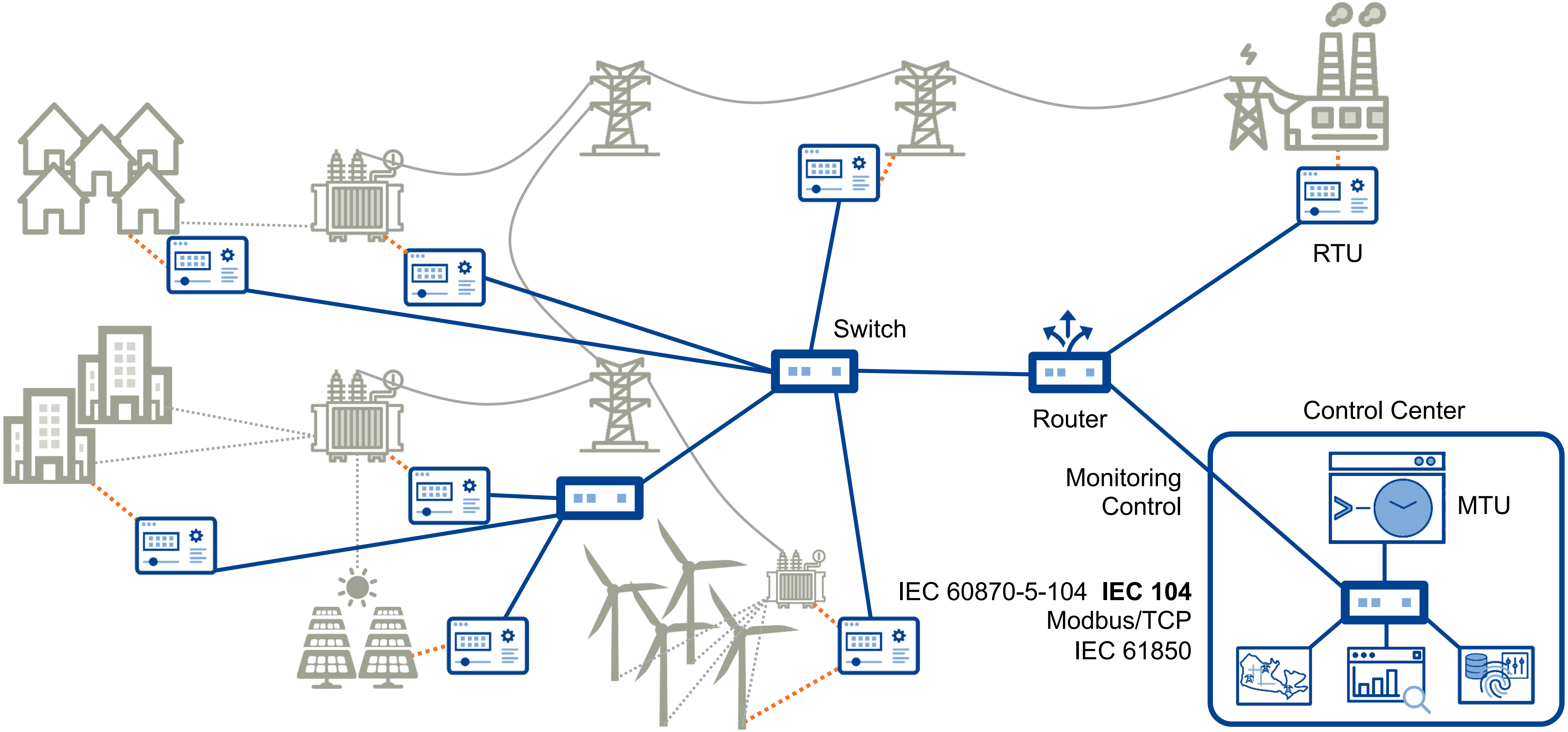
This graphic uses resources from flaticon.com

Digitized Power Grids are Vulnerable



This graphic uses resources from flaticon.com

Digitized Power Grids are Vulnerable



This graphic uses resources from flaticon.com

Vulnerabilities and Common Attacks

Compelling target

- Critical infrastructure
- Physical consequences

Vulnerabilities and Common Attacks

Compelling target

- Critical infrastructure
- Physical consequences

Physical access

- Unmanned facilities
- Geographic scale
- Multiple actors

Vulnerabilities and Common Attacks

Compelling target

- Critical infrastructure
- Physical consequences

Physical access

- Unmanned facilities
- Geographic scale
- Multiple actors

Limited security

- Encryption, authentication
- Network segmentation

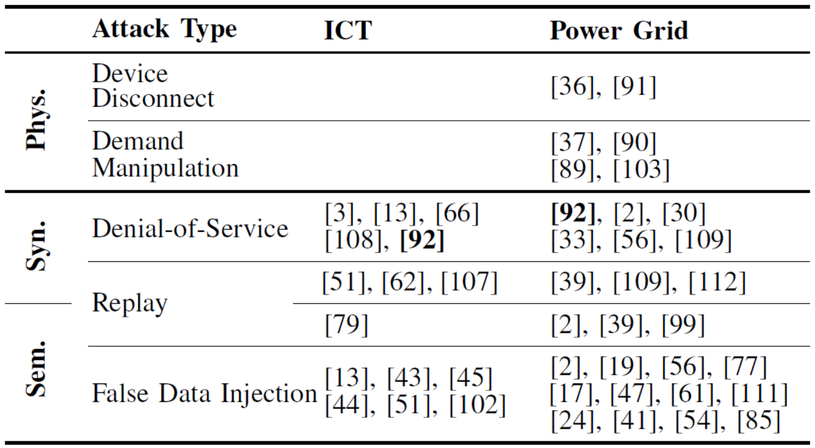
Vulnerabilities and Common Attacks

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



	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]

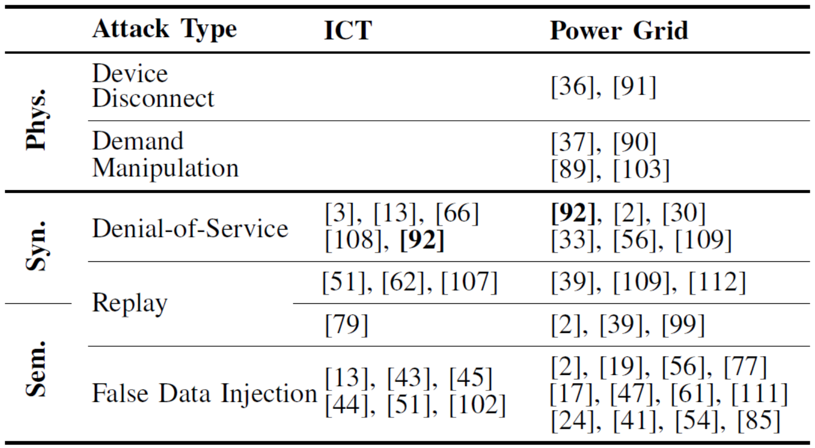
Vulnerabilities and Common Attacks

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]

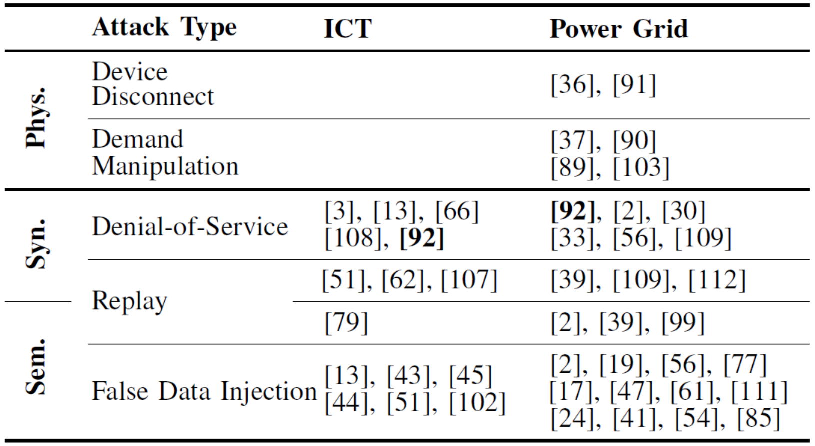
Vulnerabilities and Common Attacks

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

Methods for Realistic Cross-Domain Evaluations of Cyberattacks

The real power grid

+ Maximum realism

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

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

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

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

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**

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

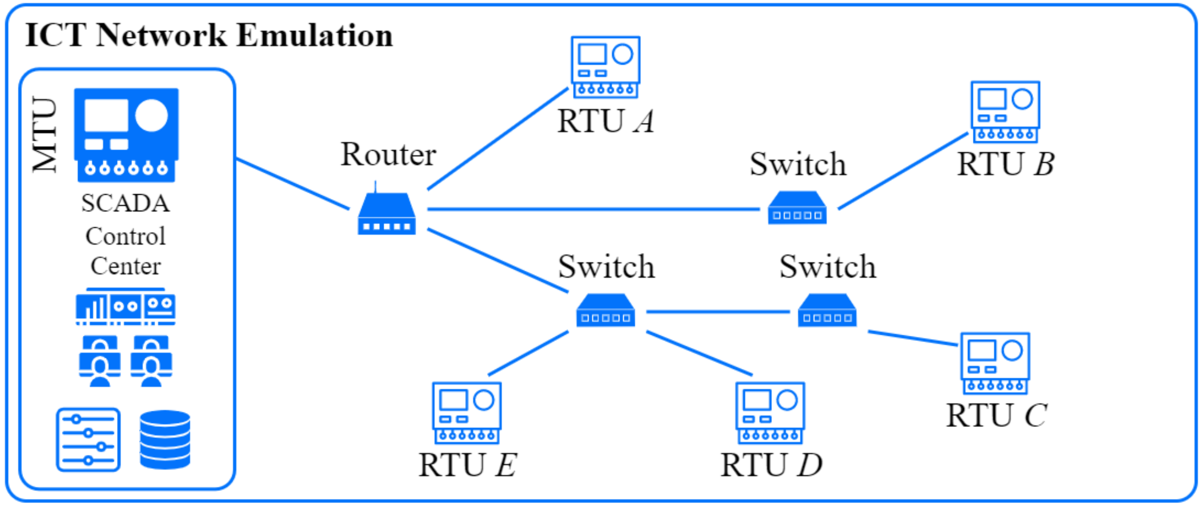
- Often specific focus / use case
  - No **real network traffic**
  - Insufficient **accuracy** (for one domain)
  - Limited **scalability**
- Usage of proprietary hard- or software
  - Limited **availability**

Our proposal

WATTSON

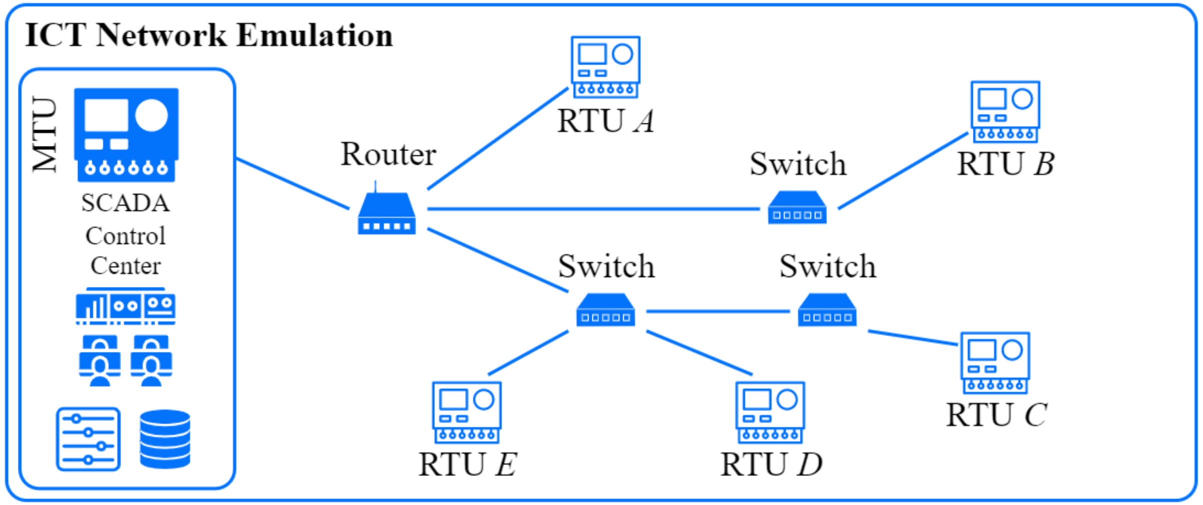
- Open source
- Co-simulation environment
- Cybersecurity focus

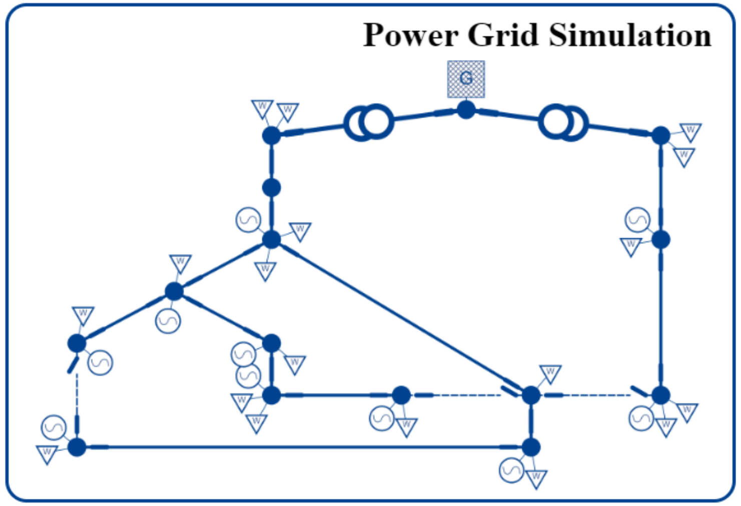
Wattson: A Cybersecurity Research Testbed for Power Grids



- **Network emulation** Containernet-based
  - Realistic network traffic down to Layer 2

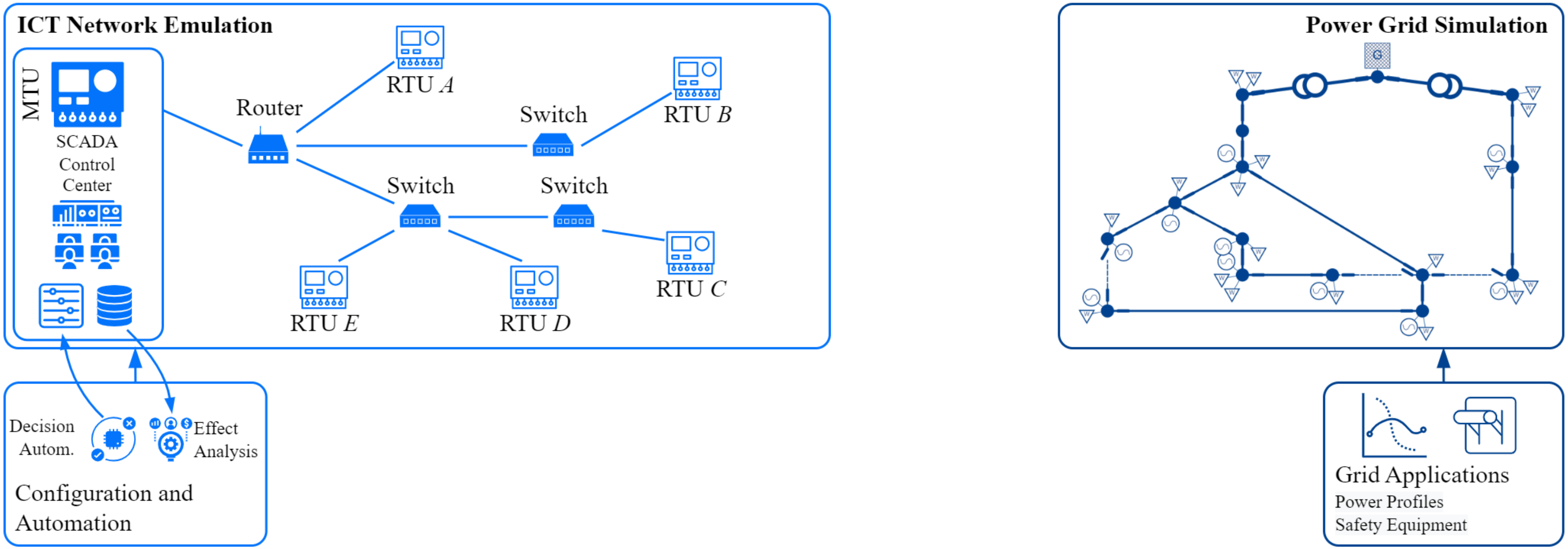
Wattson: A Cybersecurity Research Testbed for Power Grids





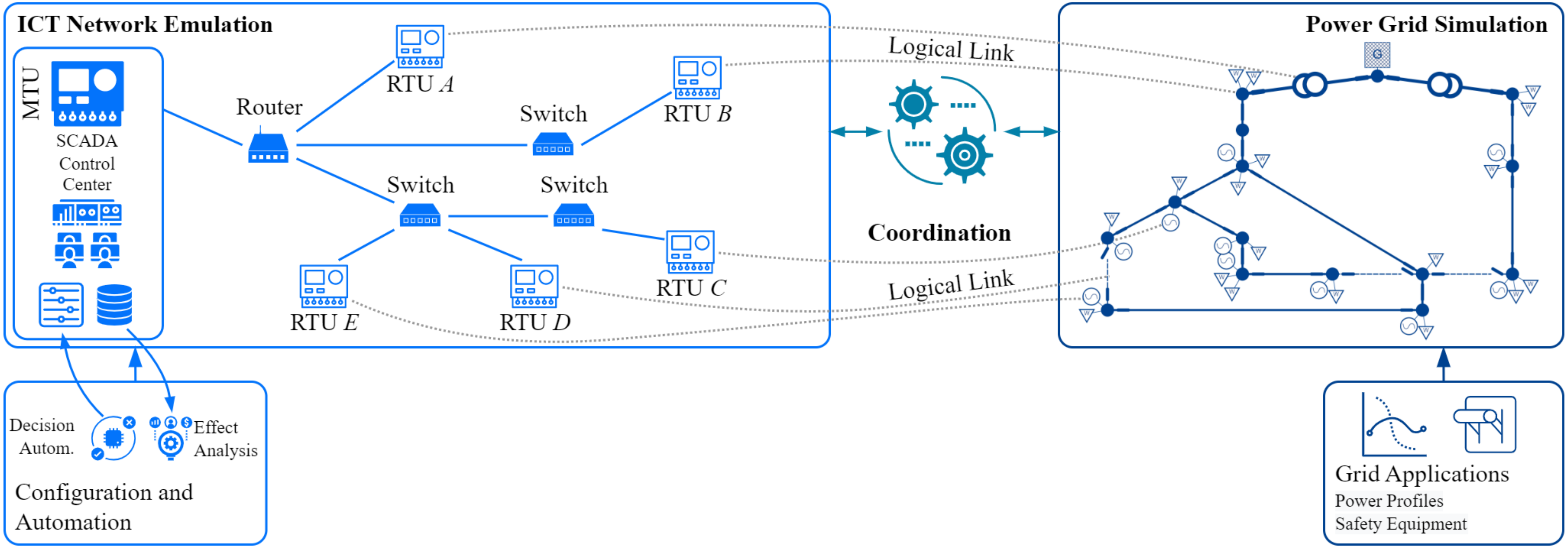
- **Network emulation** Containernet-based
  - Realistic network traffic down to Layer 2
- **Power grid simulation** Pandapower-based
  - Static on-demand power flow computation

