Cyber-Physical Resilience via Physics-Aware Devices

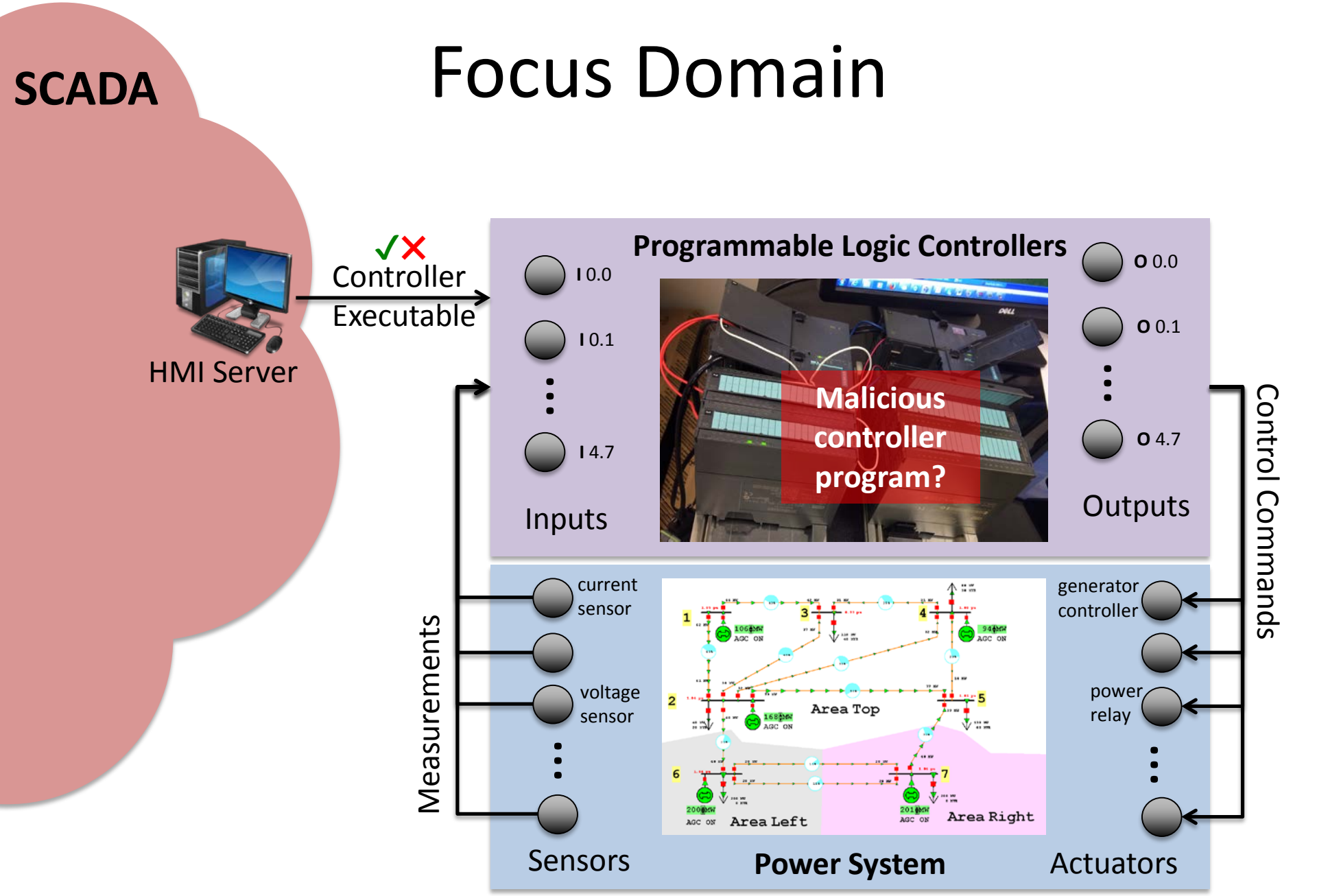
Saman Zonouz

June 2016

RUTGERS

4N6

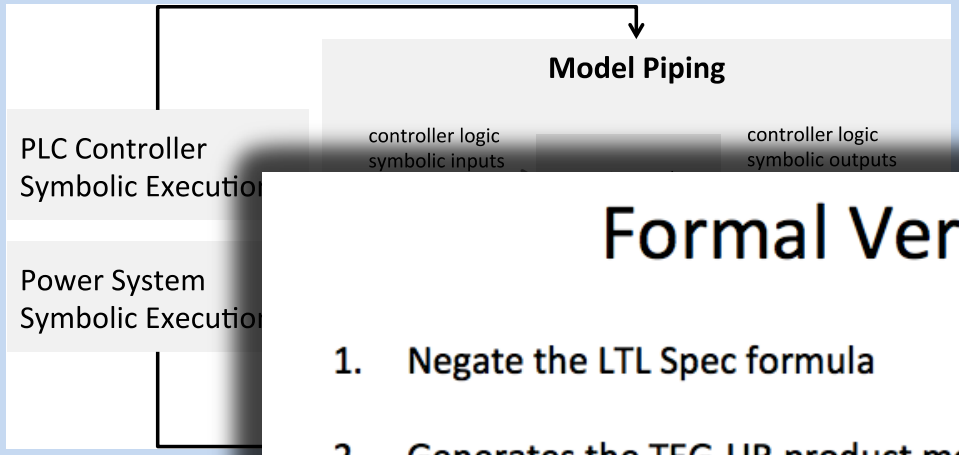
Focus Domain

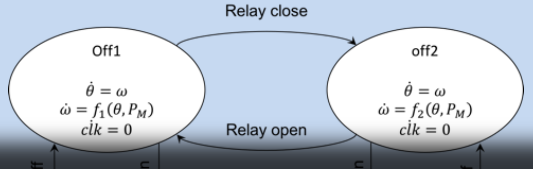


Intermediate level code (ILIL):

Symbolic Scan Cycle:

Generate PLC output safety value constraints automatically





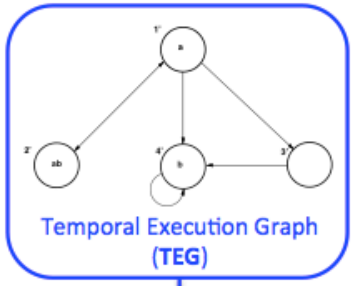
PLC

