Resilient Smart Grids

André Teixeira

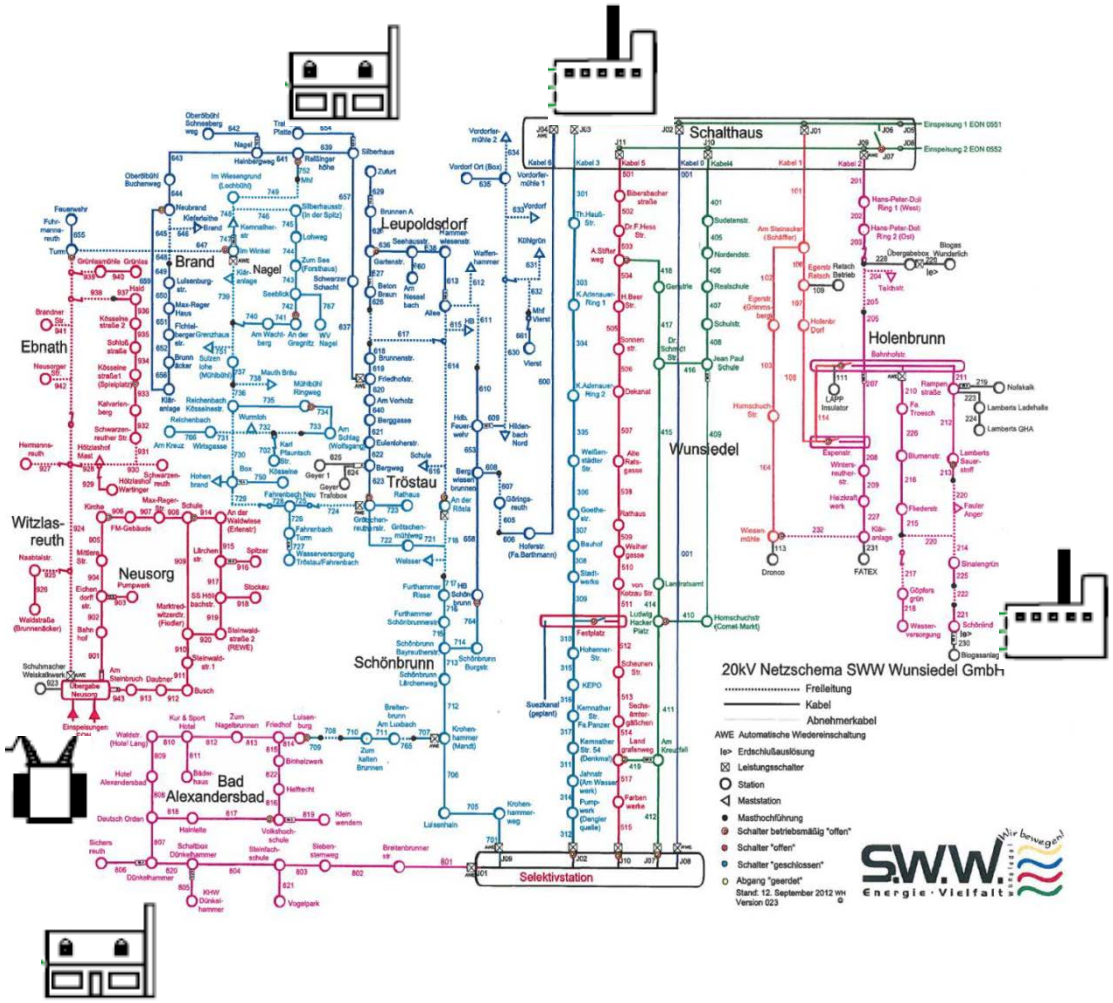
Kaveh Paridari, Henrik Sandberg

KTH Royal Institute of Technology, Sweden

SPARKS 2nd Stakeholder Workshop
Cork, Ireland
March 25th, 2015

EU FP7 Programme Contract No. 608224

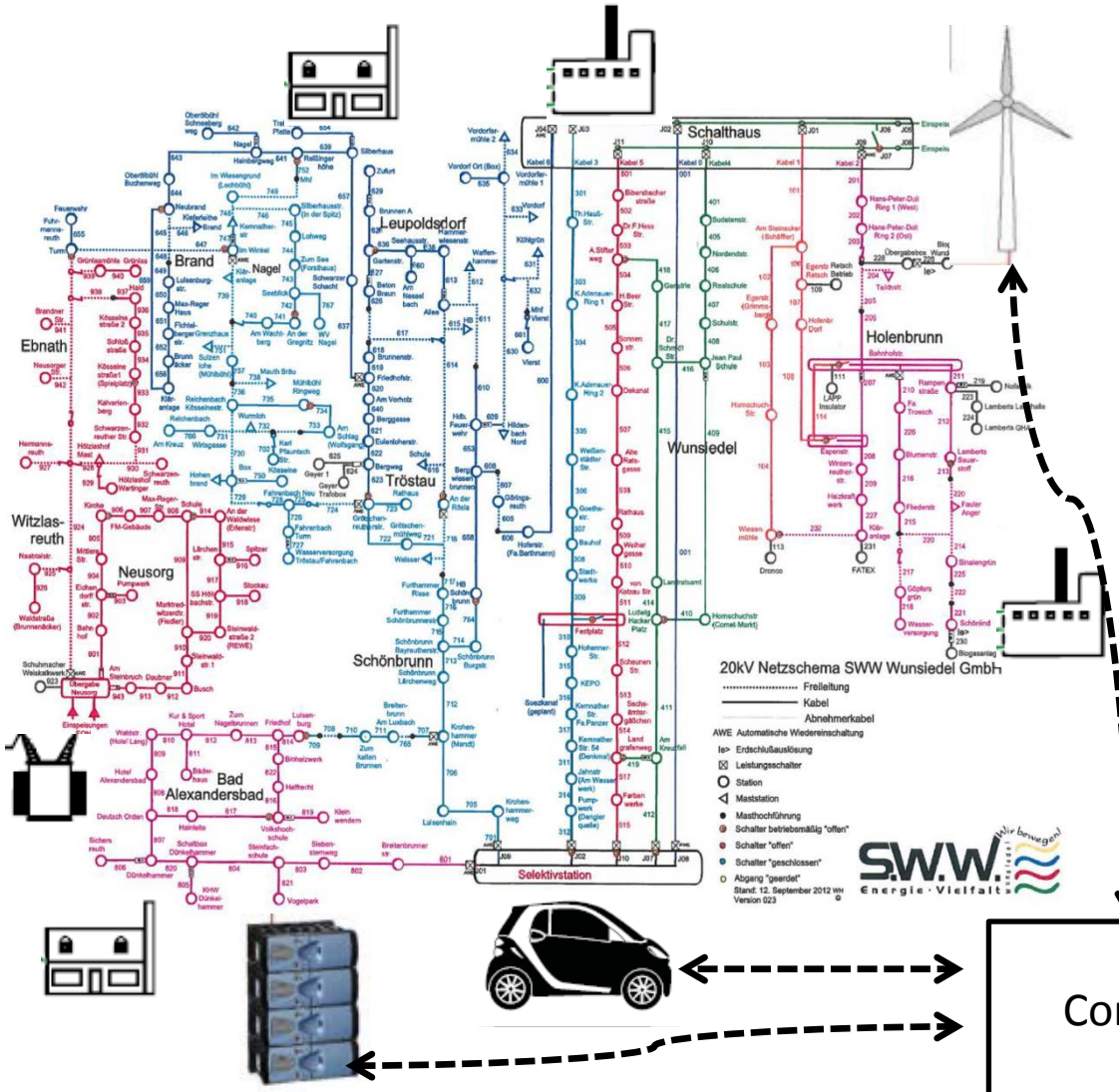
Legacy Distribution Grids



- Main objectives
  - Satisfy power demand
  - Keep nominal voltage levels
  - Maintain frequency at 50Hz
- Limited capabilities:
- Passive loads
  - cannot be freely controlled
- Small number of measurements
  - Feeders, transformers, end of line voltage
- Few control points
  - Transformers, switches