Wattson: A Cybersecurity Research Testbed for Power Grids



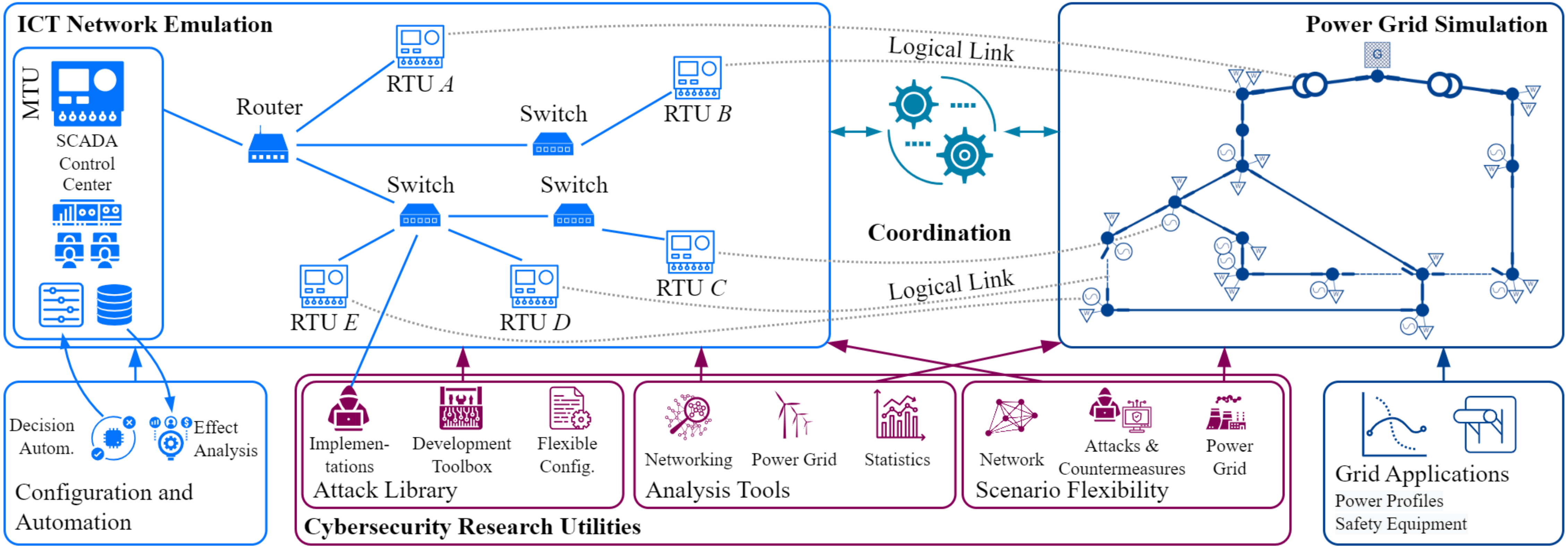
- **Network emulation** Containernet-based
  - ▶ Realistic network traffic down to Layer 2
- **Power grid simulation** Pandapower-based
  - ▶ Static on-demand power flow computation

Wattson: A Cybersecurity Research Testbed for Power Grids



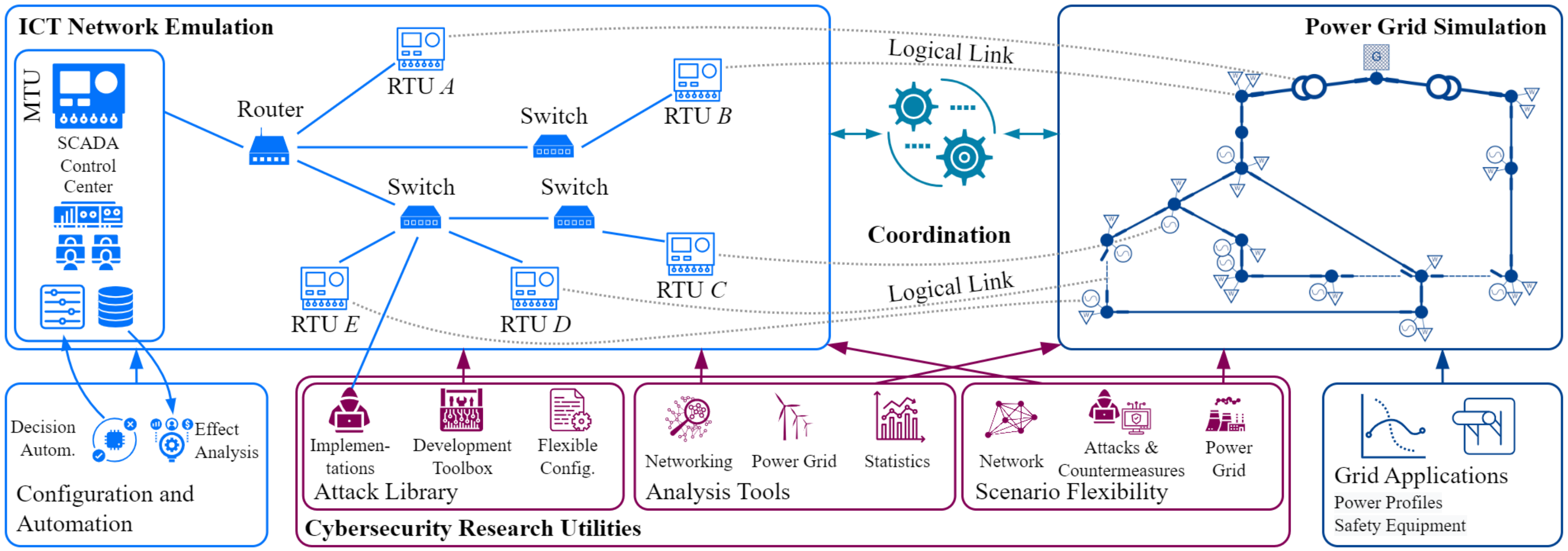
- **Network emulation** Containernet-based
  - ▶ Realistic network traffic down to Layer 2
- **Power grid simulation** Pandapower-based
  - ▶ Static on-demand power flow computation
- **Transparent coordination**
  - ▶ Interactions between ICT and grid components

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

Wattson: A Cybersecurity Research Testbed for Power Grids



ICT Network Emulation

MTU

SCADA Control Center

Router

Switch

Switch

Switch

RTU *A*

RTU *B*

RTU *C*

RTU *D*

RTU *E*

Logical Link

Coordination

Logical Link

Power Grid Simulation

Decision Autom.

Effect Analysis

Configuration and Automation

Implementations

Development Toolbox

Flexible Config.

Attack Library

Networking

Power Grid

Statistics

Analysis Tools

Network

Attacks & Countermeasures

Power Grid

Scenario Flexibility

Cybersecurity Research Utilities

Grid Applications

Power Profiles

Safety Equipment

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

Wattson is Accurate and Scalable

Validation against laboratory grid at RWTH Aachen Univ.

Fraunhofer
RWTH AACHEN UNIVERSITY
Fraunhofer-Zentrum Digitale Energie
Interdisziplinäre Exzellenz aus dem Rheinischen Revier zur Digitalisierung kritischer Energieversorgungsinfrastrukturen

© Martin Braun

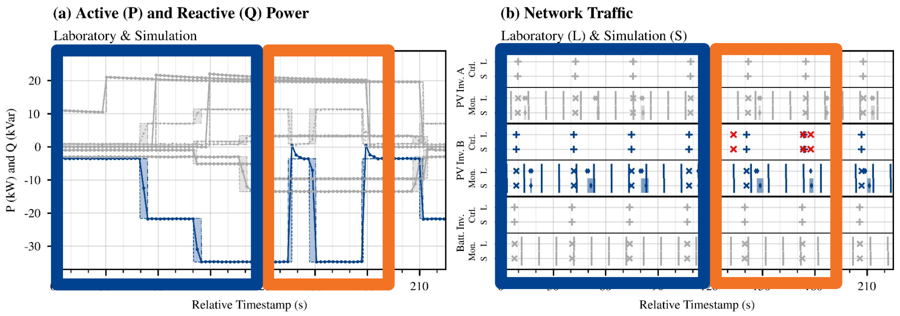
Wattson is Accurate and Scalable

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

© Martin Braun

Wattson is Accurate and Scalable

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

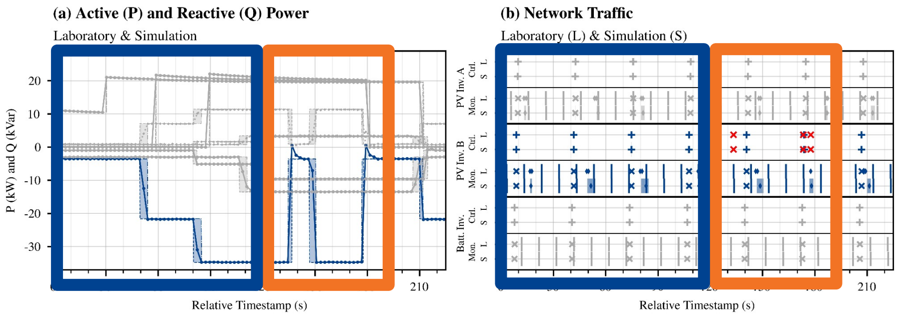


Accurately matching behavior under normal and attack conditions

© Martin Braun

Wattson is Accurate and Scalable

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



(a) Active (P) and Reactive (Q) Power

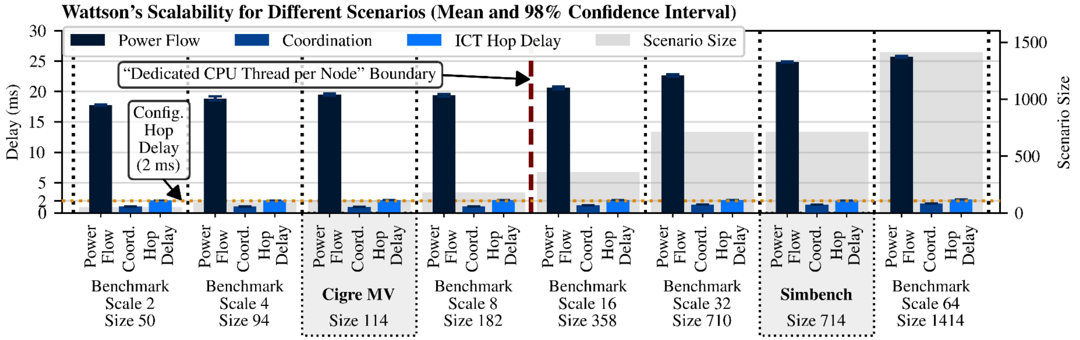
(b) Network Traffic

© 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



Wattson’s Scalability for Different Scenarios (Mean and 98% Confidence Interval)

Evaluating Cyberattacks against Power Grids with Wattson

Destruction of equipment

Interference with network traffic

Manipulation of application layer traffic

Evaluating Cyberattacks against Power Grids with Wattson

Destruction of equipment

0101
0011

Interference with network traffic

Manipulation of application layer traffic

Physical Attack

- Destruction of substation
  - Power grid assets
  - ICT equipment

Evaluating Cyberattacks against Power Grids with Wattson

Destruction of equipment

Physical Attack

- Destruction of substation
  - Power grid assets
  - ICT equipment

Interference with network traffic

Flooding

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

ARP Spoofing

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

Manipulation of application layer traffic

Evaluating Cyberattacks against Power Grids with Wattson

Destruction of equipment

Physical Attack

- Destruction of substation
  - Power grid assets
  - ICT equipment

0101 0011 Interference with network traffic

Flooding

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

ARP Spoofing

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

Manipulation of application layer traffic

Industroyer

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

False Data Injection

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

Evaluating Cyberattacks against Power Grids with Wattson

Destruction of equipment

Physical Attack

- Destruction of substation
  - Power grid assets
  - ICT equipment

Interference with network traffic

Flooding

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

ARP Spoofing

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

Manipulation of application layer traffic

Industroyer

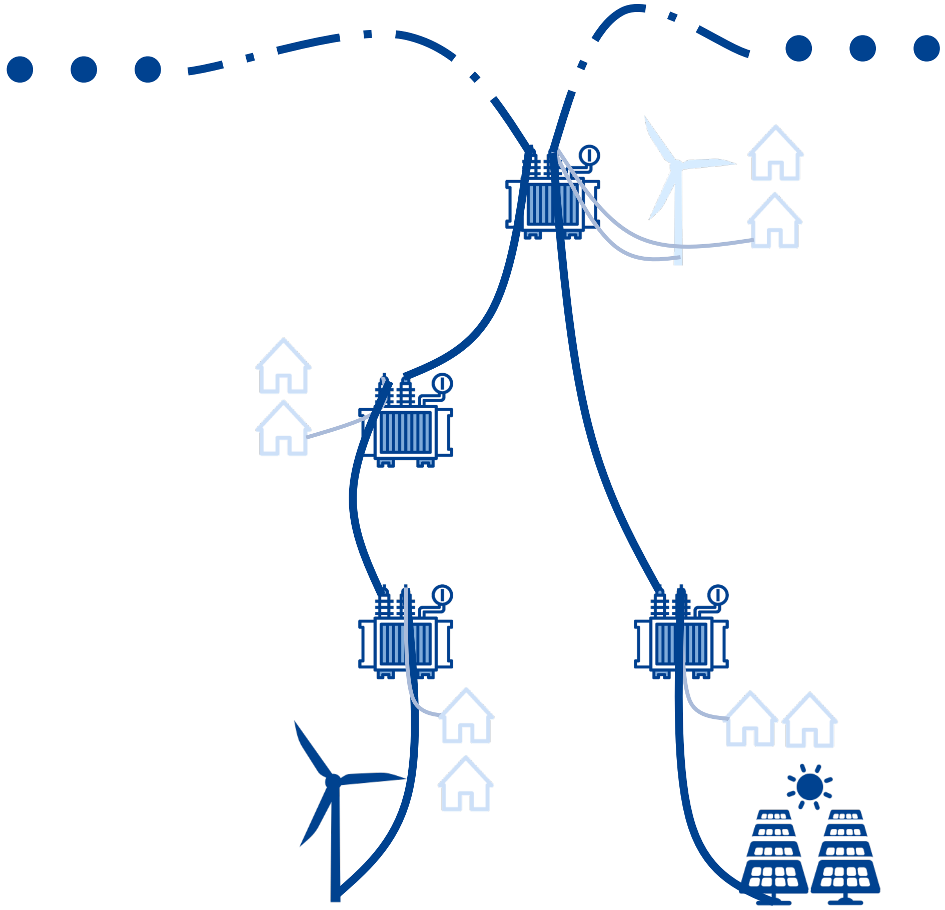
- Secondary IEC 104 client
- Issues control commands
- Disconnects large parts of the power grid

False Data Injection

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

Lennart Bader
lennart.bader@fkie.fraunhofer.de

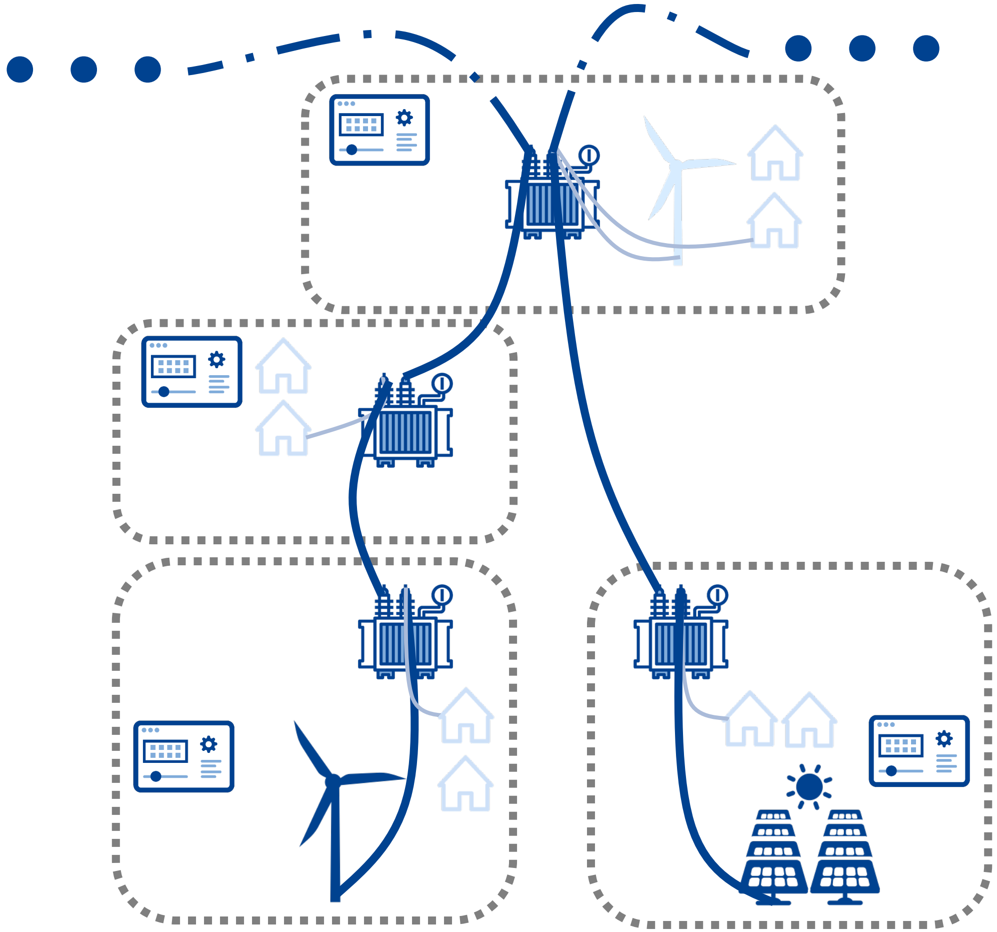
False Data Injection Attack: Scenario



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

This graphic uses resources from flaticon.com

False Data Injection Attack: Scenario

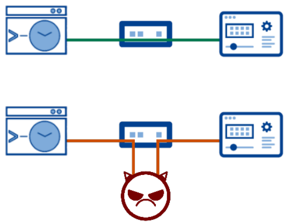


Simbench semi-urban medium-voltage scenario
~ 110 substations, 119 RTUs
Represents a district