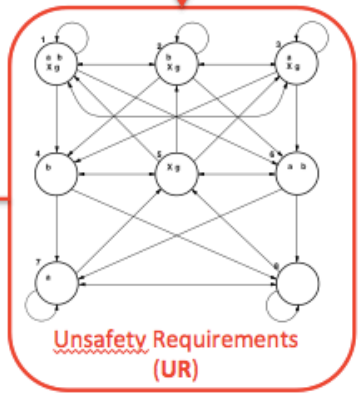
Formal Verification

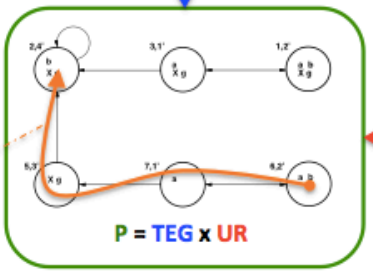
1. Negate the LTL Spec formula
2. Generates the TEG-UR product model P
3. Search for a path in P
4. Get concrete input values

Safety requirements:
! (a_1 **U** a_2)

Negation







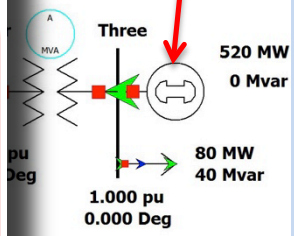
Req-violating input vector:

$(i^0, i^1, i^2) = (10, 2, 15)$

Req-violating path condition:

$(i^0 < 12)$ & $(0 < i^1)$ & $(i^2 < 20)$

$b_{max_{ang}}$ **b**

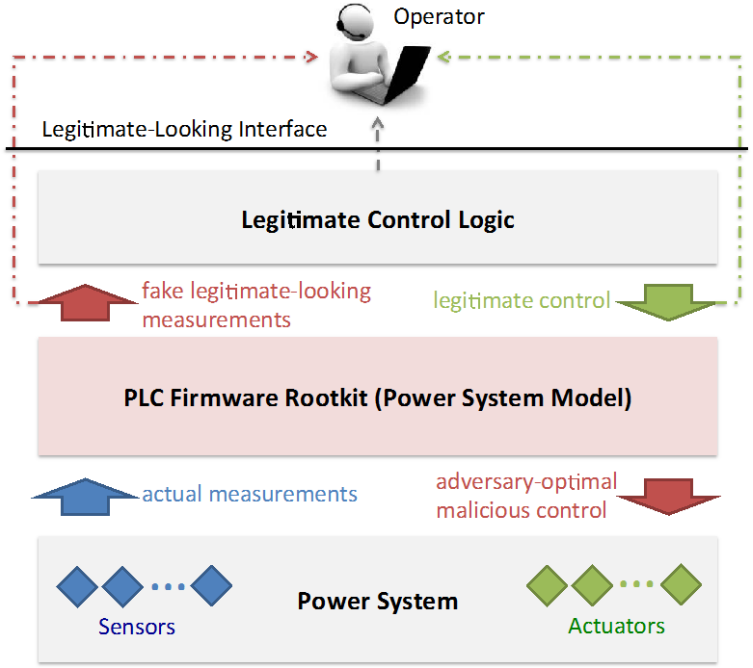


EMS: bus voltage < capacity

Responsible Disclosures

Allen-Bradley PLC Firmware (collaboration with TU-Darmstadt)

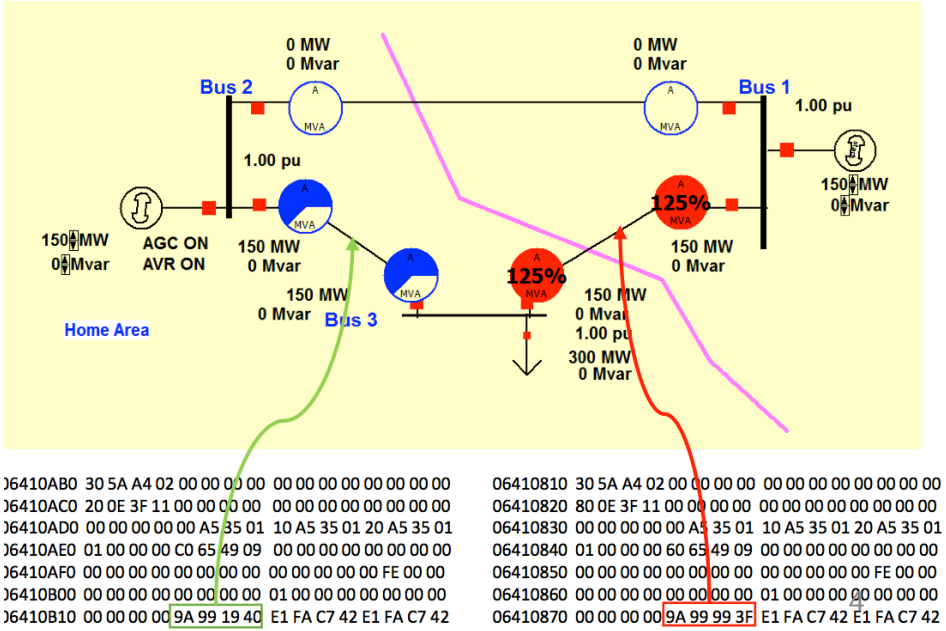
- Physics-aware rootkit damaged physical system
- Faked measurements to the operators to comply with physics



Google and PowerWorld (collaboration with AT&T and MIT)