EU FP7 Programme Contract No. 608224

From Legacy Grids to Smart Grids

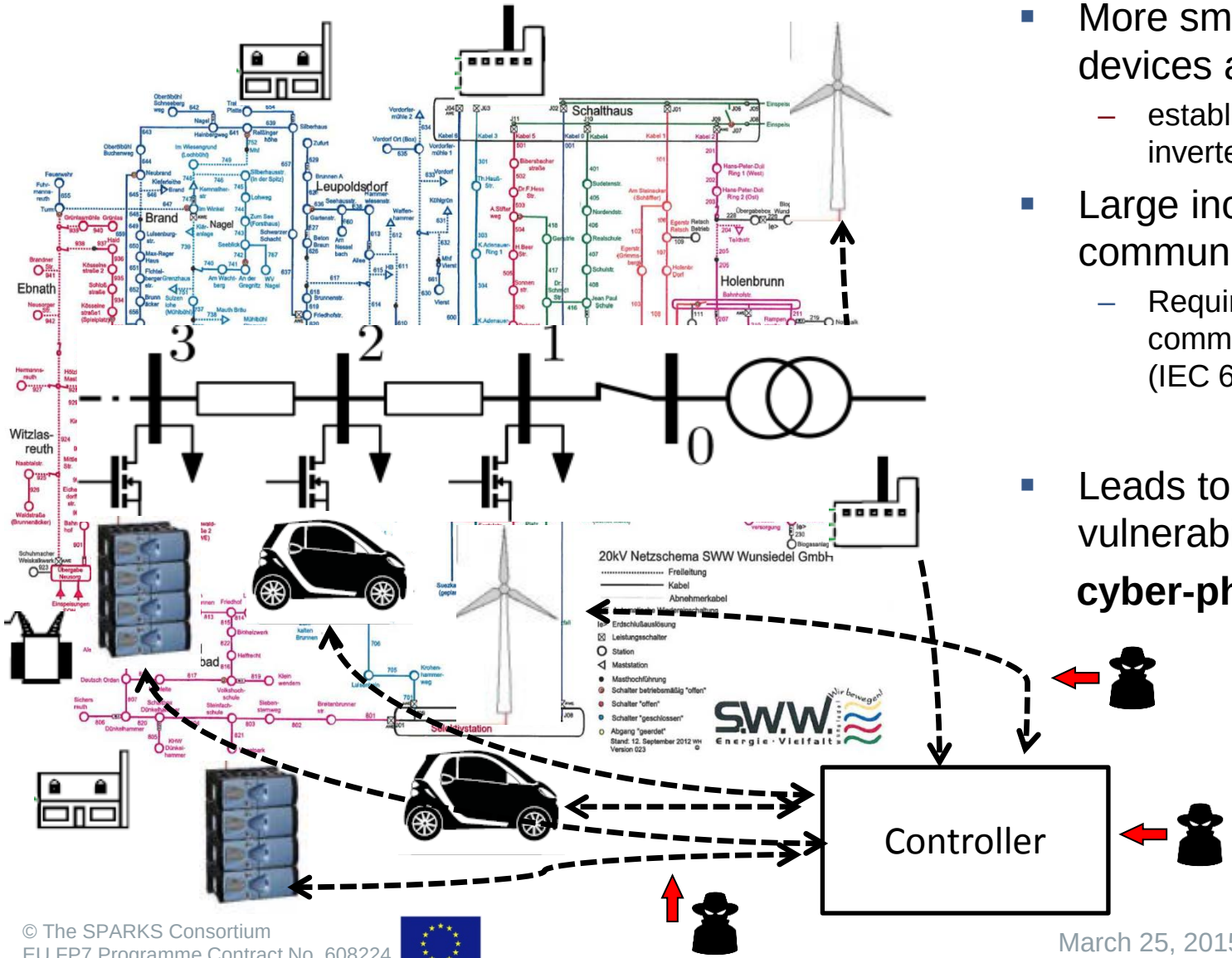


- Main objectives
  - Satisfy power demand
  - Keep nominal voltage levels
  - Maintain frequency at 50Hz
- Enhanced capabilities:
- Smart controllable devices
- Large increase in measurements
  - Smart meters, **power inverters**
- Large increase in control loops (devices with **power inverters**)
  - Electric vehicles
  - Solar panels
  - Wind turbines
  - Batteries

Controller

EU FP7 Programme Contract No. 608224

Smart Grids

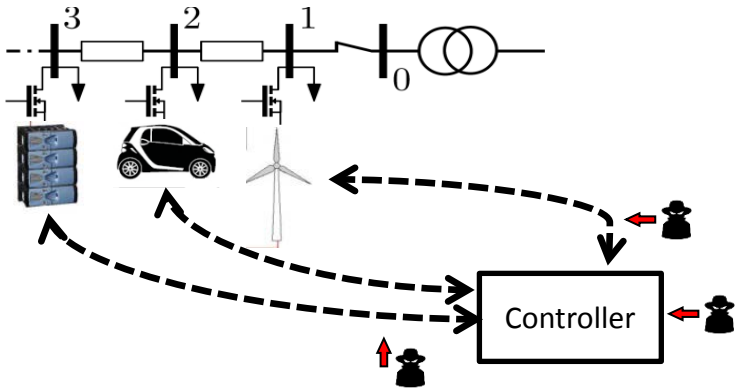


- More smart controllable devices and control loops
  - established through power inverters
- Large increase in communication and data
  - Requires standard communication protocols (IEC 61850)
- Leads to increasing vulnerability to **cyber-physical threats**

EU FP7 Programme Contract No. 608224

Resilient Smart Grids

- The Smart Grid is a cyber-physical system
  - **Power system** and **IT infrastructure** tightly coupled through control loops



- Traditional IT security provides necessary tools
  - but not sufficient to secure cyber-physical systems
  - **Cyber** threats can have **physical** consequences!
- Need for methods to understand and mitigate attacks:
  - Which threats should we care about?
  - What impact can we expect from attacks?
  - How to reduce the impact of such threats?