This graphic uses resources from flaticon.com

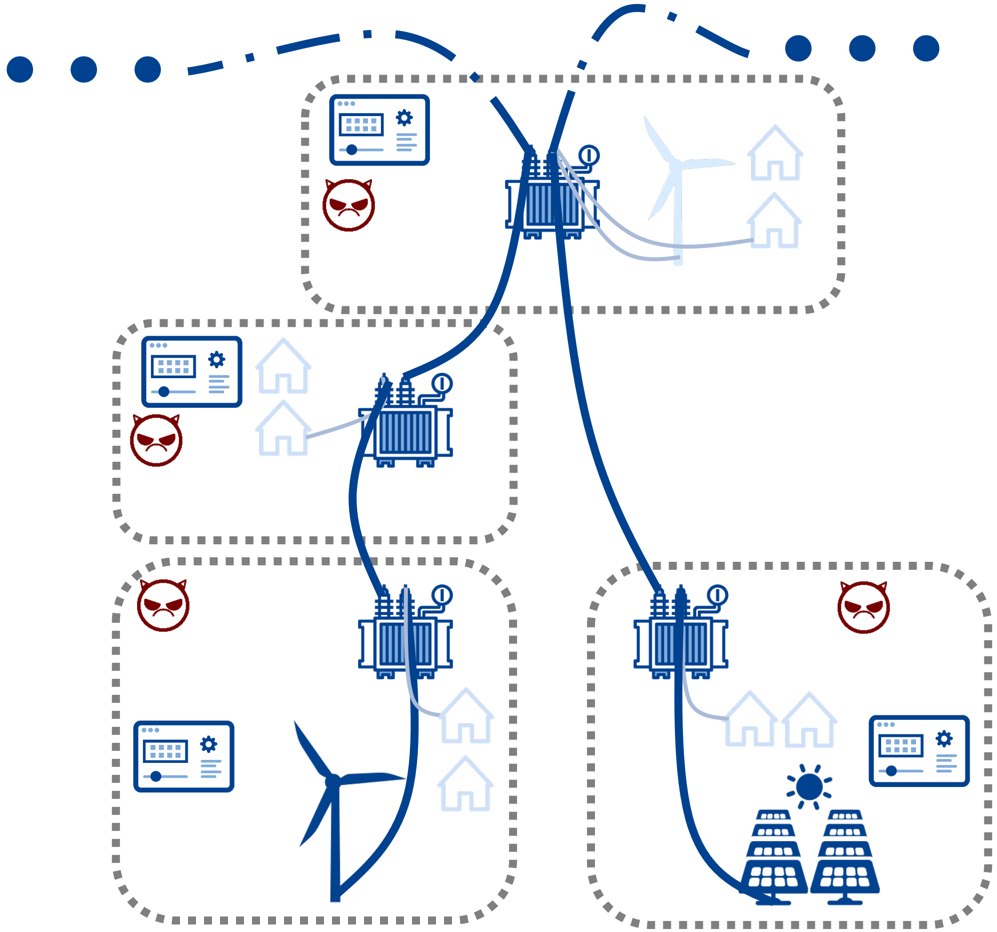
Lennart Bader
lennart.bader@fkie.fraunhofer.de

False Data Injection Attack: Scenario



Attack Phases

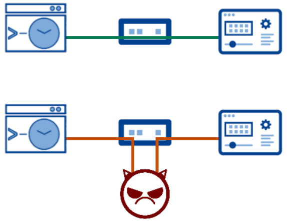
- MitM via ARP spoof
  - Learn SEQ/ACK (TCP) and SSN/RSN (IEC 104)



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

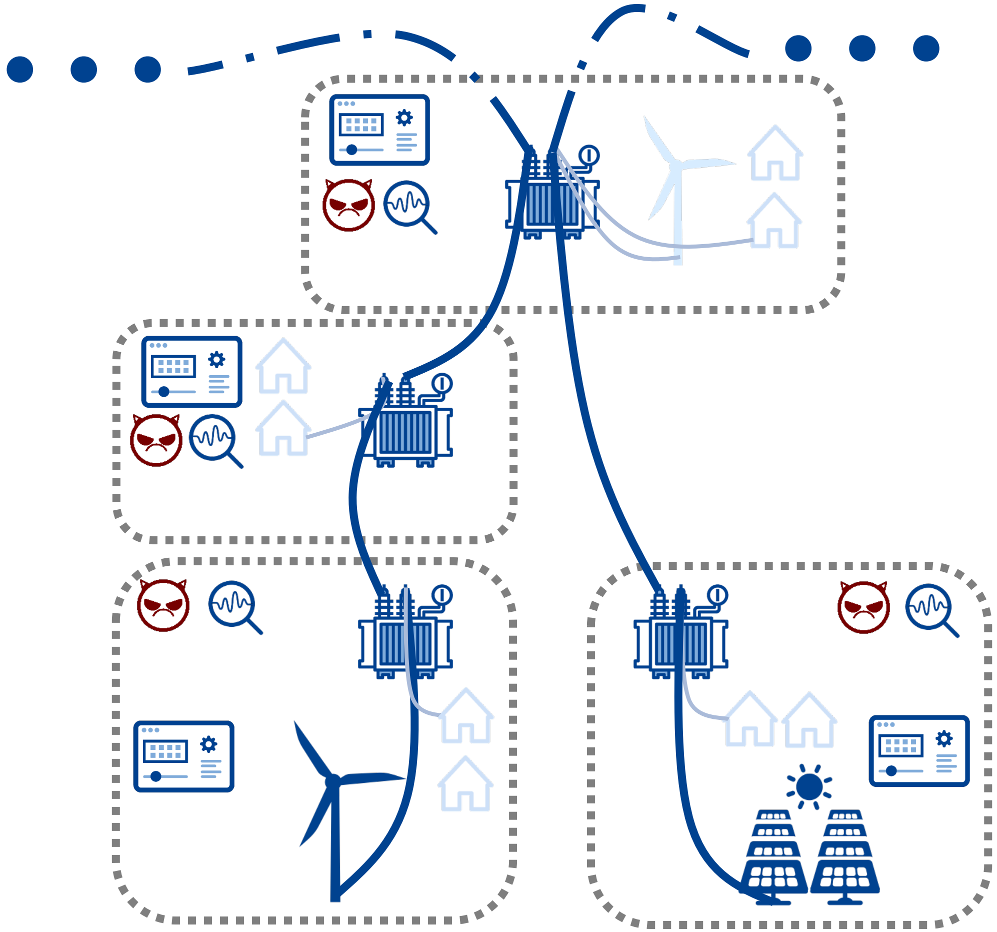
False Data Injection Attack: Scenario

Attack Phases



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

- Eavesdropping & recording
  - Learn measurement values & store history

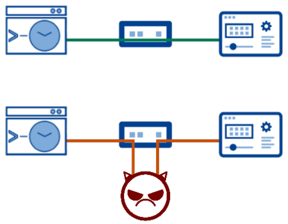


Simbench semi-urban medium-voltage scenario
~ 110 substations, 119 RTUs
Represents a district

This graphic uses resources from flaticon.com

Lennart Bader
lennart.bader@fkie.fraunhofer.de

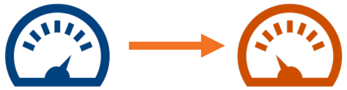
False Data Injection Attack: Scenario



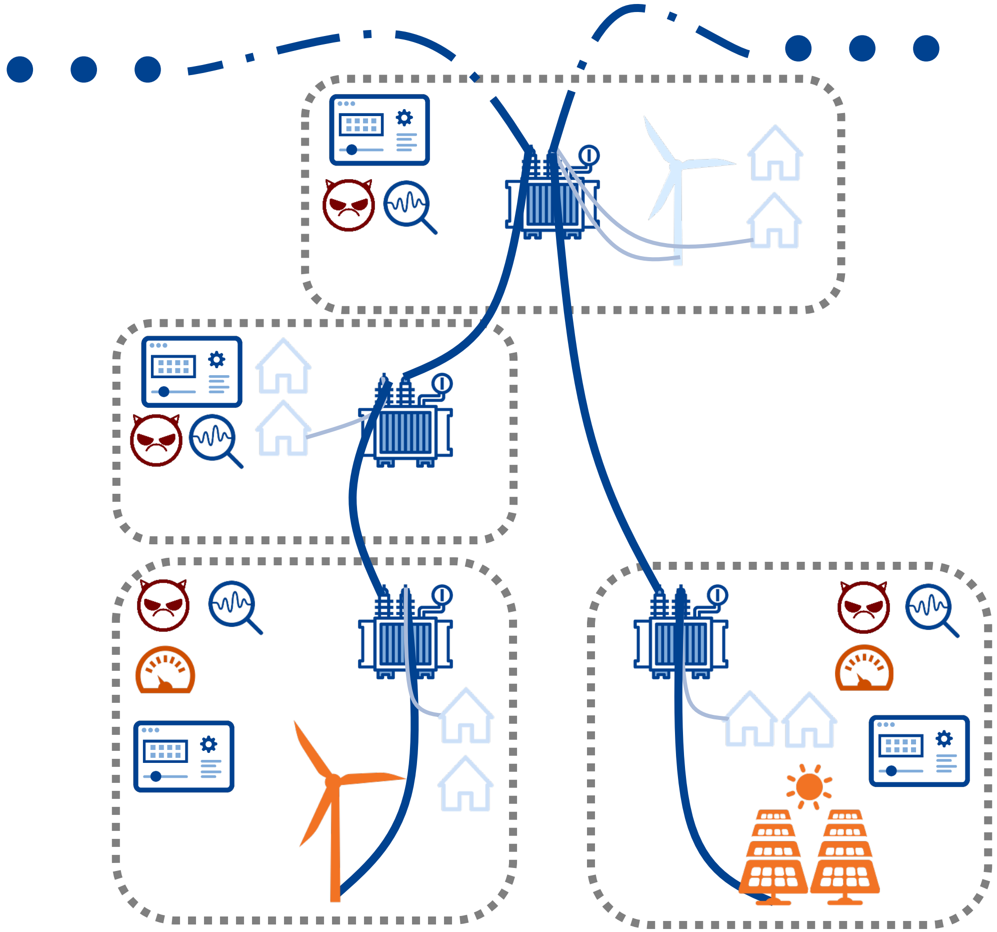
Attack Phases

- 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

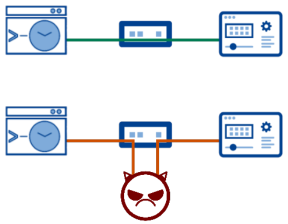


Simbench semi-urban medium-voltage scenario
~ 110 substations, 119 RTUs
Represents a district

This graphic uses resources from flaticon.com

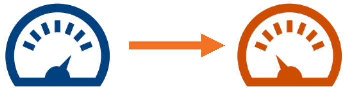
False Data Injection Attack: Scenario

Attack Phases

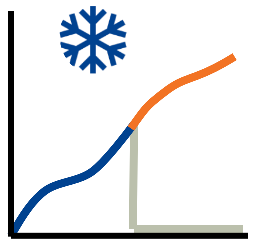


- MitM via ARP spoof
  - Learn SEQ/ACK (TCP) and SSN/RSN (IEC 104)

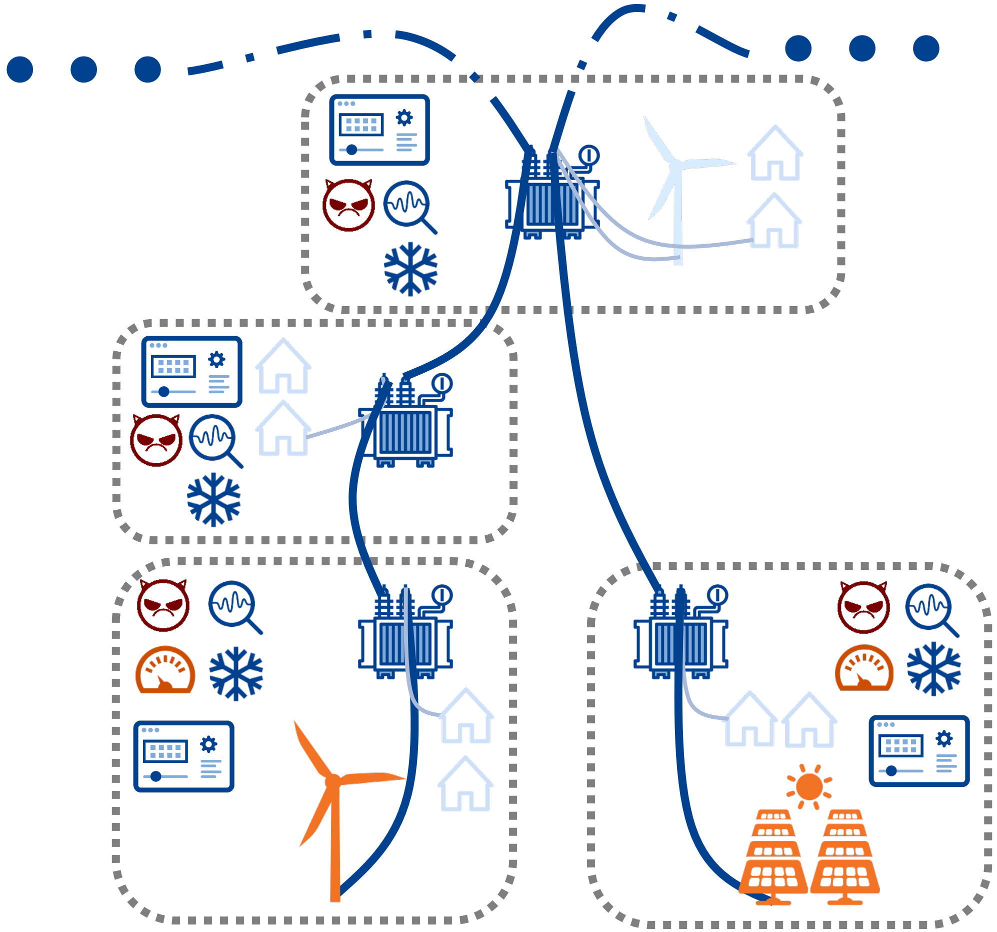
- Eavesdropping & recording
  - Learn measurement values & store history



- Command Injection
  - Inject control commands into active connection



- Freezing
  - Manipulate measurements to represent former grid state

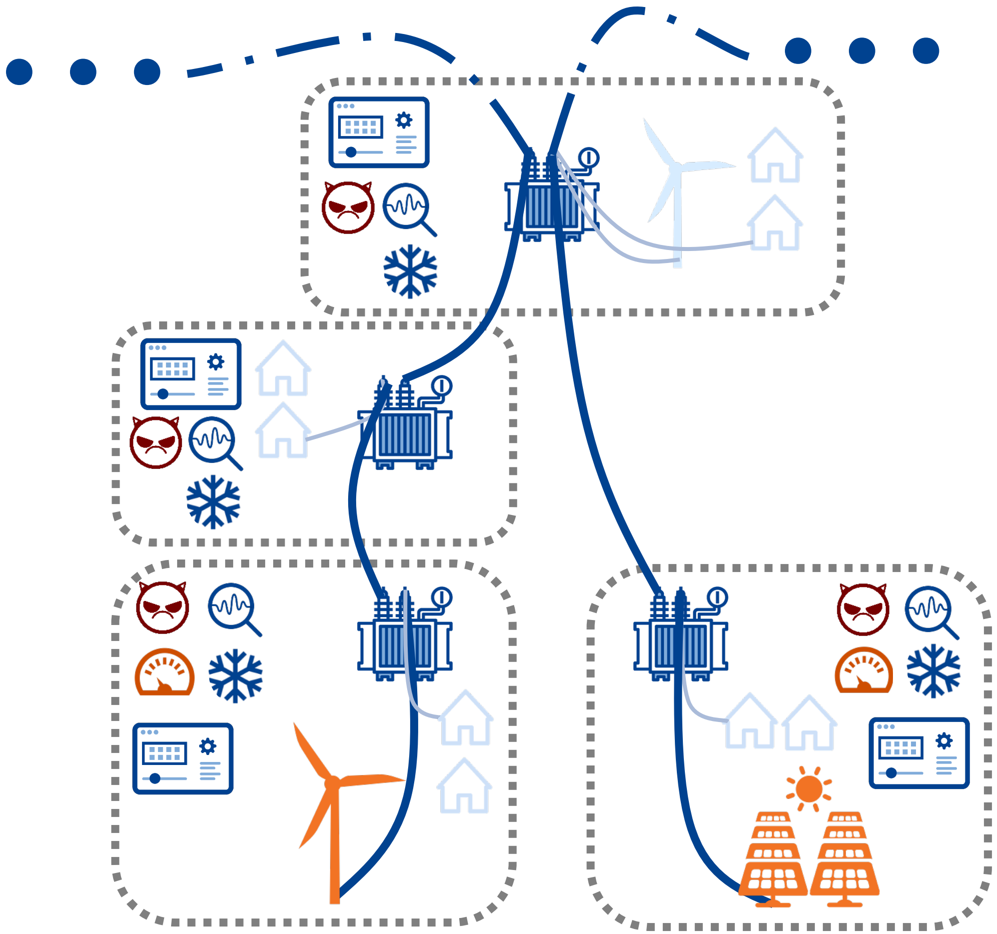


Simbench semi-urban medium-voltage scenario
~ 110 substations, 119 RTUs
Represents a district