- Non-control data attacks
- Google $10K –Hall of Fame

Related paper at Phrack 2016.




```
06410AB0  30 5A A4 02 00 00 00 00  00 00 00 00 00 00 00 00
06410AC0  20 0E 3F 11 00 00 00 00  00 00 00 00 00 00 00 00
06410AD0  00 00 00 00 00 A5 35 01  10 A5 35 01 20 A5 35 01
06410AE0  01 00 00 00 C0 65 49 09  00 00 00 00 00 00 00 00
06410AF0  00 00 00 00 00 00 00 00  00 00 00 00 FE 00 00
06410B00  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00
06410B10  00 00 00 00 9A 99 19 40  E1 FA C7 42 E1 FA C7 42
```

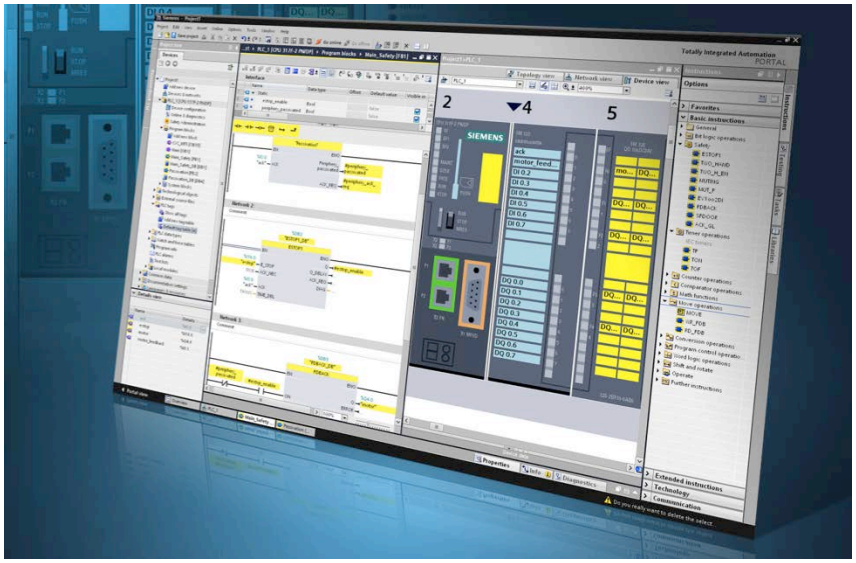
```
06410810  30 5A A4 02 00 00 00 00  00 00 00 00 00 00 00 00
06410820  80 0E 3F 11 00 00 00 00  00 00 00 00 00 00 00 00
06410830  00 00 00 00 00 A5 35 01  10 A5 35 01 20 A5 35 01
06410840  01 00 00 00 60 65 49 09  00 00 00 00 00 00 00 00
06410850  00 00 00 00 00 00 00 00  00 00 00 00 FE 00 00
06410860  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00
06410870  00 00 00 00 9A 99 99 3F  E1 FA C7 42 E1 FA C7 42
```

Technology Transfer (Siemens)

Operator-Side Program Checking

- Siemens TIA-Portal control logic programming IDE

Project sponsored by Siemens



On-Device Safety Monitoring

- Siemens S7-1500 coupled PLCs with on-board coprocessors

Paper at Resilience Week 2016

Practical Feasibility

Offline verification does NOT scale!