Risk Assessment

Resilient Control

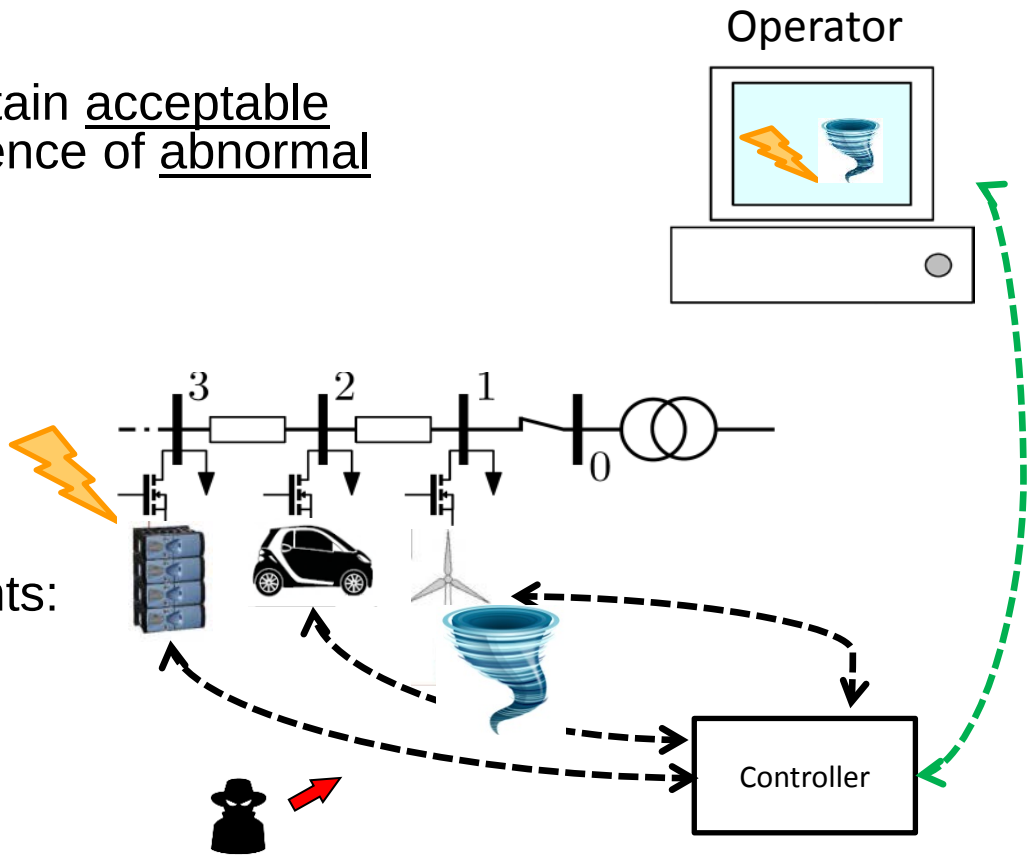
Resilient Smart Grids

- **Resilience**: the ability to maintain acceptable levels of operation in the presence of abnormal conditions.

- Sources of abnormality:
  - Disturbances
  - Faults
  - **Cyber-threats**

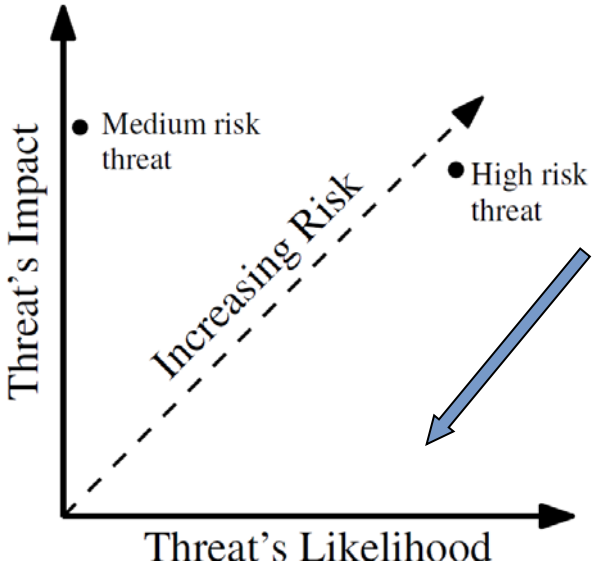
- Resilient operation requirements:
  - Satisfy power demand
  - Keep nominal voltage levels
  - Maintain frequency at 50Hz