This graphic uses resources from flaticon.com

Lennart Bader
lennart.bader@fkie.fraunhofer.de

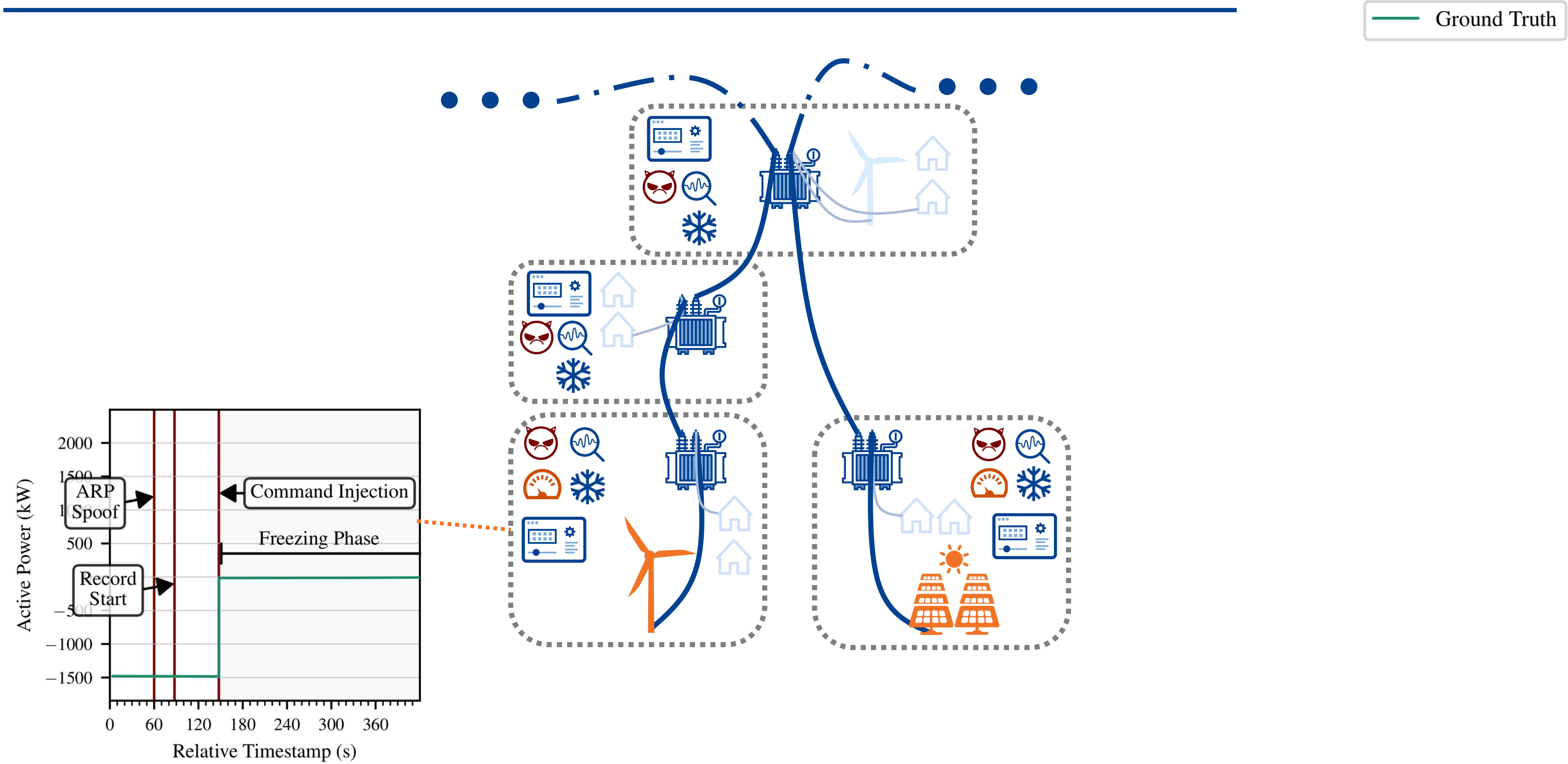
False Data Injection Attack: Evaluation



This graphic uses resources from flaticon.com

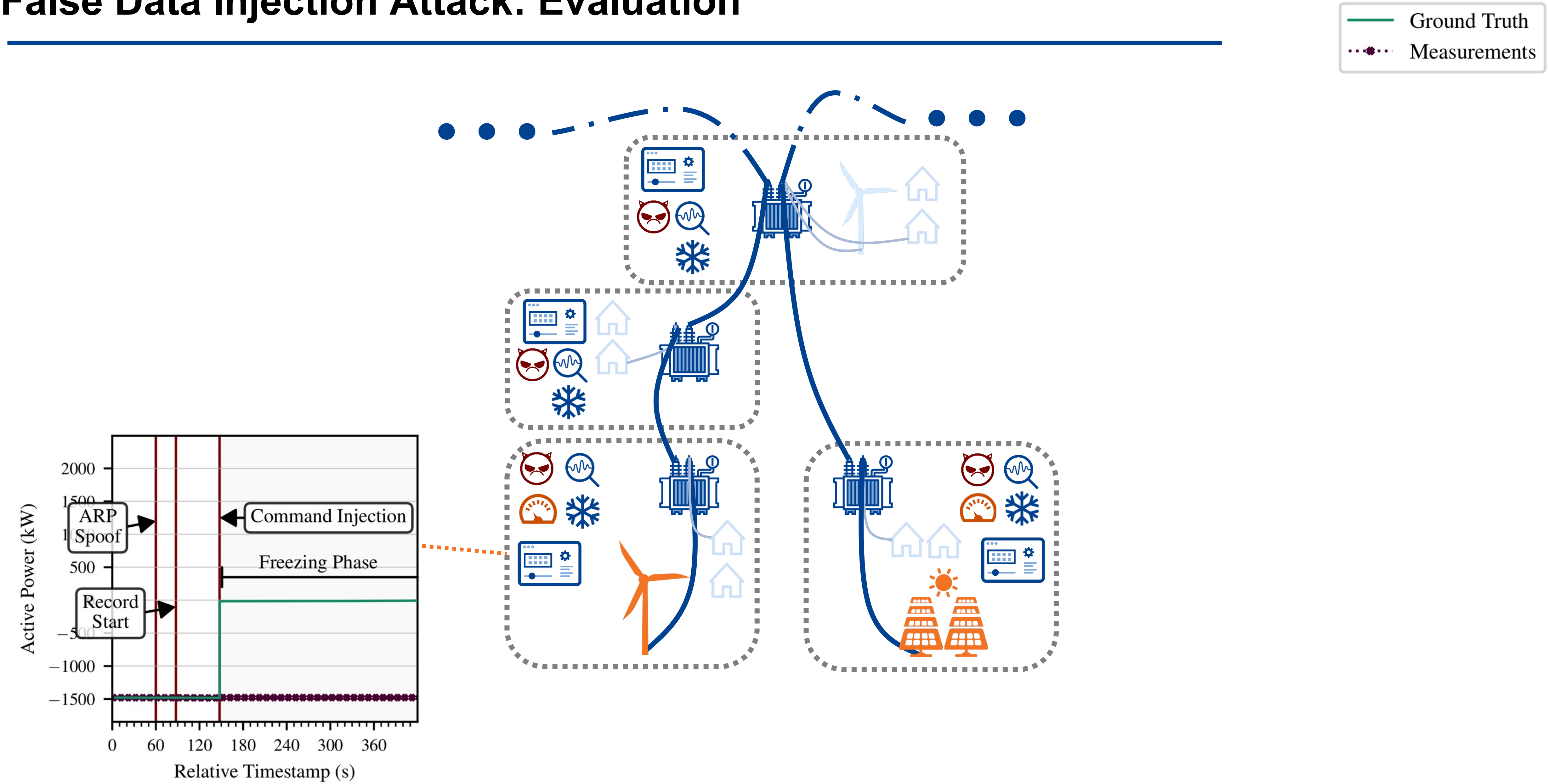
Lennart Bader
lennart.bader@fkie.fraunhofer.de

False Data Injection Attack: Evaluation



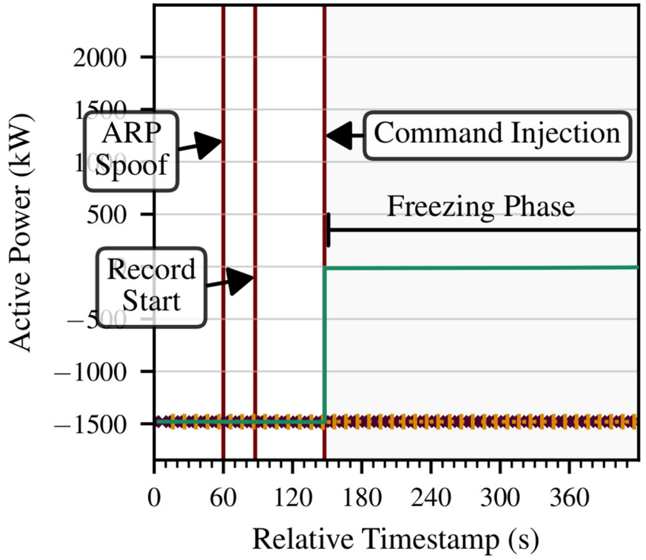
This graphic uses resources from flaticon.com

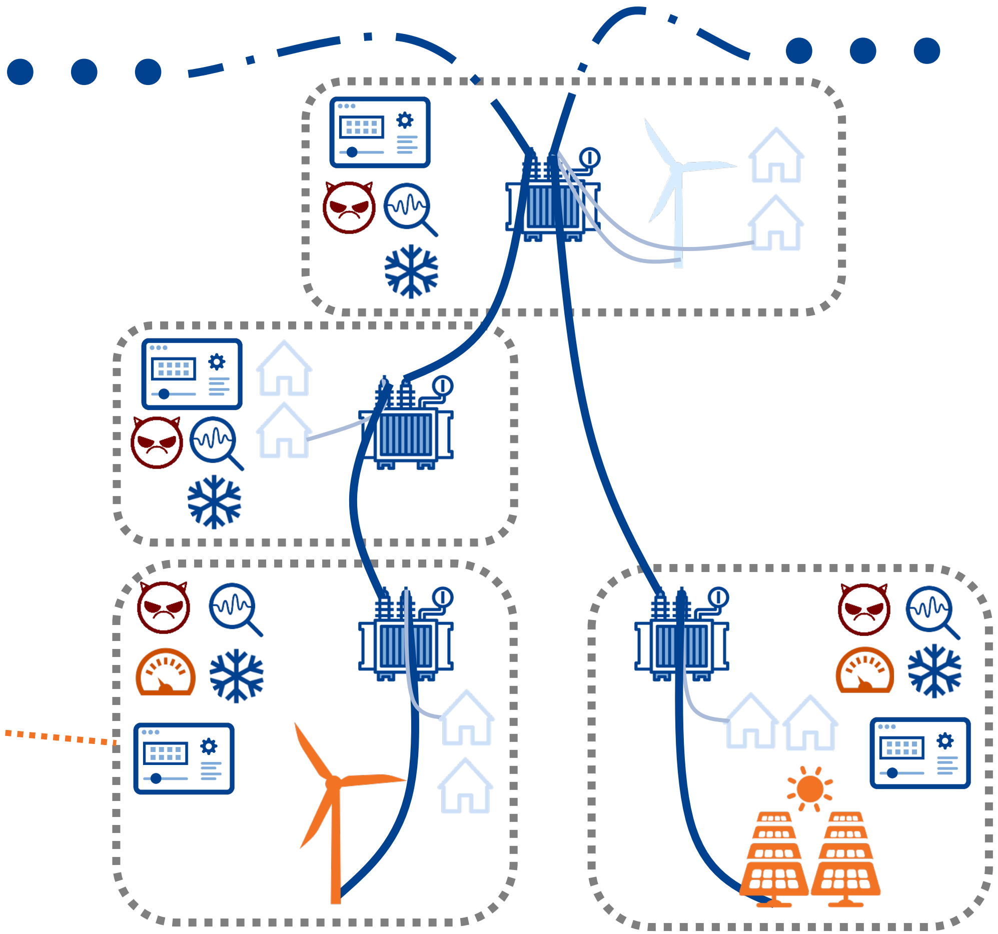
False Data Injection Attack: Evaluation



This graphic uses resources from flaticon.com

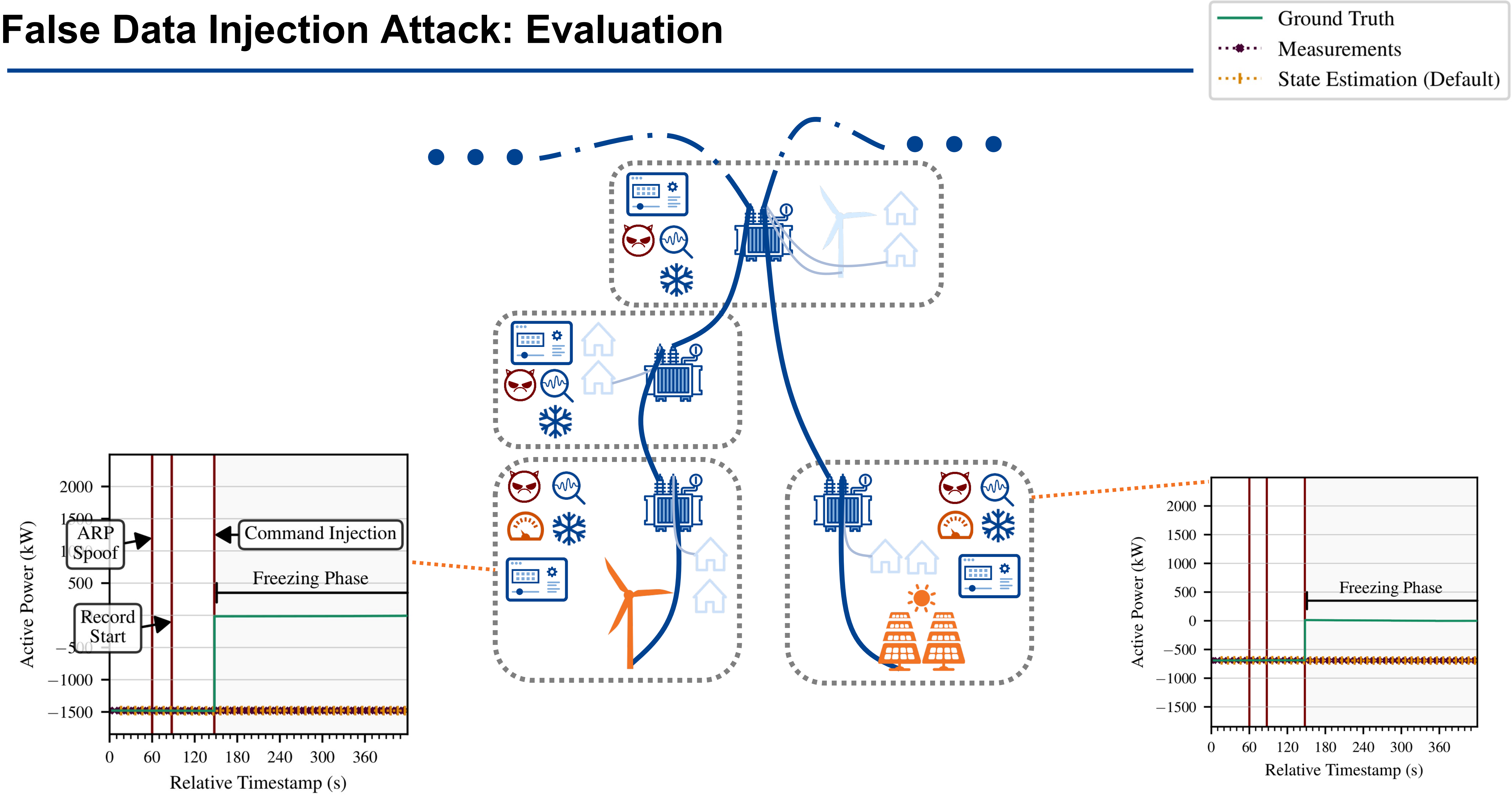
False Data Injection Attack: Evaluation





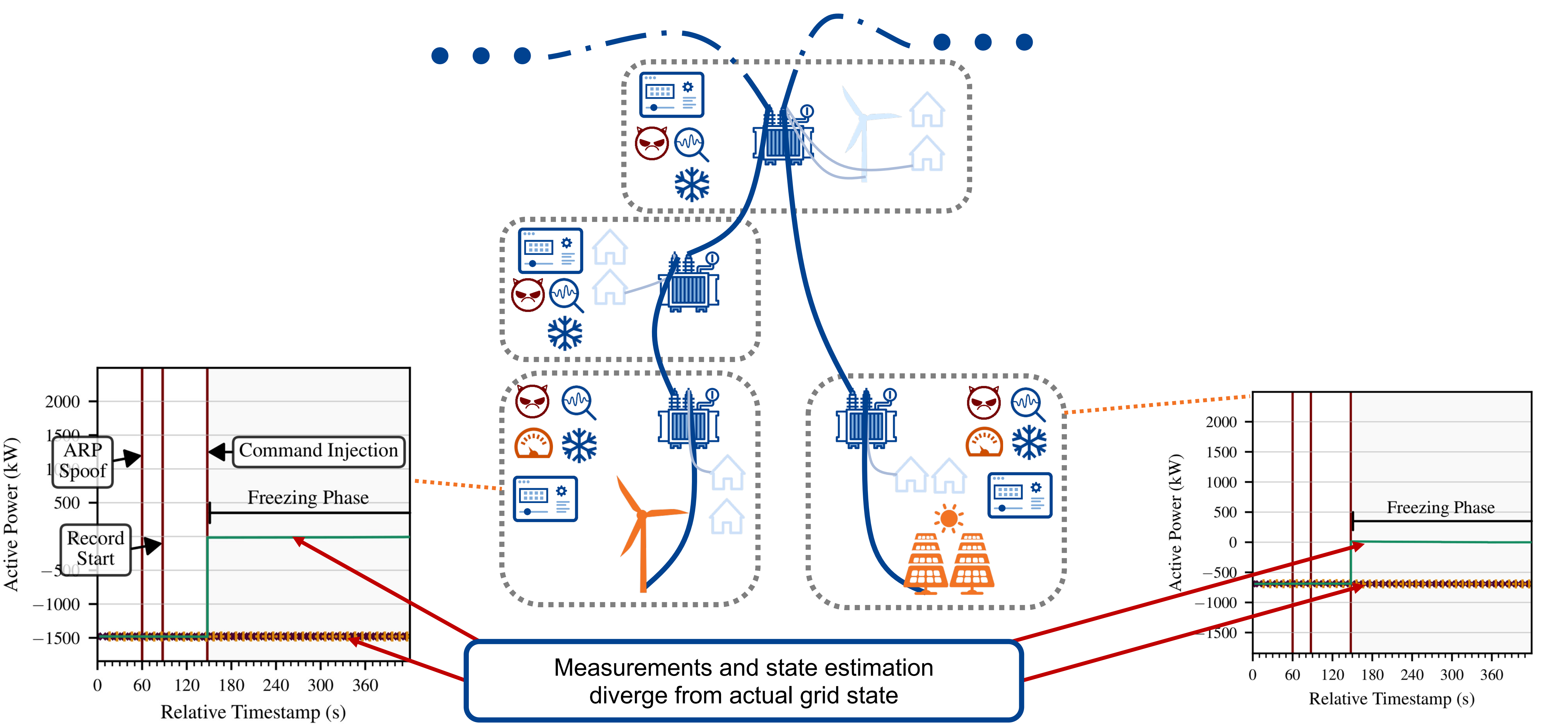
This graphic uses resources from flaticon.com