Past Work

Offline formal verification and model checking

- Unscalable for large-scale platforms

Runtime monitoring and intrusion detection

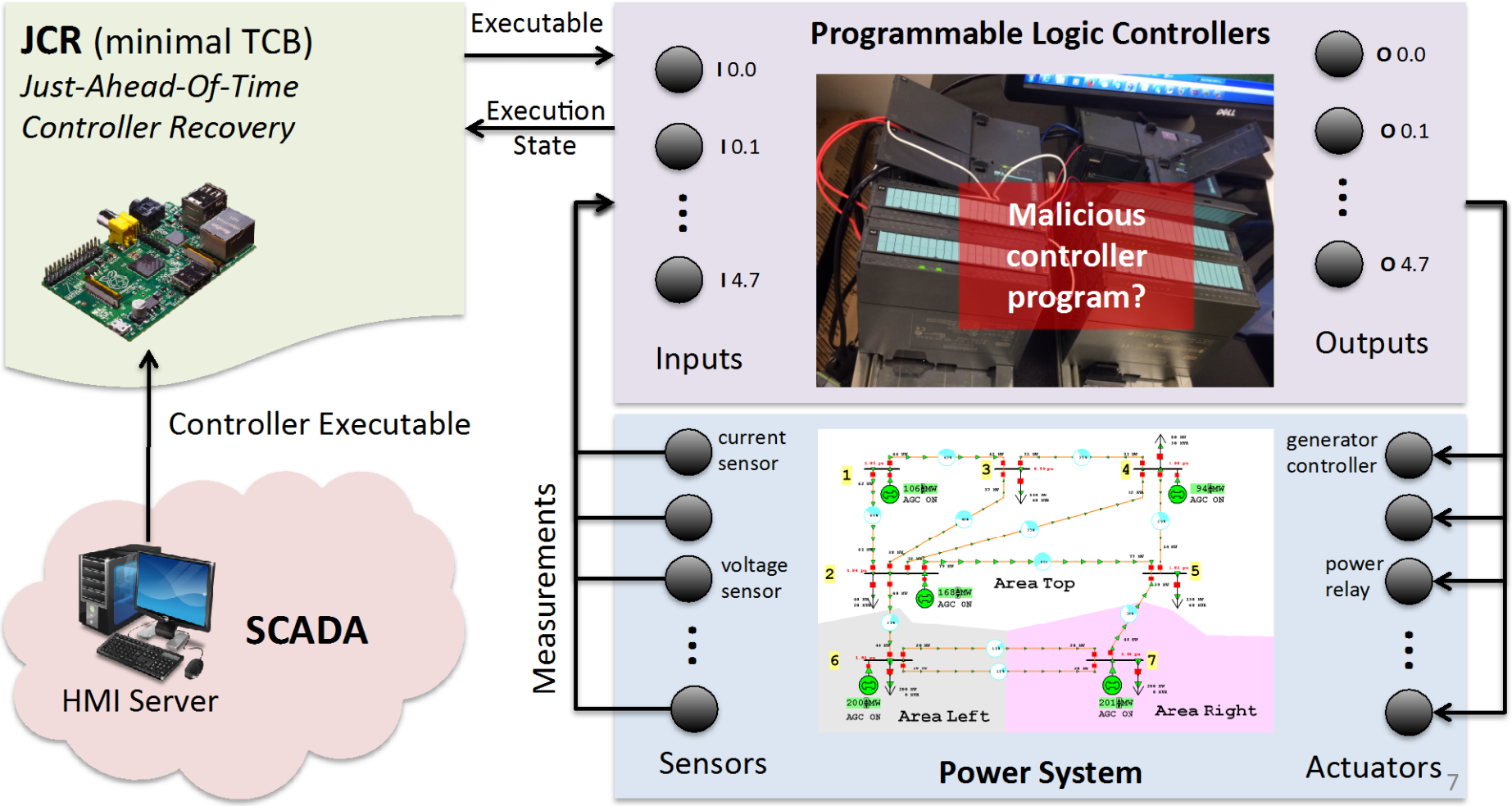
- Too late for effective response and recovery

Our Solution

Just-Ahead-Of-Time Verification and Response

+ Remarkably smaller system models to analyze

+ Sufficient time for timely intrusion tolerance

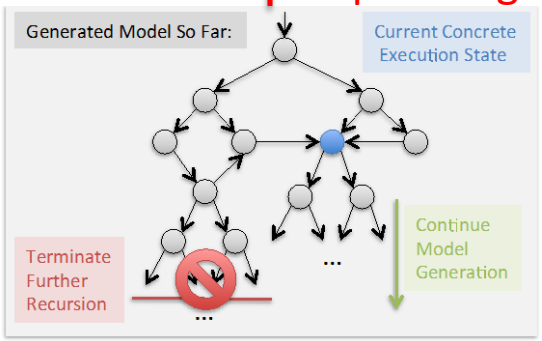


Automated Intrusion Tolerance

- *Objective:* Calculate a remedial control for the PLC before the actual execution catches up with JAT