  - Ensure state awareness
  - Satisfy operational constraints
  - Graceful degradation



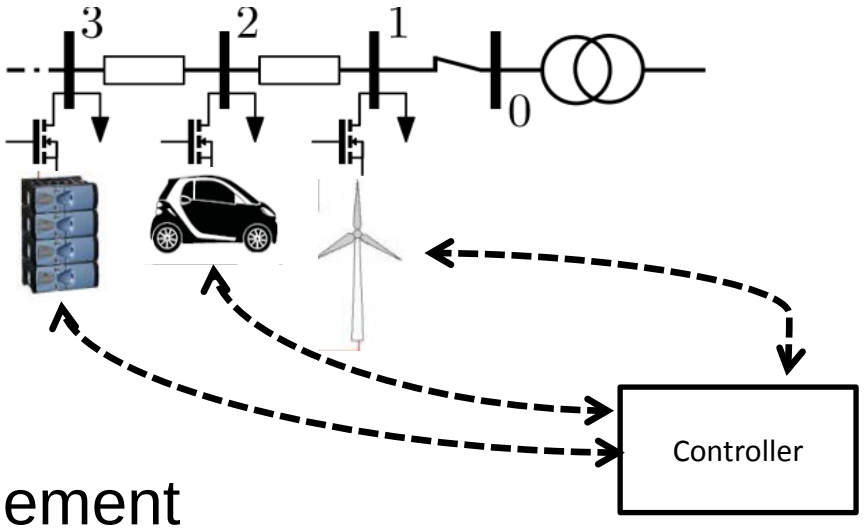
Resilient Control Methodology

- Inputs:
  - Risk assessment
  - Threat scenarios
- Resilient Control Goals:
  - Mitigate risk to increase resilience
- Resilient Control Approaches:
  - Anomaly / Intrusion Detection
  - Distributed Resource Management
  - Fault-Tolerant and Robust Control
- Desired Outputs:
  - Mitigated risk