False Data Injection Attack: Evaluation



This graphic uses resources from flaticon.com

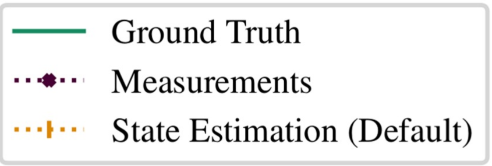
False Data Injection Attack: Evaluation

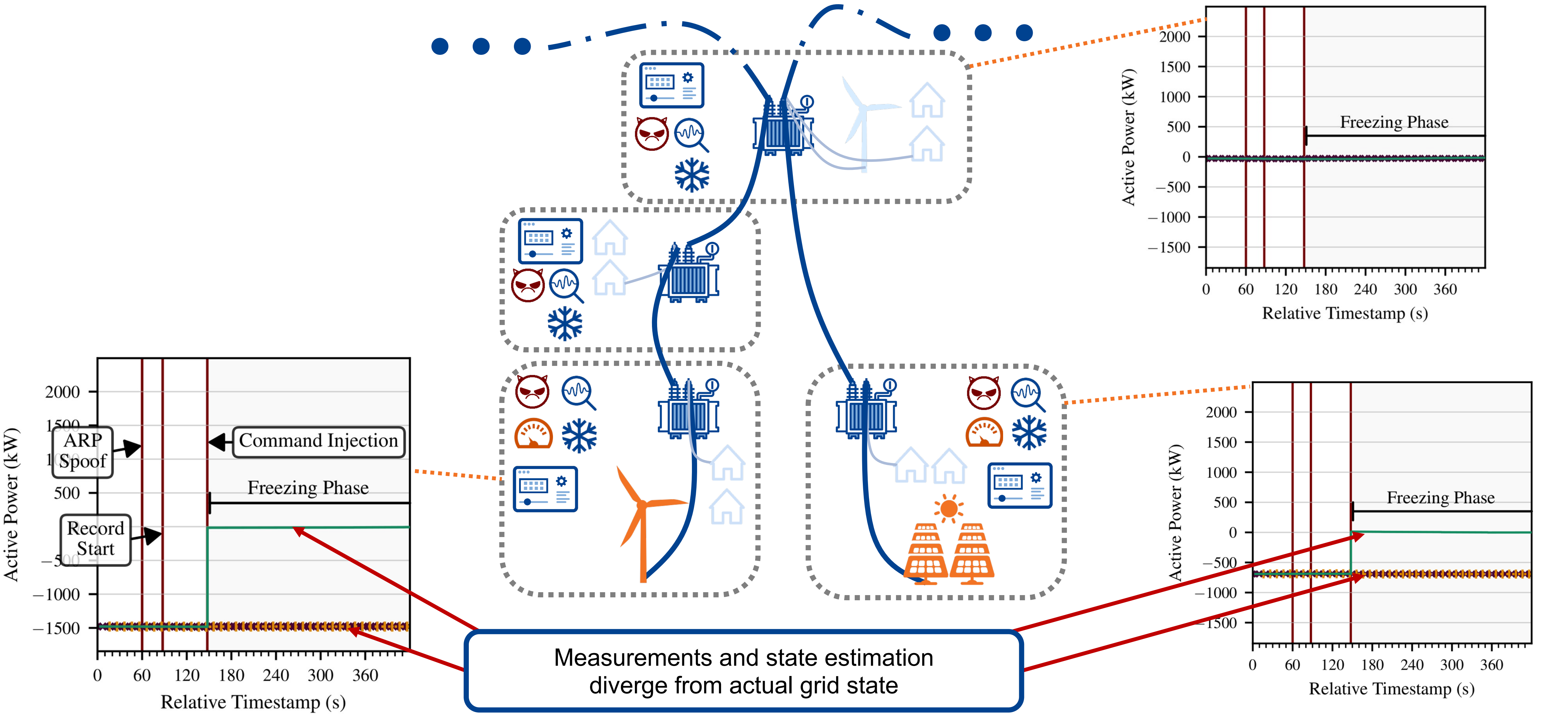


Measurements and state estimation diverge from actual grid state

This graphic uses resources from flaticon.com

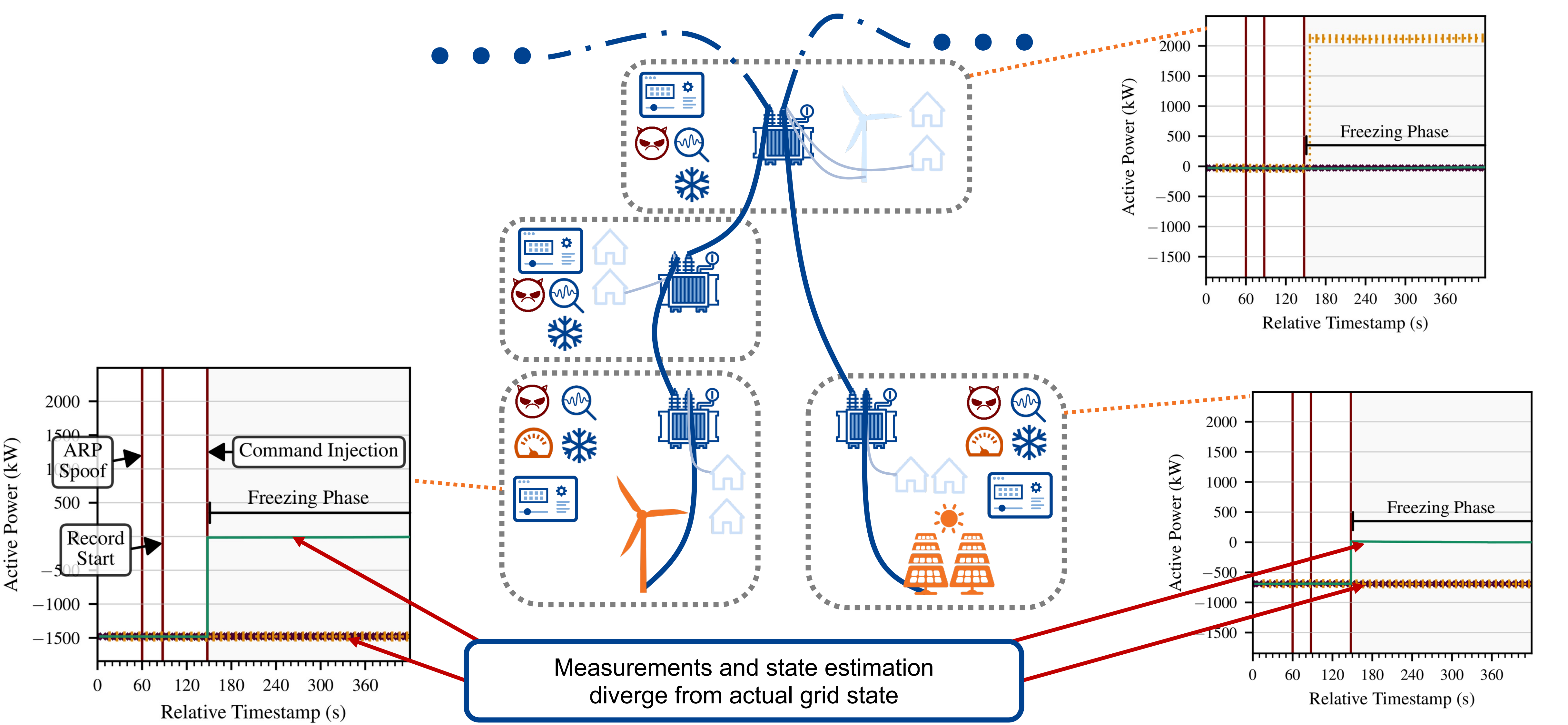
False Data Injection Attack: Evaluation





Measurements and state estimation diverge from actual grid state

False Data Injection Attack: Evaluation

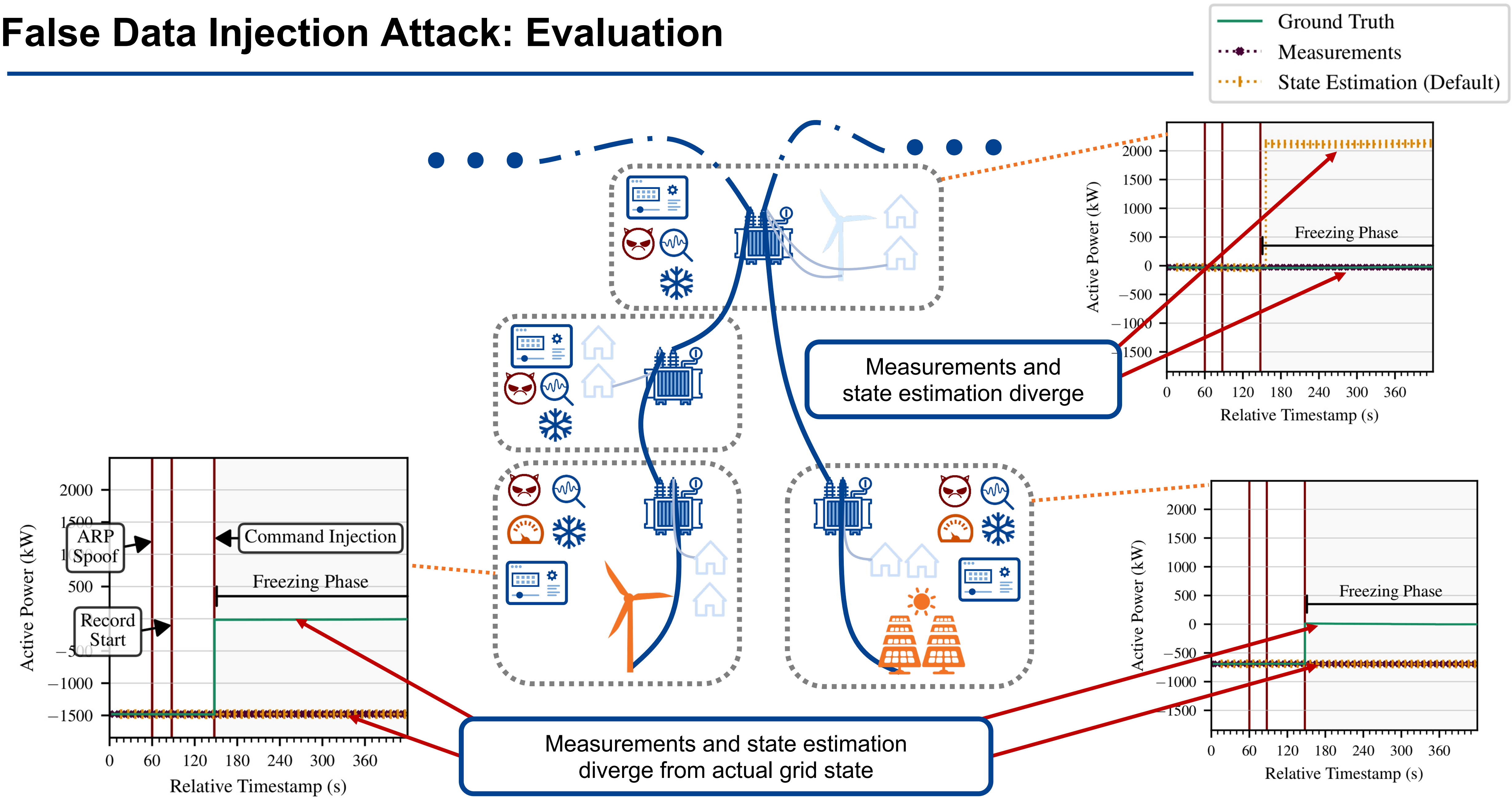


Measurements and state estimation diverge from actual grid state

This graphic uses resources from flaticon.com

Lennart Bader
lennart.bader@fkie.fraunhofer.de

False Data Injection Attack: Evaluation



Measurements and state estimation diverge

Measurements and state estimation diverge from actual grid state

This graphic uses resources from flaticon.com

False Data Injection Attack: Evaluation

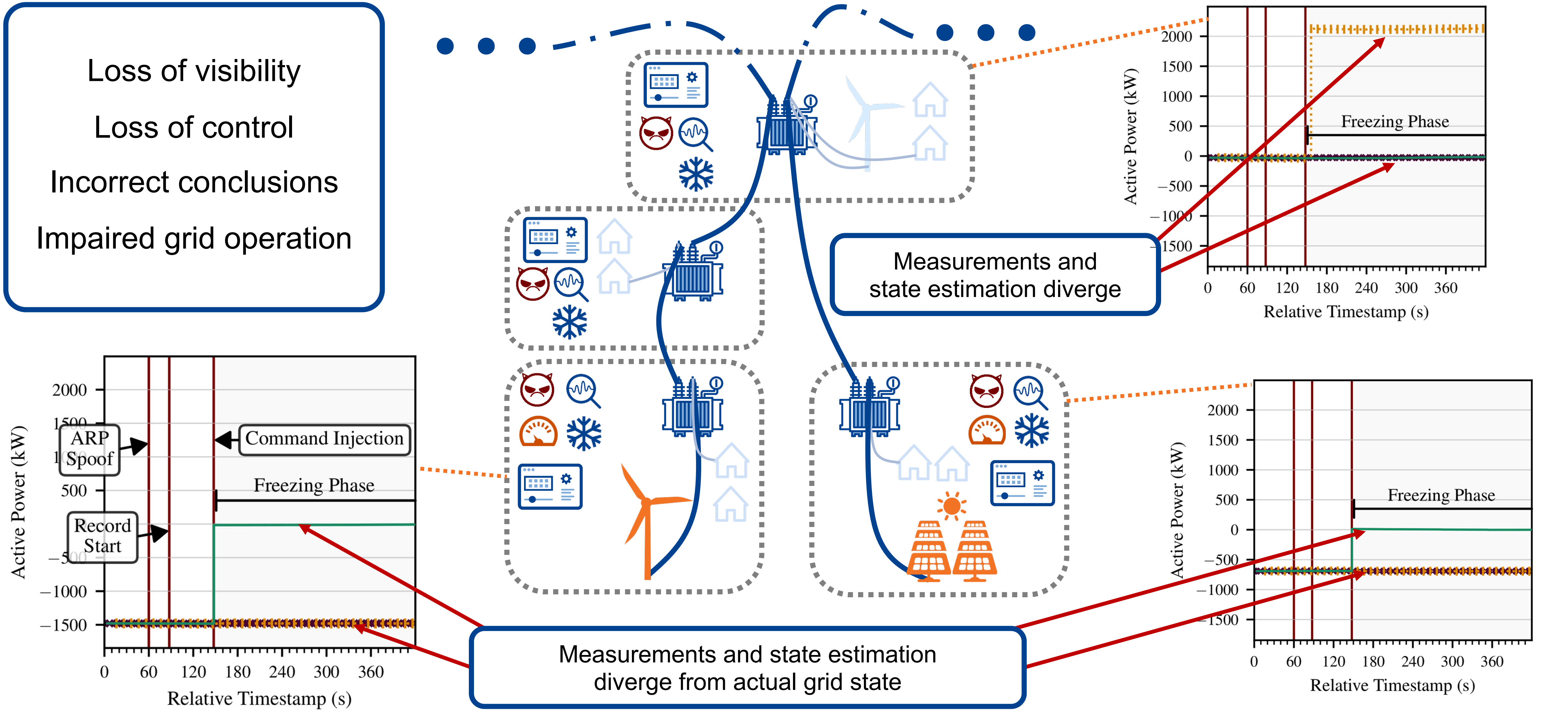
Ground Truth
Measurements
State Estimation (Default)

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

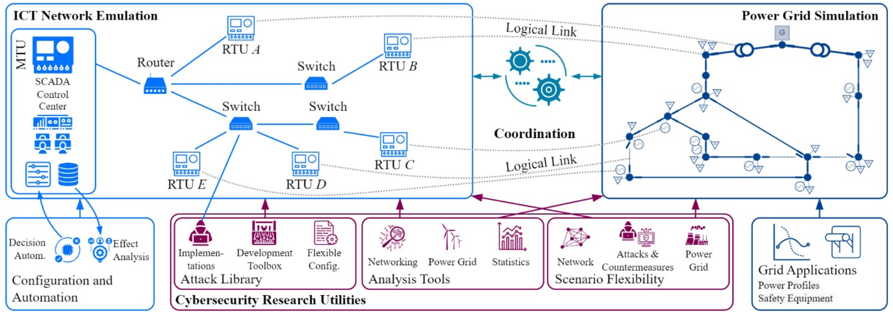
This graphic uses resources from flaticon.com

Conclusion

- **Power grids as targets for cyberattacks**
  - Digitized cyber physical system and critical infrastructure

Conclusion

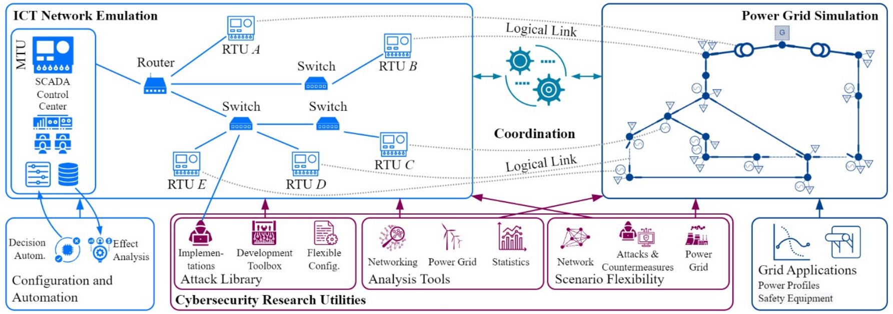
- **Power grids as targets for cyberattacks**
  - ▶ Digitized cyber physical system and critical infrastructure
- **Evaluation of attacks and their effects**
  - ▶ Co-simulation framework
  - ▶ Cybersecurity research focus
  - ▶ Evaluated attacks highlight potential vulnerabilities



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

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**



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

● ● ●

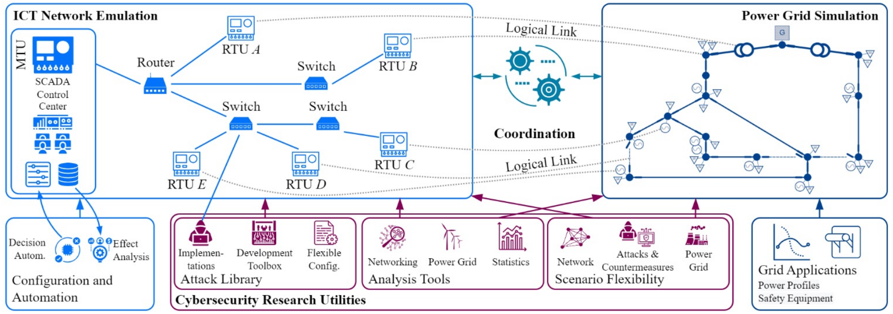
https://github.com/fkie-cad/wattson

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**

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!