Upcoming bad state

remedial countermeasure
(RAS control logic)



$$\min_{\mathbf{u}} \quad f(\mathbf{x},\mathbf{u})$$

$$\text{s.t.} \quad P_i^g - P_i^l = \sum_k |V_i||V_k|(G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik})$$

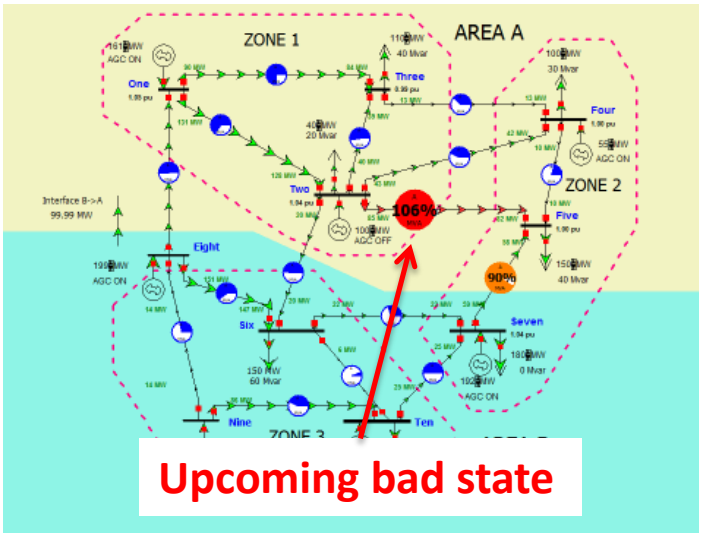
$$Q_i^g - Q_i^l = \sum_{k\in C} |V_i||V_k|(G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik})$$

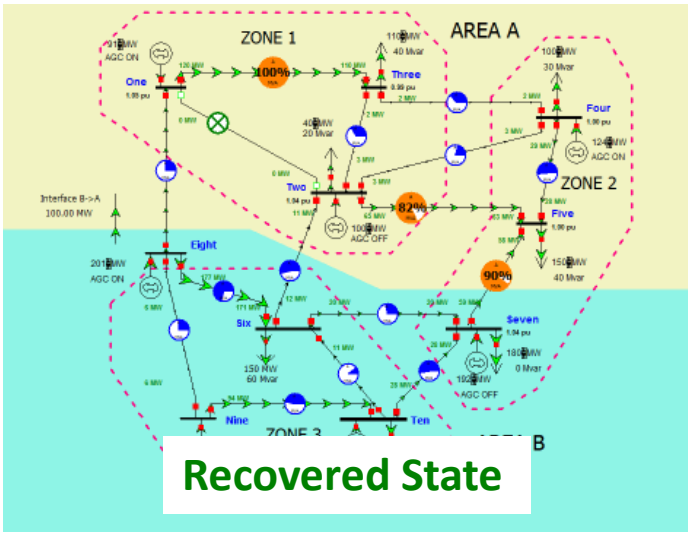
$$MVA_{ij} \le MVA_{ij}^{max}$$

$$P_l^g \le P_l^{gmax}$$

$$\forall i,j \in N,\ \forall l \in G,\ \forall k \in C$$

PLC*





Concluding Remarks

- **Optimal control vs. safety redlines**
  - *reject the **control** that **violate** the power system **safety** requirements*
  - *replace them with security/safety-preserving **countermeasures***

- **Minimal** trusted computing base for infrastructural **resilience**
  - ***easier to analyze**, verify its correctness, and **protect** its cyber-security*
  - *guarantee **safety** while **"huge"** SCADA solves for the **optimal plant control***

- **Just-Ahead-of-Time** verification allows for countermeasure **selection**
  - ***proactive** tolerance to prevent **too-late responses***
  - ***learns** decided-upon responses for later **similar** unsafe states*

Saman Zonouz saman.zonouz@rutgers.edu Thank You!