Resilient Control Approaches

- Anomaly Detection
  - Data-Analytics
  - Formal Methods

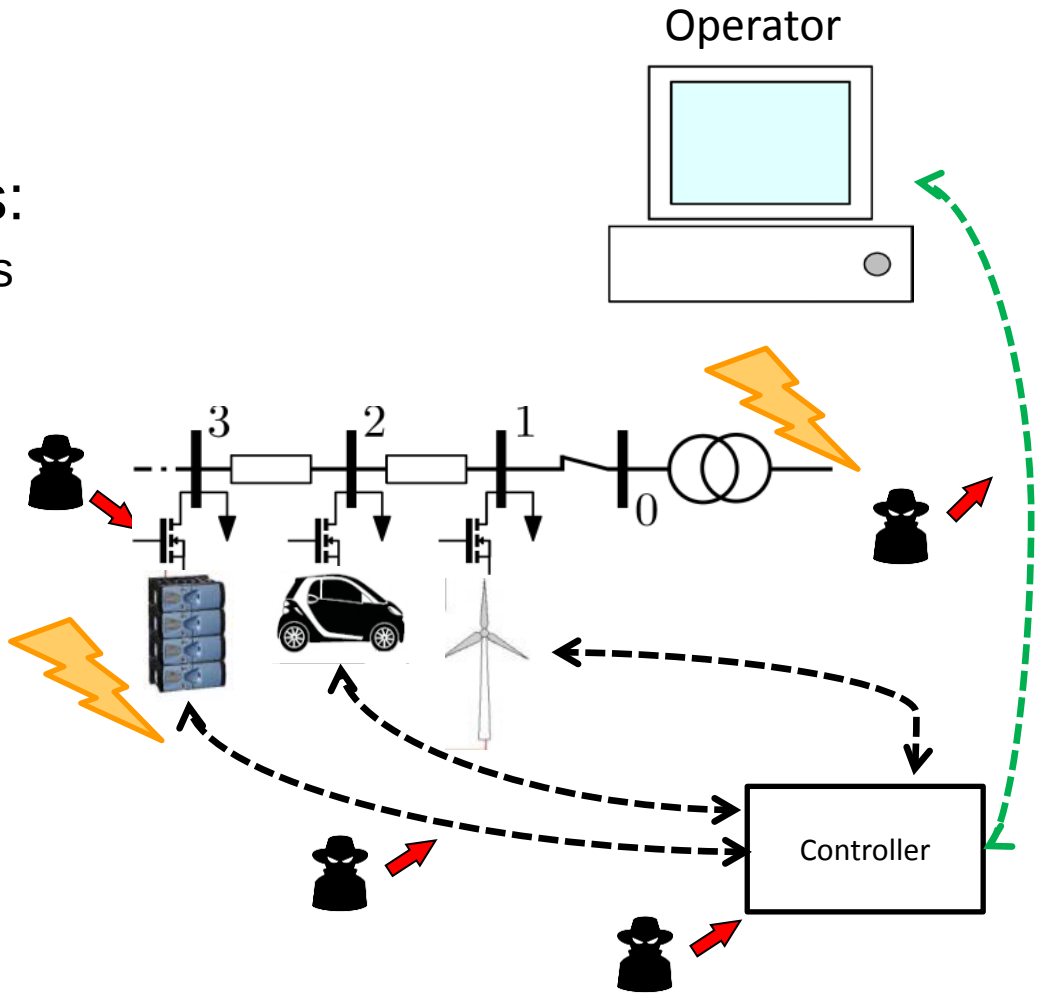


- Distributed Resource Management
  - What sensors / actuators to use?
  - How to allocate control / estimation effort?

- Fault-Tolerant and Robust Control
  - Ensure safety in spite of failures
  - How can high-risk faults / attacks be mitigated?

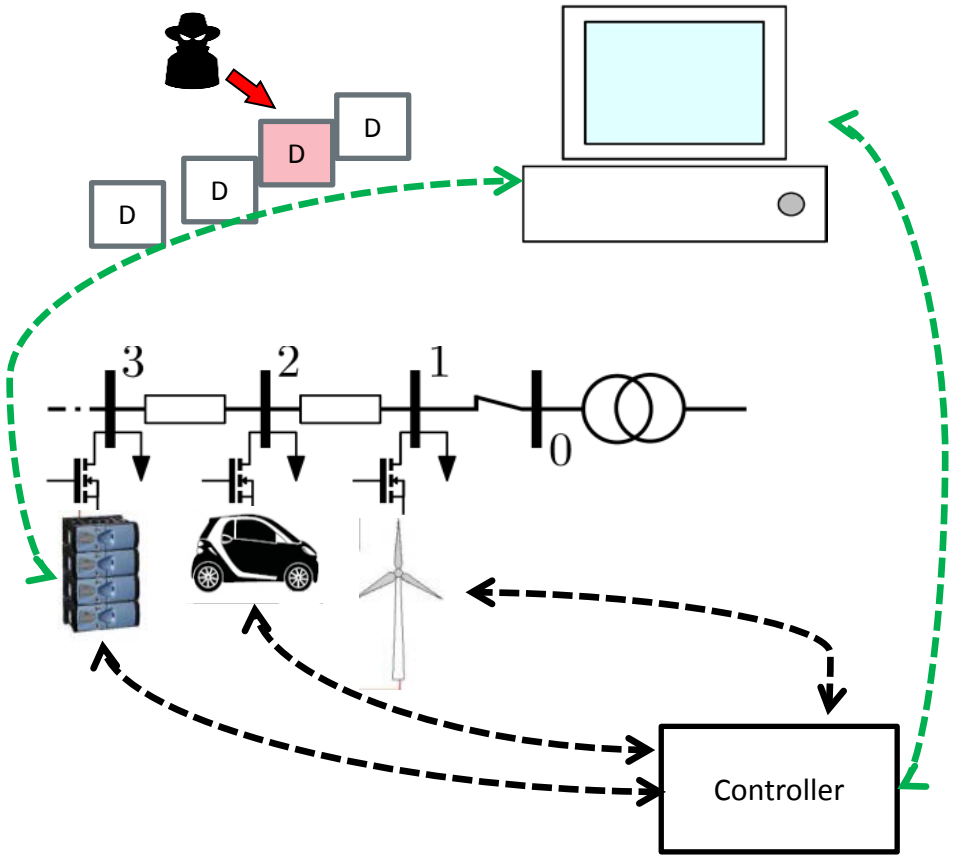
Attack Scenarios

- Potential Adversary Goals:
  - Shut-off critical power-inverters
  - Override control loops
  - Reconfigure controllers
  - Falsify monitoring data
- Potential Consequences
  - Component failure
  - Cascading failure
  - Economical losses