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

Attacks from Related Work

Physical

Syntactic

Semantic

Complexity

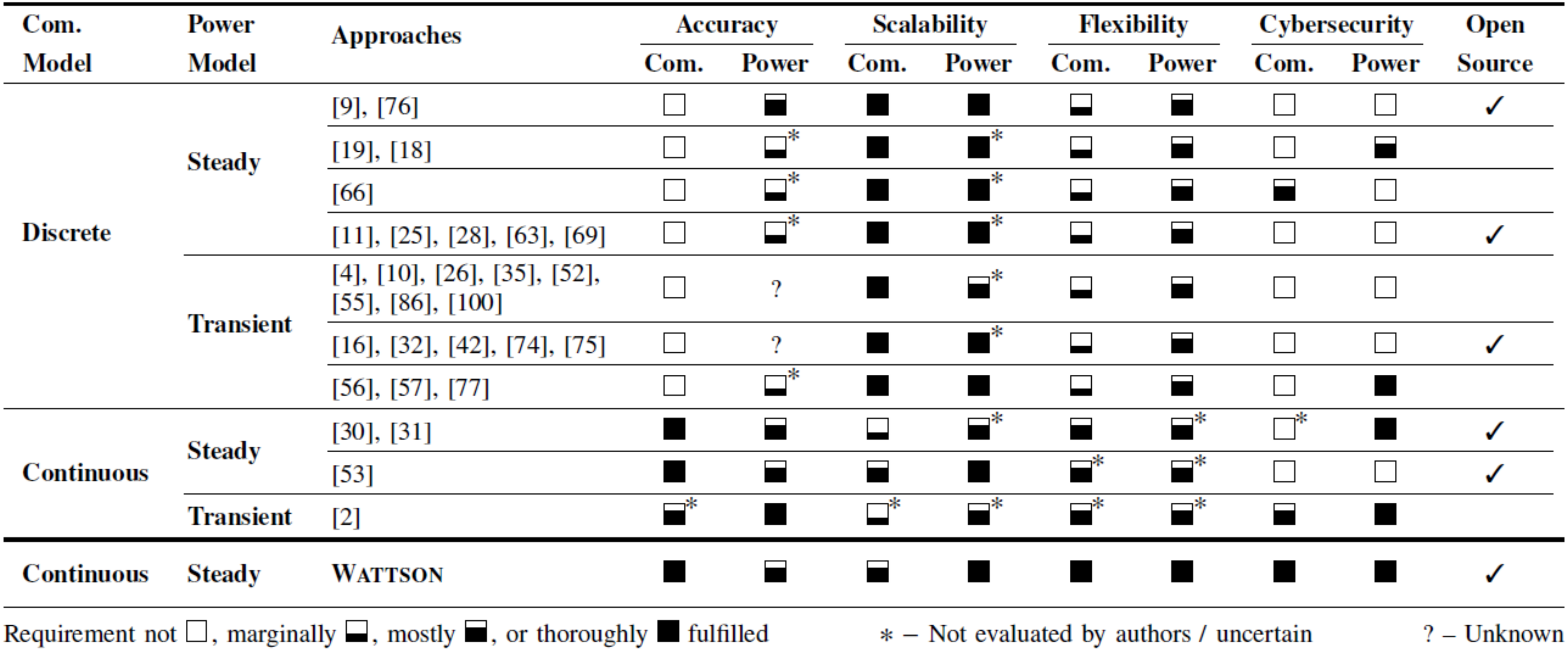
Destruction of equipment
Influencing the physical process

Interference with network traffic
e.g., Flooding, ARP Spoofing, …

Manipulation of application layer traffic
Issuance of control commands
Manipulating measurements or commands

	Attack type	ICT considered	Power grid considered
Physical	Device disconnect		[HR19A], [SZ17]
	Demand manipulation		[HCB19], [SMP18], [SGB19], [WPL+19]
Syntactic	Denial of service	[AVN12], [CCC12], [MAC+11], [ZG12], **[SK15]**	**[SK15]**, [AMD+18], [HYJ16], [HR19B], [LDS+12], [ZHW+22]
	Replay	[LLZ+14], [LCG+16], [WZ11]	[IN17], [ZHW+22], [ZWY16]
Semantic		[PR21]	[AMD+18], [IN17], [TSL13]
	False data injection	[CCC12], [KT13], [KP11], [KTT14], [LLZ+14], [WCM+20]	[AMD+18], [DYS+20], [LDS+12], [PTL+17], [D19], [KJT+11], [LNR11], [ZGD+13], [GLS+21], [JLJ19], [LZL+17], [RB15]

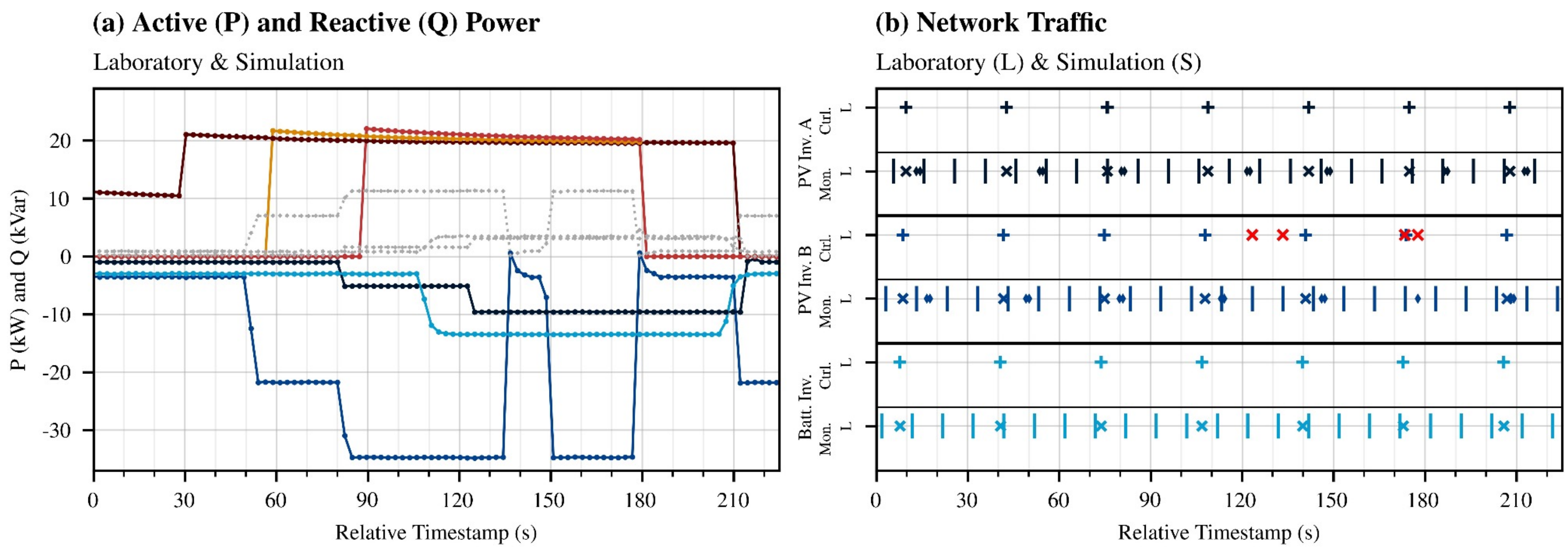
Existing Co-Simulation Environments



Com. Model	Power Model	Approaches	Accuracy		Scalability		Flexibility		Cybersecurity		Open
			Com.	Power	Com.	Power	Com.	Power	Com.	Power	Source
Discrete	Steady	[9], [76]	□	▆	■	■	⬓	▆	□	□	✓
		[19], [18]	□	⬓*	■	■*	⬓	▆	□	▆	
		[66]	□	⬓*	■	■*	⬓	▆	▆	□	
		[11], [25], [28], [63], [69]	□	⬓*	■	■*	⬓	▆	□	□	✓
	Transient	[4], [10], [26], [35], [52], [55], [86], [100]	□	?	■	▆*	⬓	▆	□	□	
		[16], [32], [42], [74], [75]	□	?	■	■*	⬓	▆	□	□	✓
		[56], [57], [77]	□	⬓*	■	■	⬓	▆	□	■	
Continuous	Steady	[30], [31]	■	▆	⬓	▆*	▆	▆*	□*	■	✓
		[53]	■	▆	▆	■	▆*	▆*	□	□	✓
	Transient	[2]	▆*	■	⬓*	▆*	▆*	▆*	▆	■	
Continuous	**Steady**	**WATTSON**	■	▆	▆	■	■	■	■	■	✓

Requirement not □, marginally ⬓, mostly ▆, or thoroughly ■ fulfilled ∗ – Not evaluated by authors / uncertain ? – Unknown

Accuracy Evaluation


(a) Active (P) and Reactive (Q) Power

Laboratory & Simulation

(b) Network Traffic

Laboratory (L) & Simulation (S)

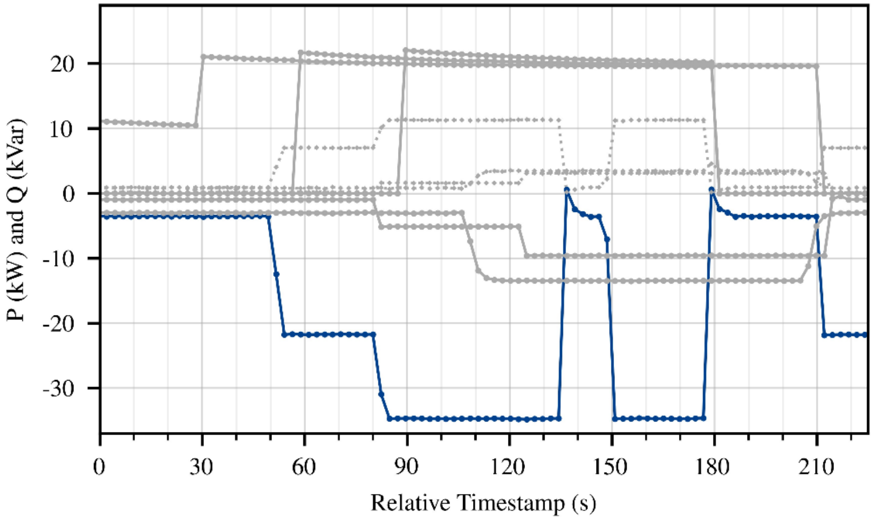
© Martin Braun

- **Recreate laboratory topology and scenario in Wattson**
  - Normal behavior and attack
- **Compare laboratory and simulation**
  - Network communication
  - Power grid components

Accuracy Evaluation

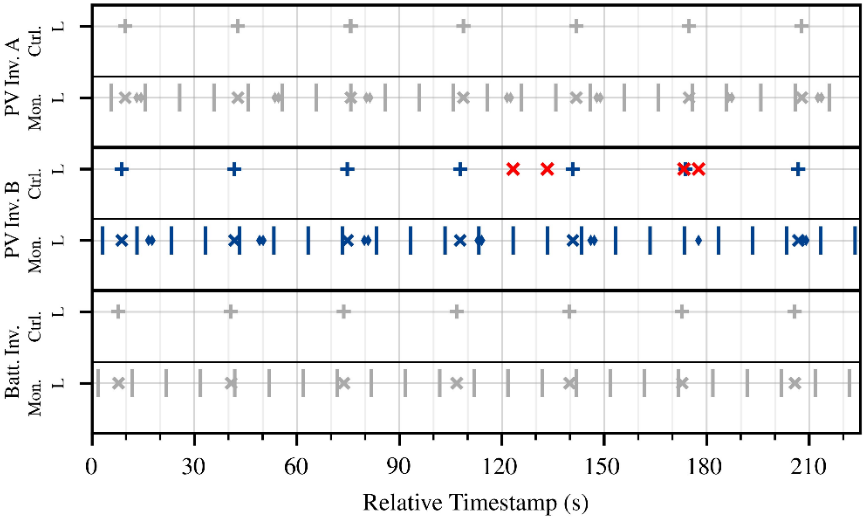
(a) Active (P) and Reactive (Q) Power

Laboratory & Simulation



(b) Network Traffic

Laboratory (L) & Simulation (S)

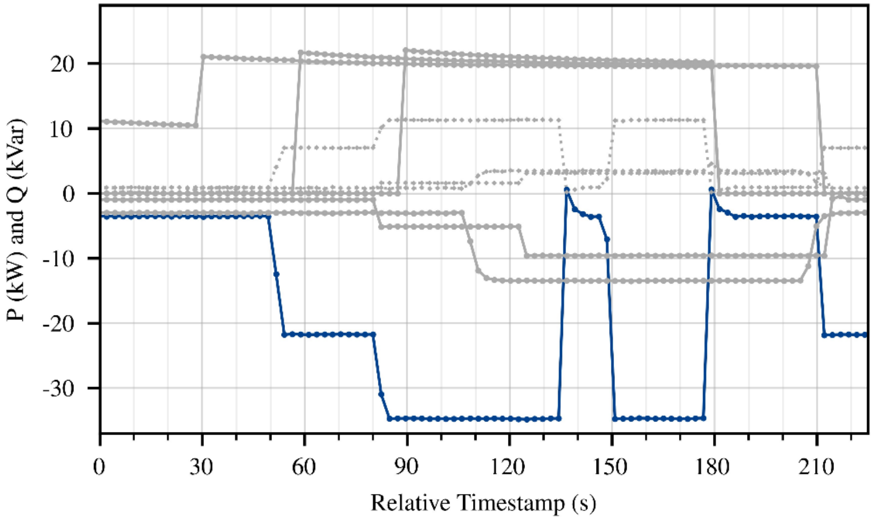


© Martin Braun

Accuracy Evaluation

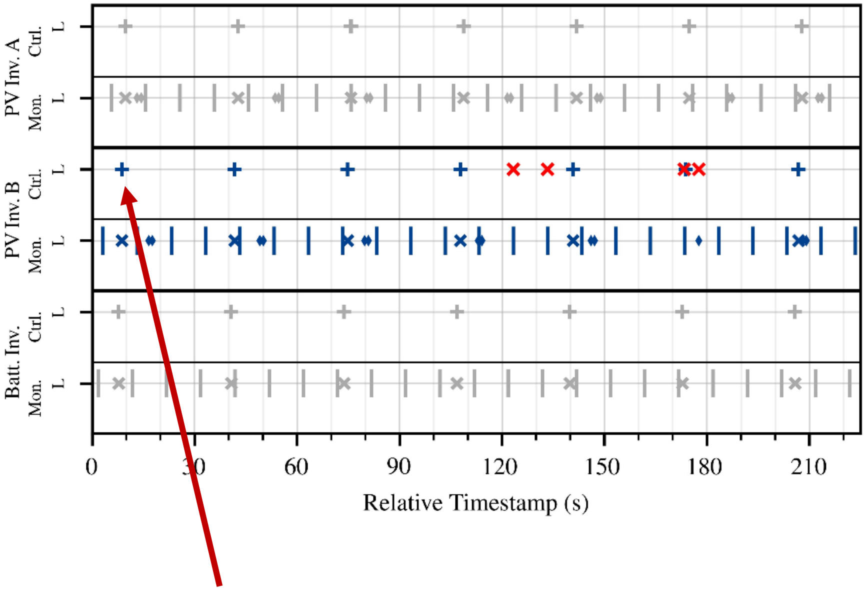
(a) Active (P) and Reactive (Q) Power

Laboratory & Simulation



(b) Network Traffic

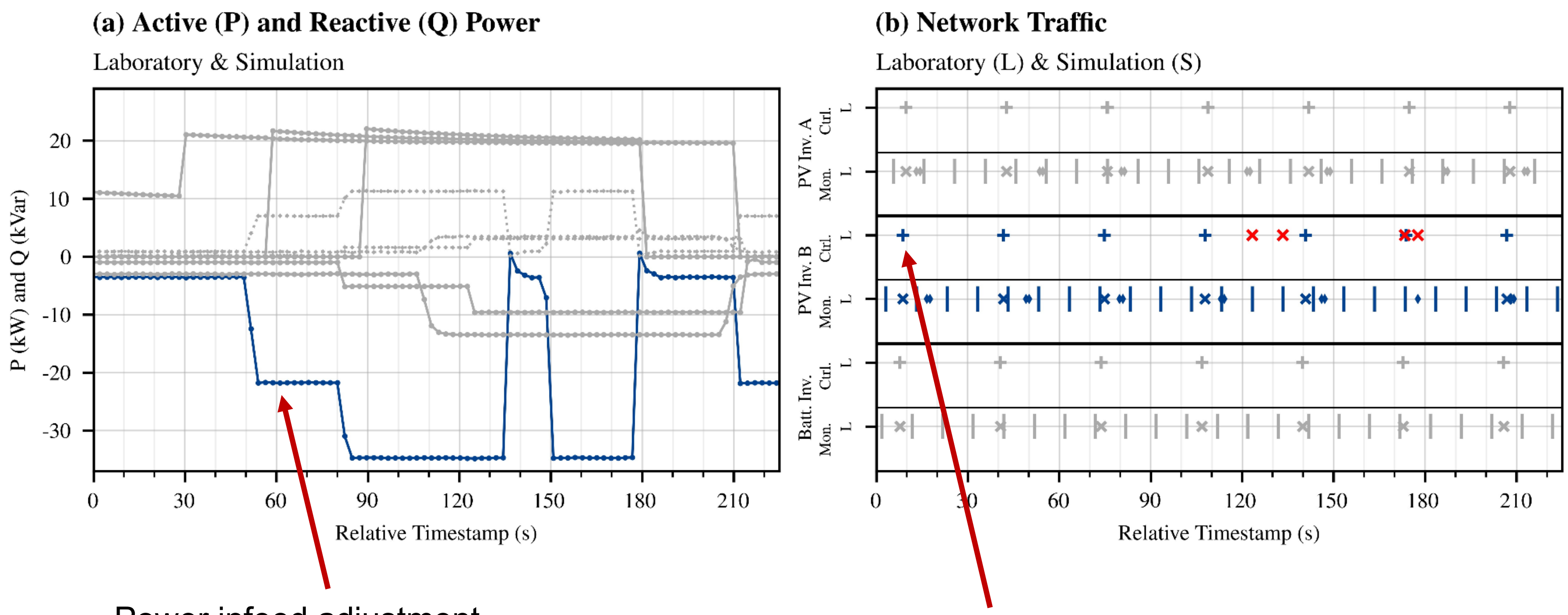
Laboratory (L) & Simulation (S)



Periodic control commands +

© Martin Braun

Accuracy Evaluation



(a) Active (P) and Reactive (Q) Power

Laboratory & Simulation

(b) Network Traffic

Laboratory (L) & Simulation (S)

Power infeed adjustment by grid operator

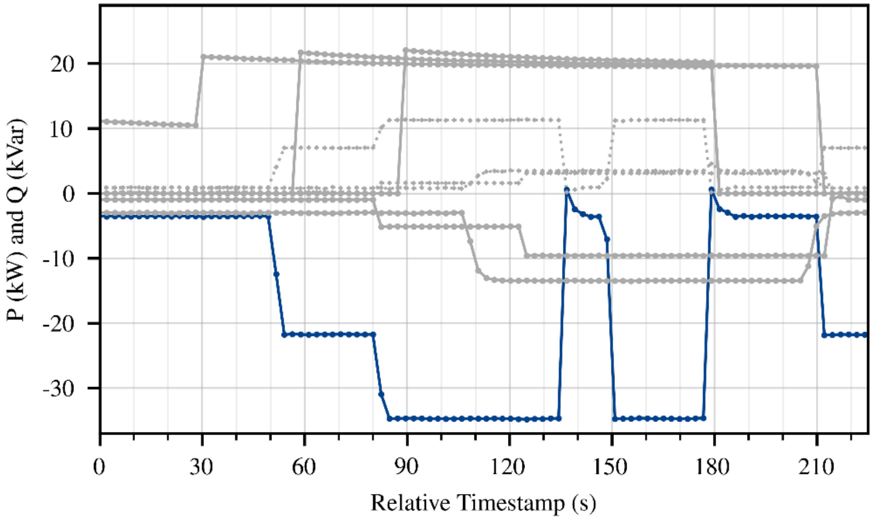
Periodic control commands +

© Martin Braun

Accuracy Evaluation

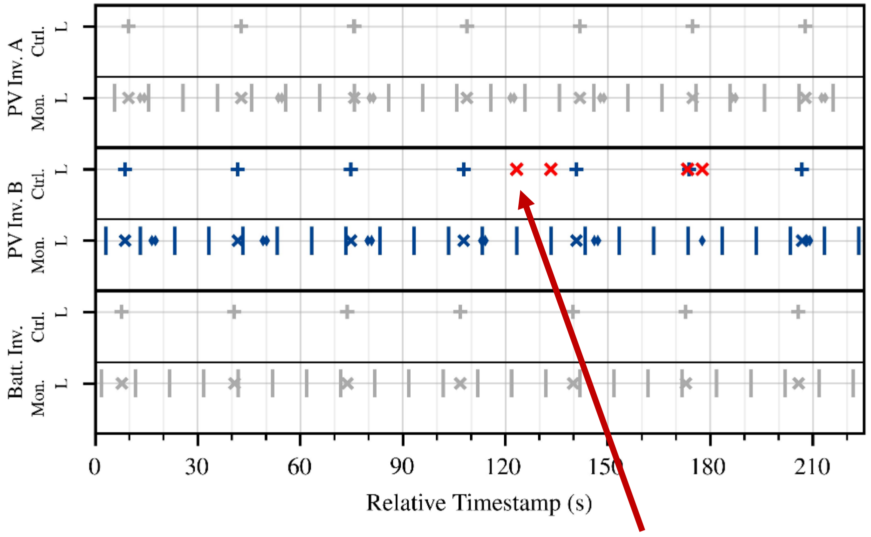
(a) Active (P) and Reactive (Q) Power

Laboratory & Simulation



(b) Network Traffic

Laboratory (L) & Simulation (S)



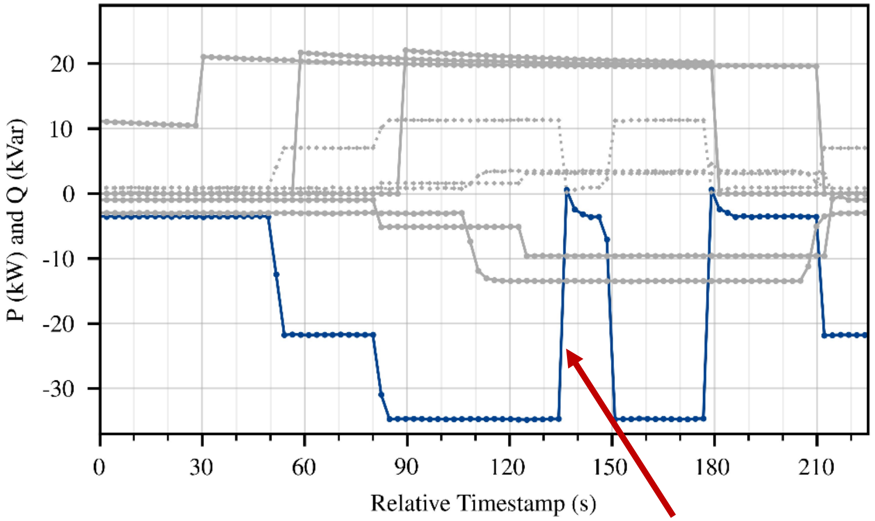
Malicious control commands ×

© Martin Braun

Accuracy Evaluation

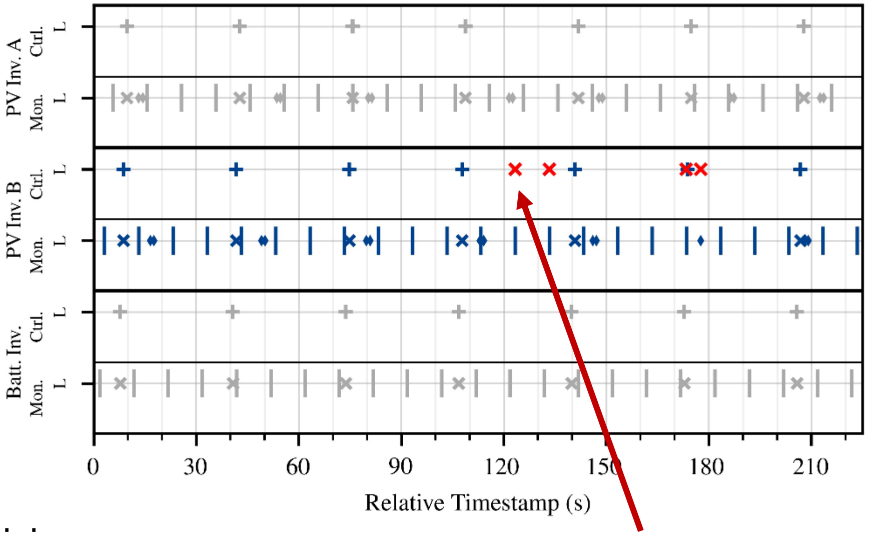
(a) Active (P) and Reactive (Q) Power

Laboratory & Simulation



(b) Network Traffic

Laboratory (L) & Simulation (S)



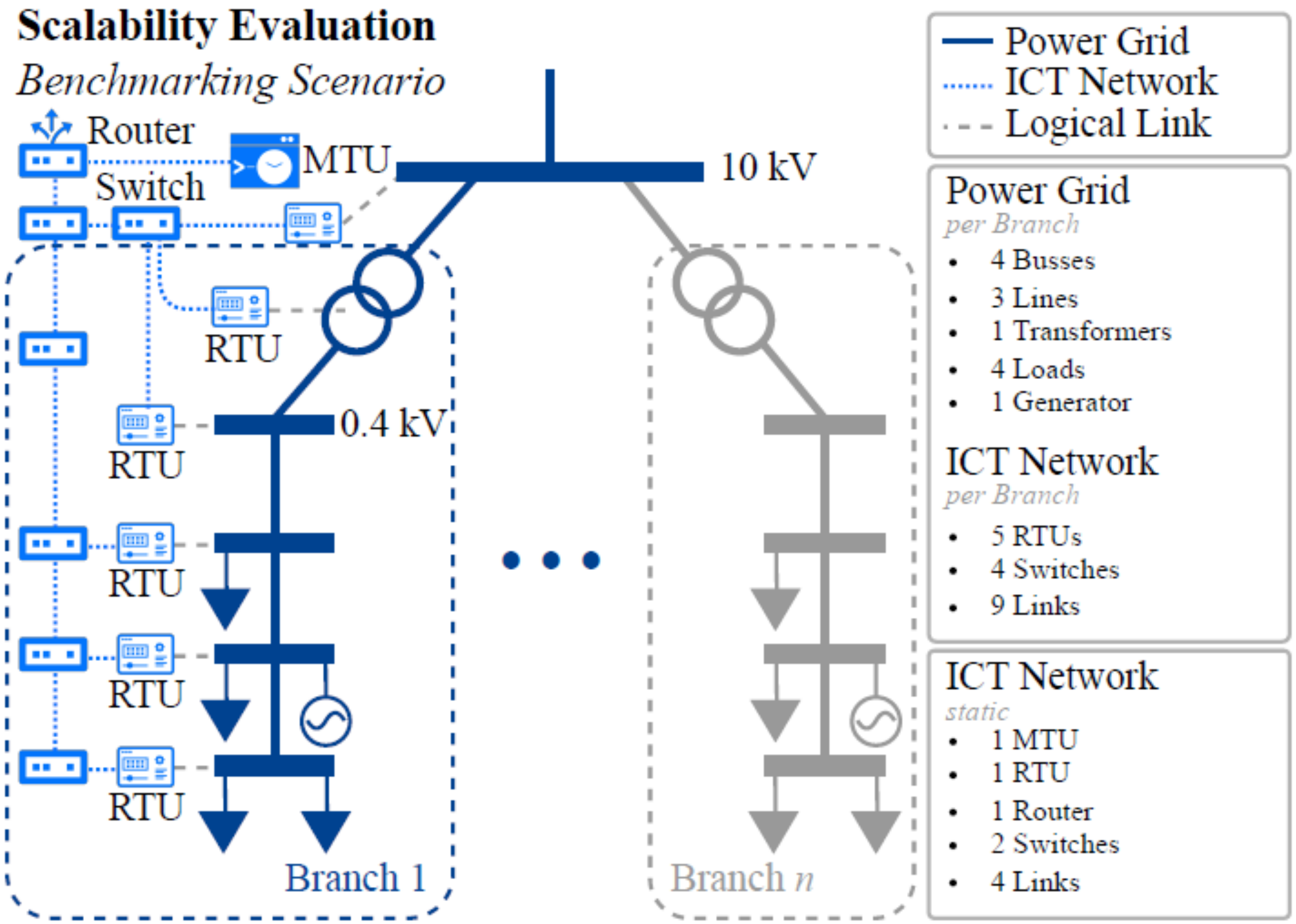
© Martin Braun

Effect of malicious control commands

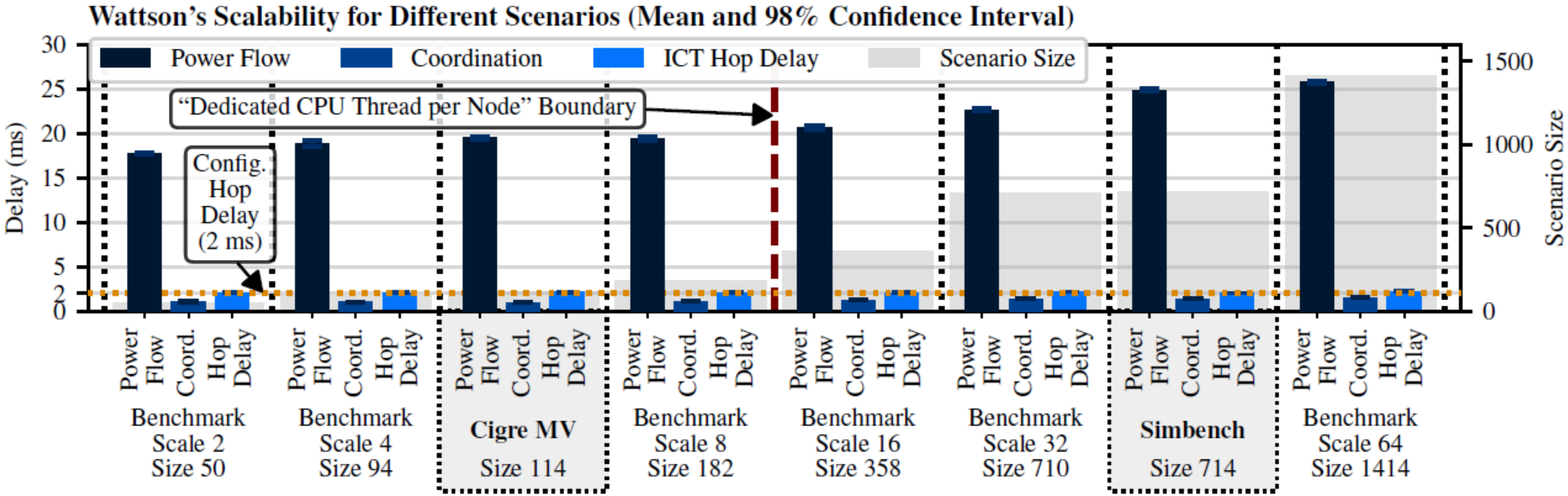
Malicious control commands ×

Scalability Evaluation

- **Benchmarking grids**
  - ~ Linear scaling of all aspects
- **Reference grids**
  - Realistic grids from literature
- **Metrics**
  - Network delay
  - Power grid simulation
  - Coordination overhead