Data-Driven Anomaly Detection

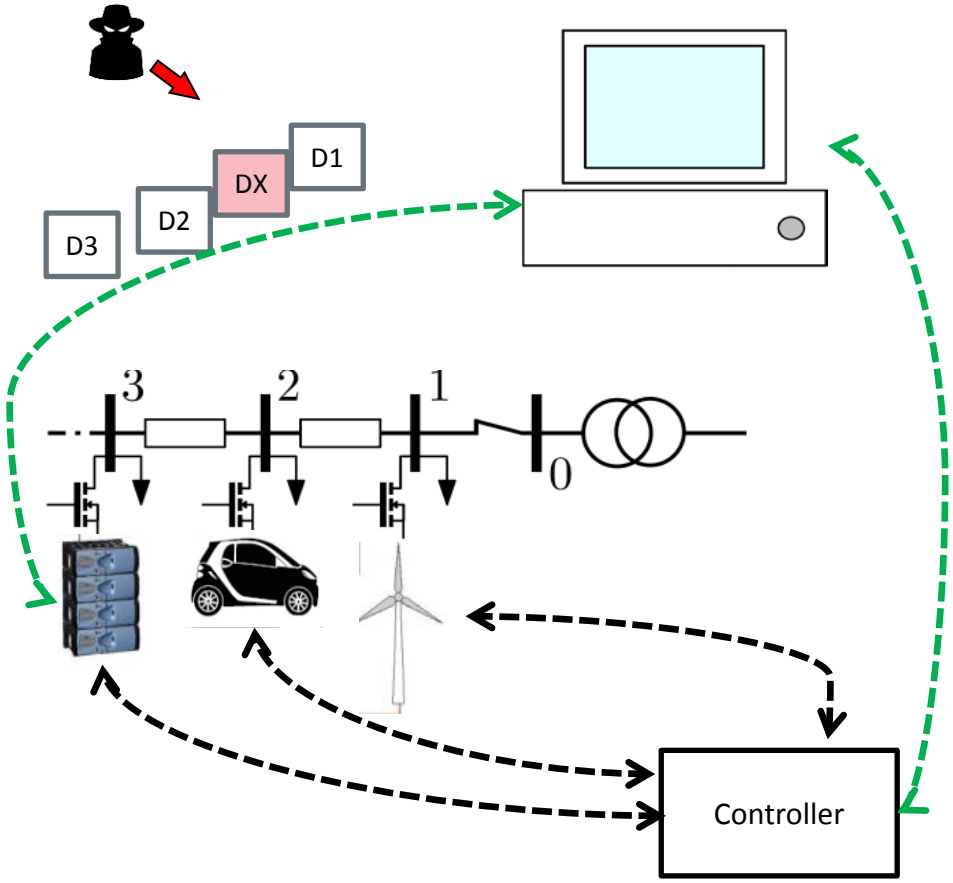
- Learn normal behaviours from historic data
  - Network traffic
  - Power consumption/generation
  - Wind / solar generation profiles
- Include physical laws
  - Three-phase power flows
  - Correlations between variables
- Detect abnormal patterns
  - Unusual data traffic
  - Unusual switching commands
  - Non-conforming data



Formal Anomaly Detection Methods

- SCADA Protocol specification
- Allowed sequences of commands
- Allowed data-exchange

- Detect non-conforming behaviors
  - Unauthorized commands
  - Unauthorized data exchange
  - Non-conforming data traces