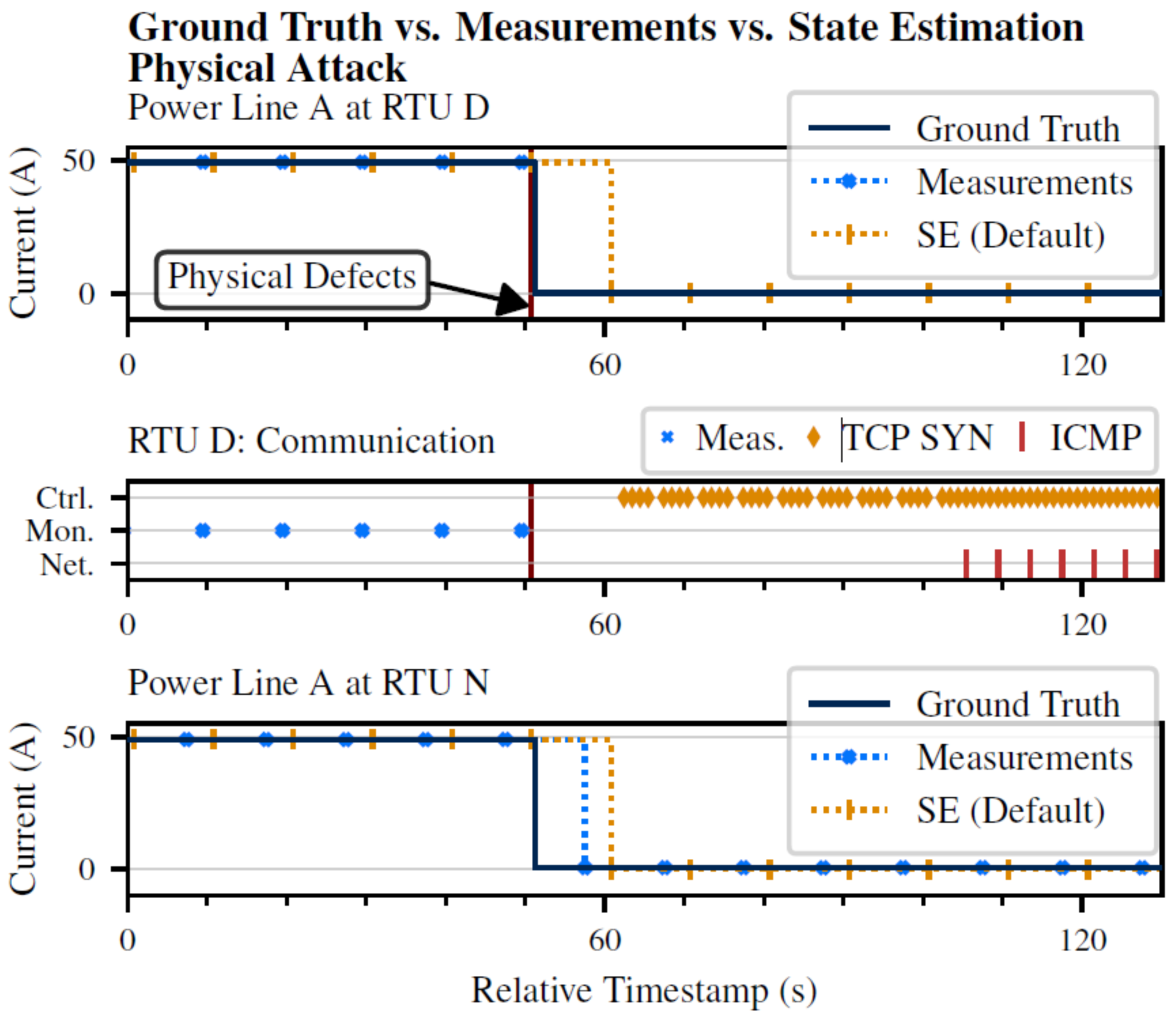


Scalability Evaluation

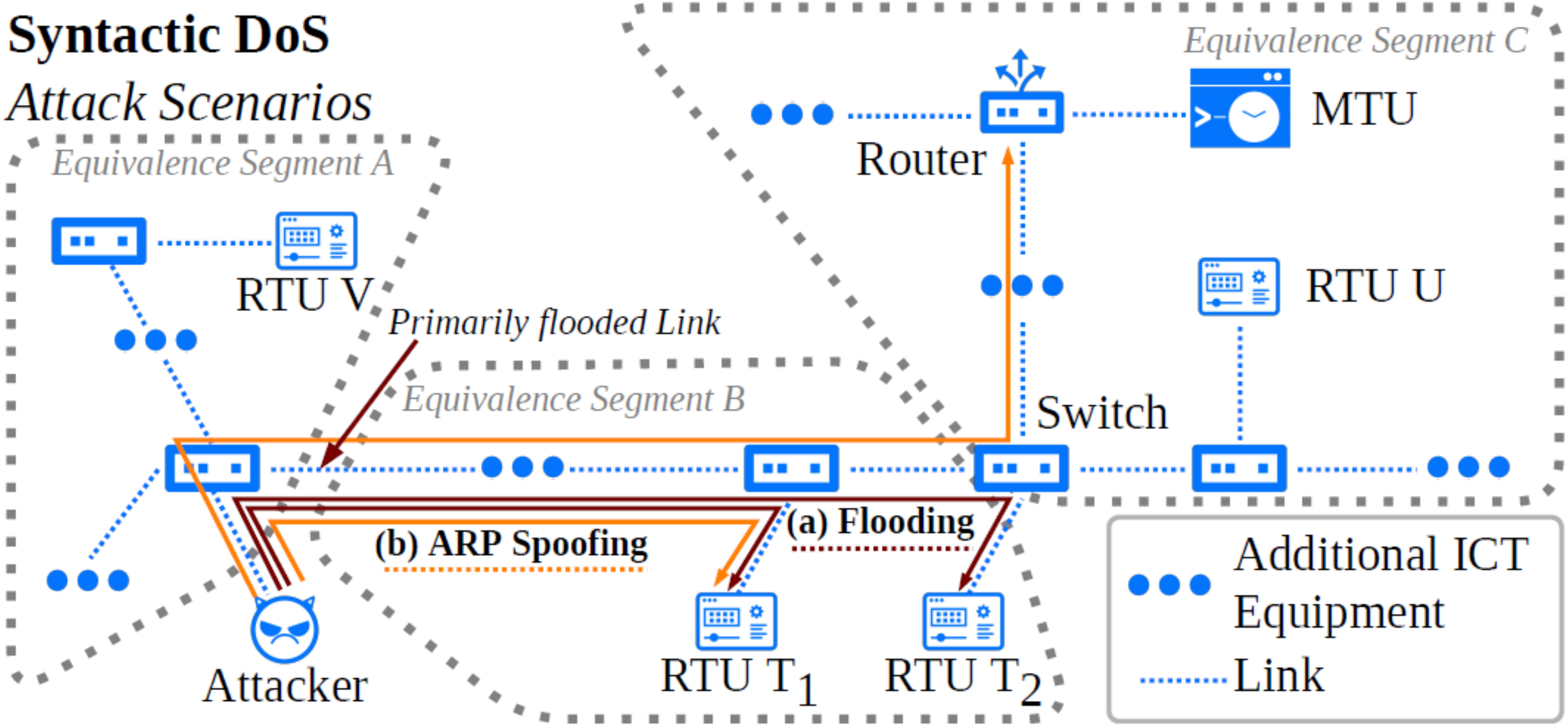


Physical Attack

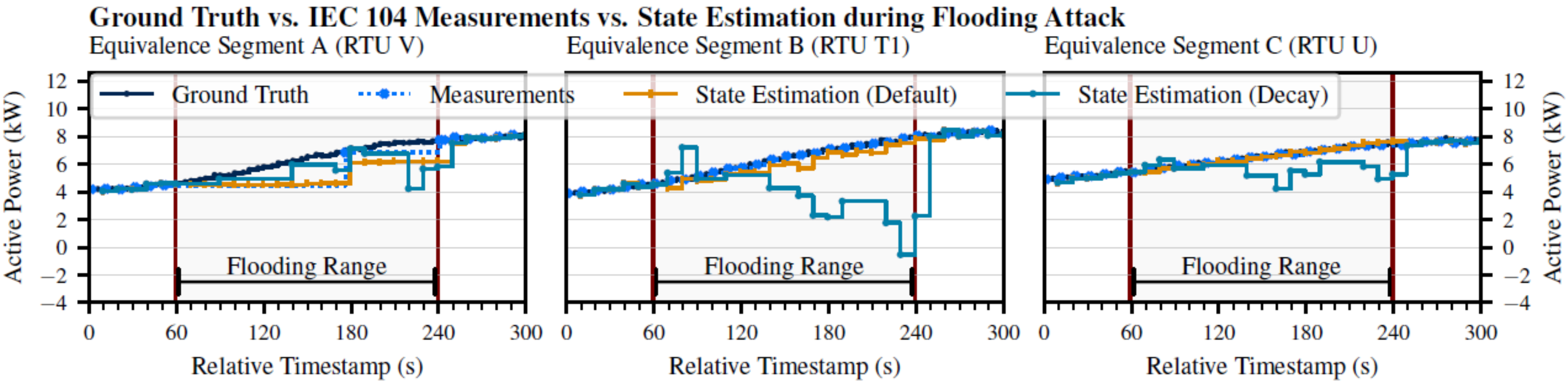
- **Destruction of assets**
  - Substation
    - Lines / Switches / Bus
  - Network equipment
    - Switch(es), RTU
- **Measurements missing**
  - No new measurements arrive
- **State estimation detects fault**
  - Based on measurements from other substations



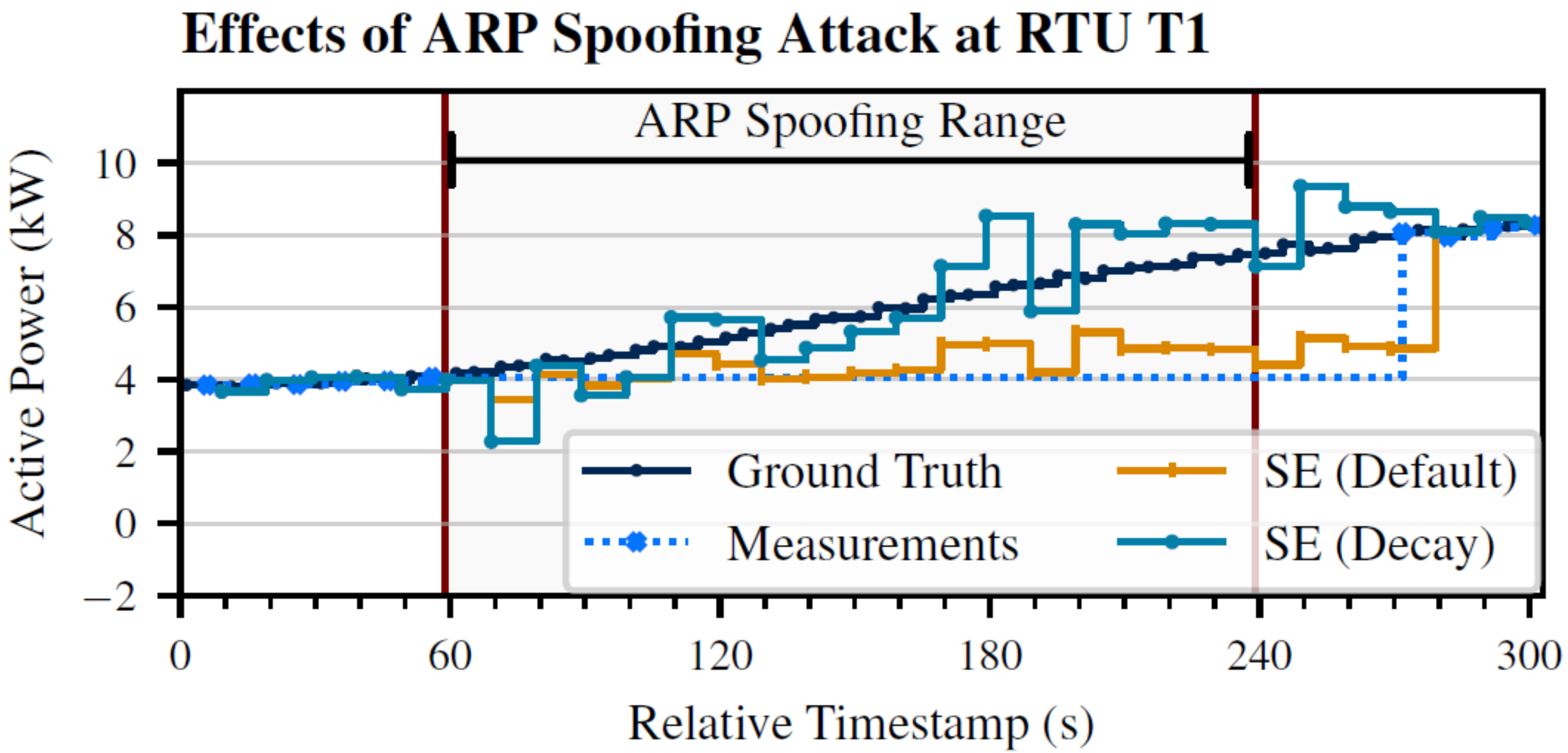
Syntactic Attacks: Scenario



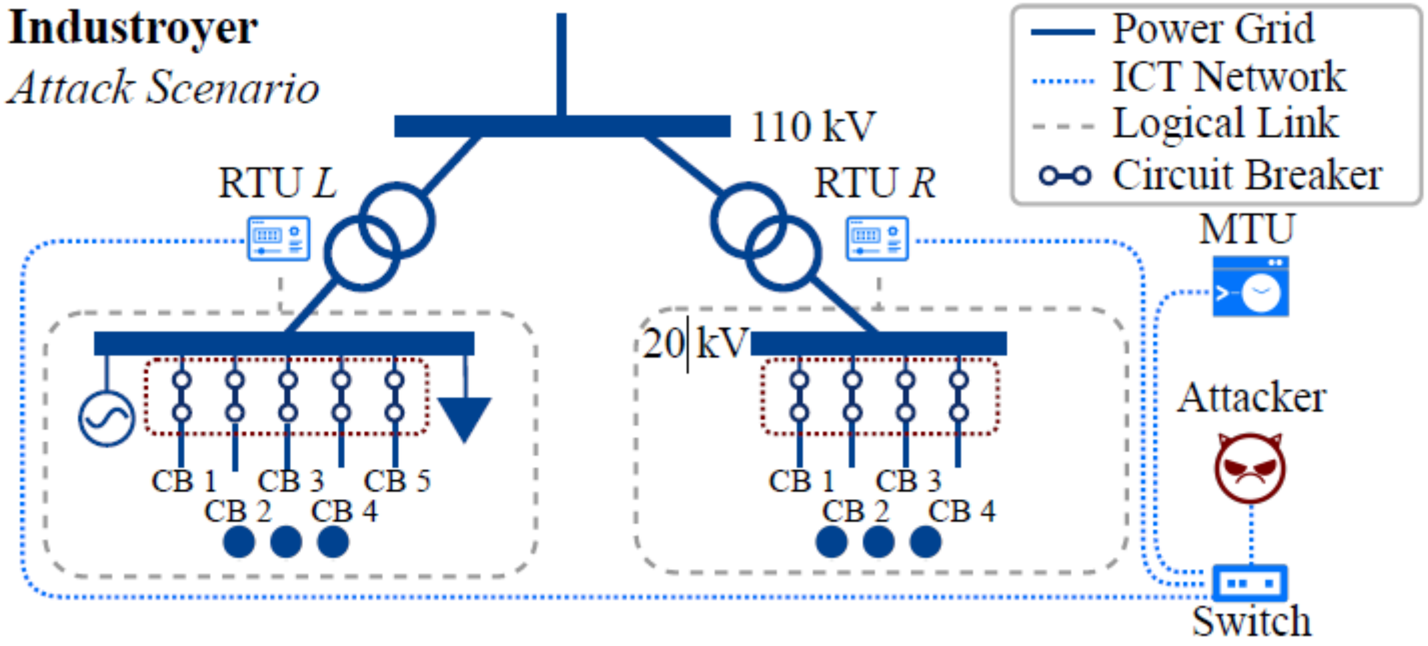
Syntactic Attack: Flooding (DoS)



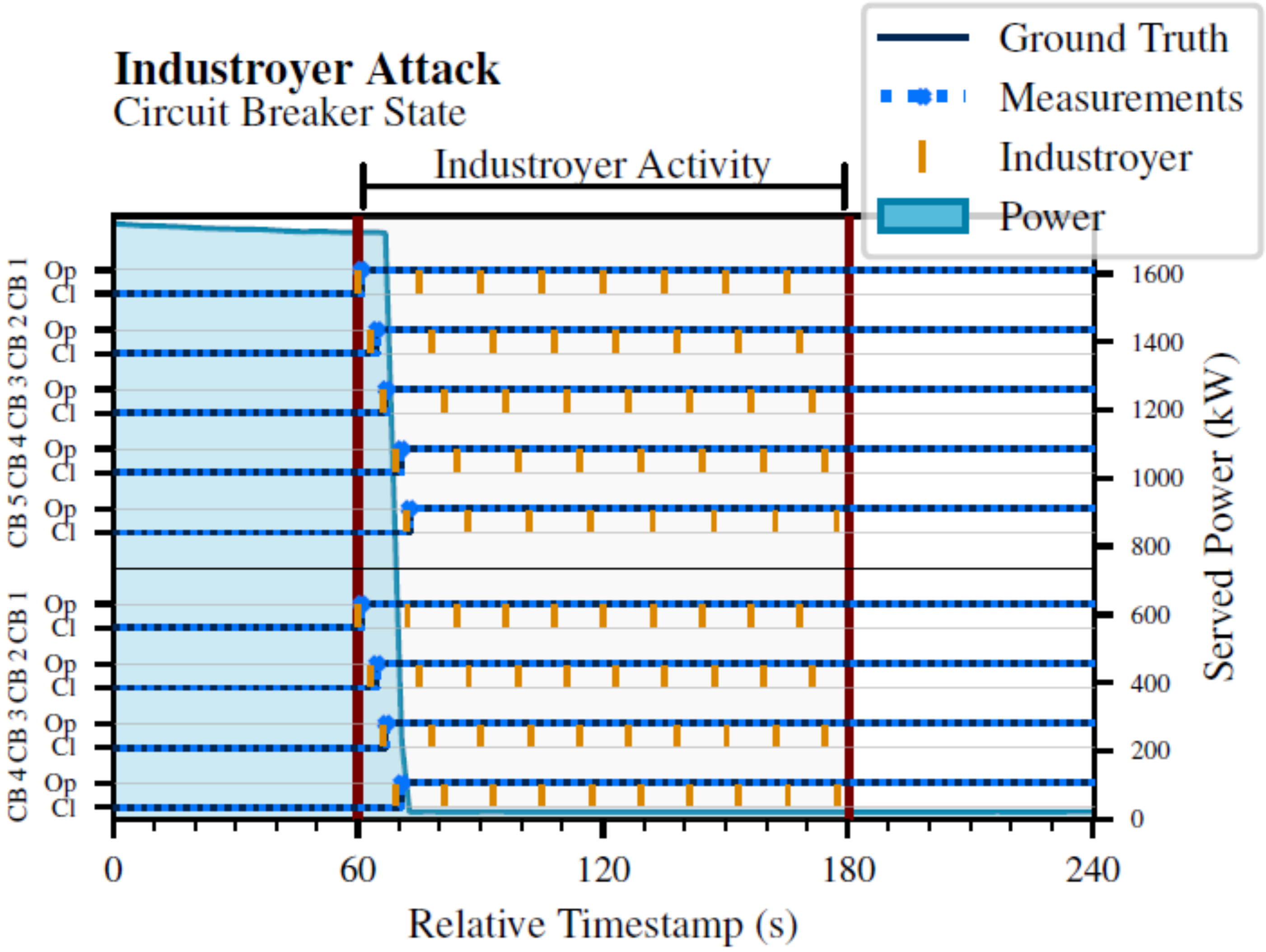
Syntactic Attack: ARP Spoofing (DoS)



Semantic Attack: Industroyer



Semantic Attack: Industroyer


Industroyer Attack
Circuit Breaker State
Industroyer Activity
Ground Truth
Measurements
Industroyer
Power
CB 1
CB 2
CB 3
CB 4
CB 5
CB 1
CB 2
CB 3
CB 4
Op
Cl
Relative Timestamp (s)
Served Power (kW)