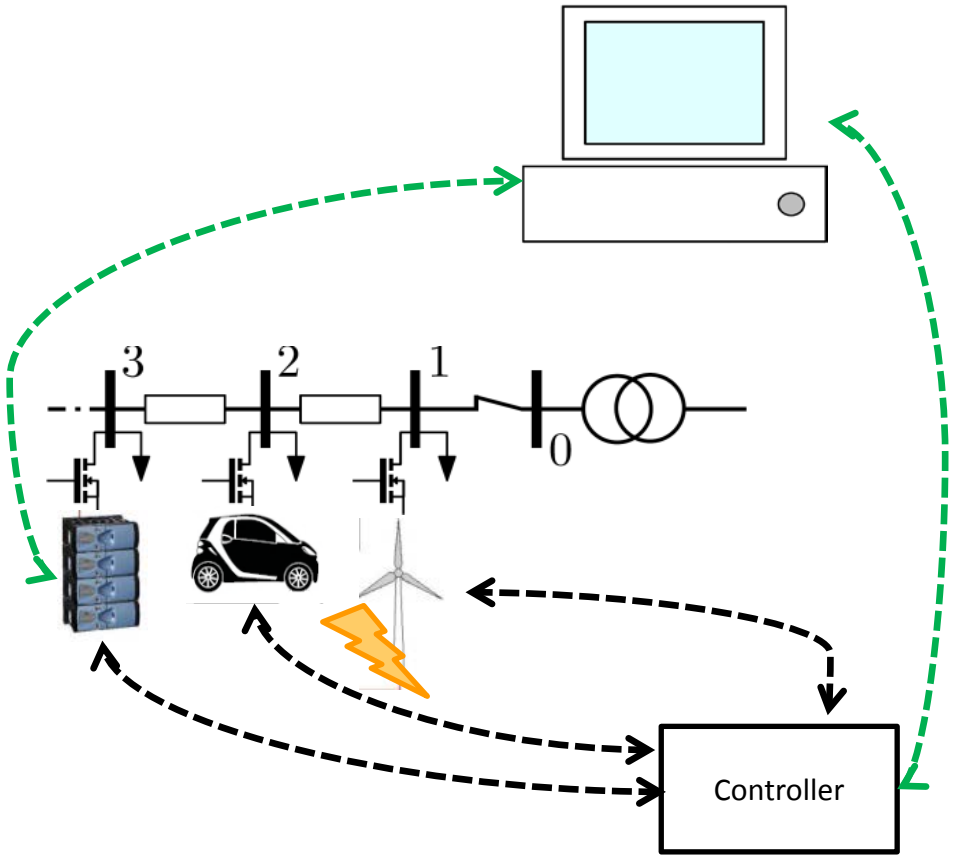


Distributed Resource Management

Threat scenario:

- DER device failure
  - Safety protection (over-frequency / over-voltage)
  - Cyber attack

- **Distributed power compensation**
  - Compute new feasible set-points to maintain power balance
  - Coordination between main grid and several power inverters (battery, wind turbine, electric vehicles)

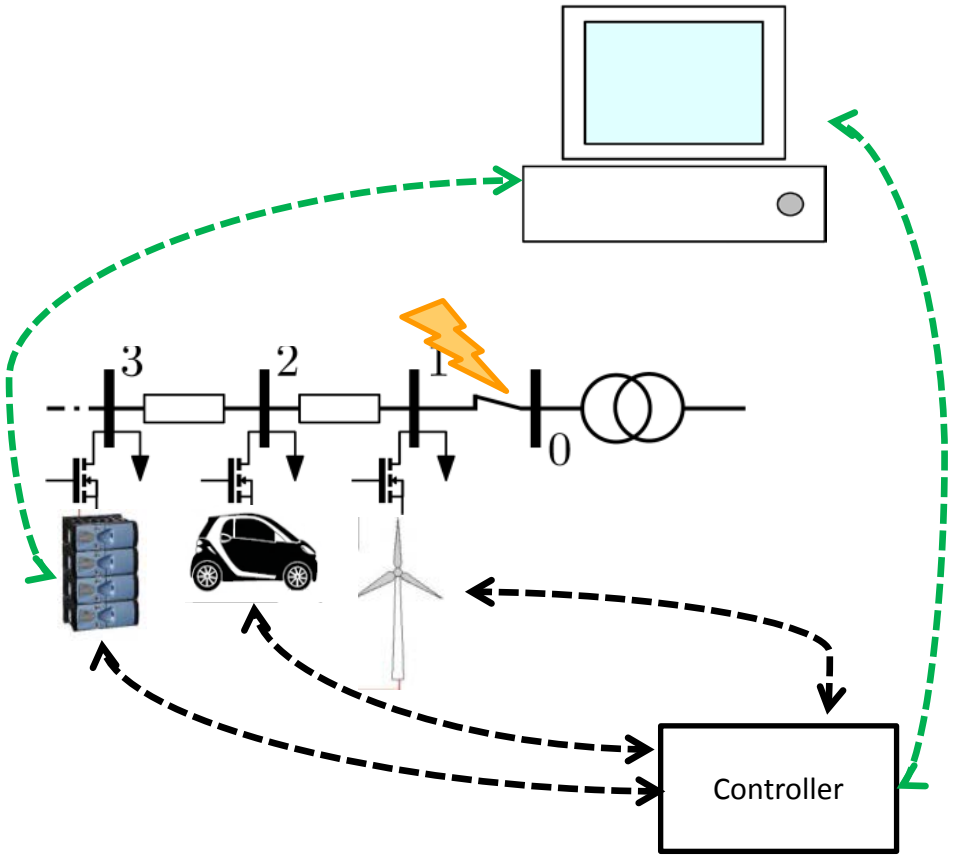


Fault-Tolerant and Robust Control

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Threat scenario:

- Critical DER device failure
  - Disconnection from main grid
- Predictive Control with Contingencies
  - Maintain a N-1 reliability level:
  - ”Meet operational constraints with **at most one component failure**”
  - Ensure computed setpoints satisfy safety coinstraints **under hypothetical failures**



EU FP7 Programme Contract No. 608224

SPARKS: Resilient Smart Grids

- Inputs:
  - Risk assessment
  - Threat scenarios
- Resilient Control Goals:
  - Mitigate risk to increase resilience
- Resilient Control Approaches:
  - Anomaly / Intrusion Detection
  - Distributed Resource Management
  - Fault-Tolerant and Robust Control
- Desired Outputs:
  - Mitigated risk