U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Cyber Resilient Flexible Alternating Current Transmission Systems ABB Inc

Reynaldo Nuqui

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Cyber Resilient Flexible AC Transmission Systems (XFACTS)

Objective

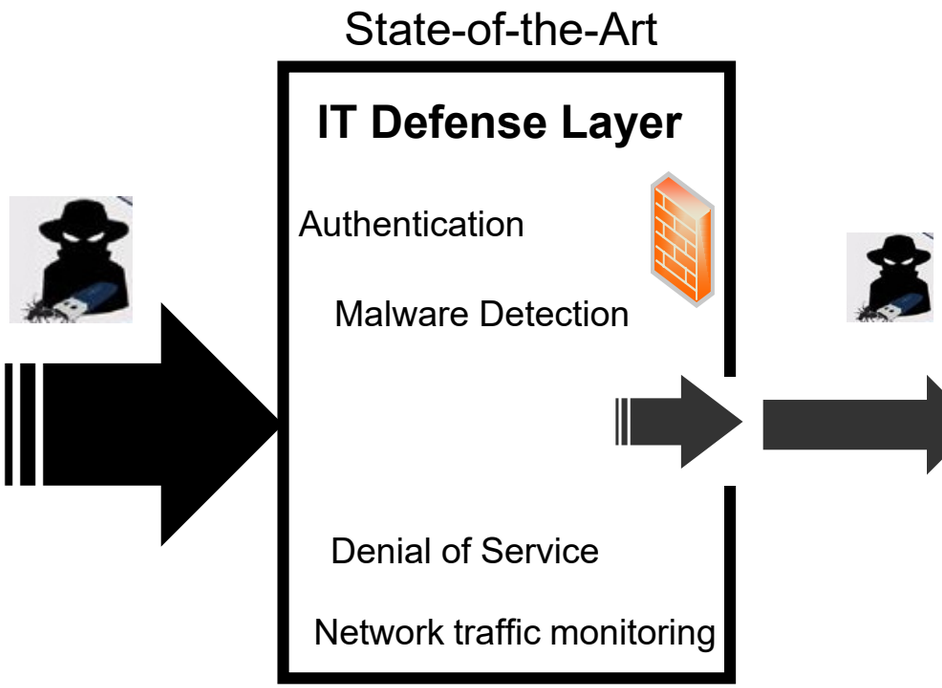
- The objective is to develop domain-based methods for defense-in-depth cybersecurity solutions of Flexible Alternating Current Transmission Systems (FACTS). We address the vulnerabilities associated with insider attacks on FACTS control systems, such as with syntactically correct malicious commands and measurements. Opportunities exist to extend FACTS controls into cybersecurity. The main technical challenge is designing controller extensions that meet the speed requirements of the operational process being secured. We plan to use state estimation to secure against false data injections; look ahead simulation to secure against malicious commands; and Time Failure Propagation Graph and Markov process for intrusion detection and controller failure prognosis. We will leverage the unique dynamic response of FACTS devices, such as through probing signals or simulations to identify and alert operators of any malicious cyber commands and measurements acting on the FACTS device. We will develop cybersecurity solutions for distributed FACTS systems interacting with Wide Area Measurement, Protection, and Control (WAMPAC) and with supervisory control and data acquisition (SCADA)/Energy Management Systems (EMS). Matrix Pencil Method will be used to secure against man-in-the middle attacks in wide area-controlled FACTS. Variational mode decomposition (VMD) technique with decision trees (DT) and moving target defense to secure Wide Area Voltage Controlled FACTS. The developed methods shall be tested using various FACTS devices, such as Static Var Compensators (SVC), Series Capacitors (SC), Static Compensators (STATCOM), and Thyristor Controlled Series Compensators (TCSC).

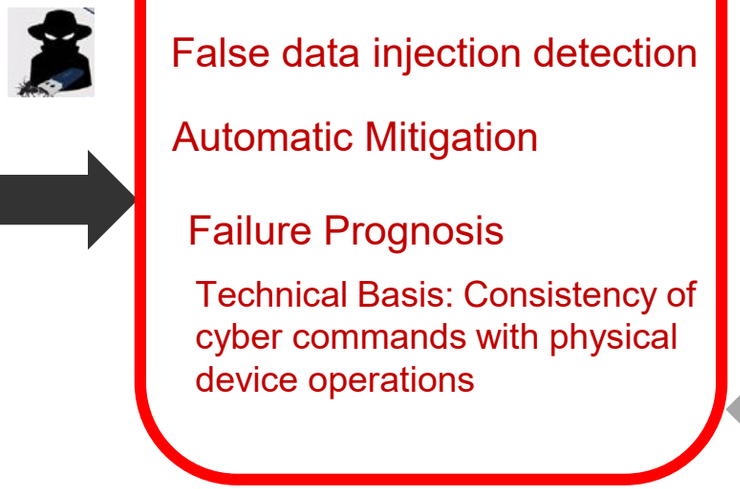
Schedule

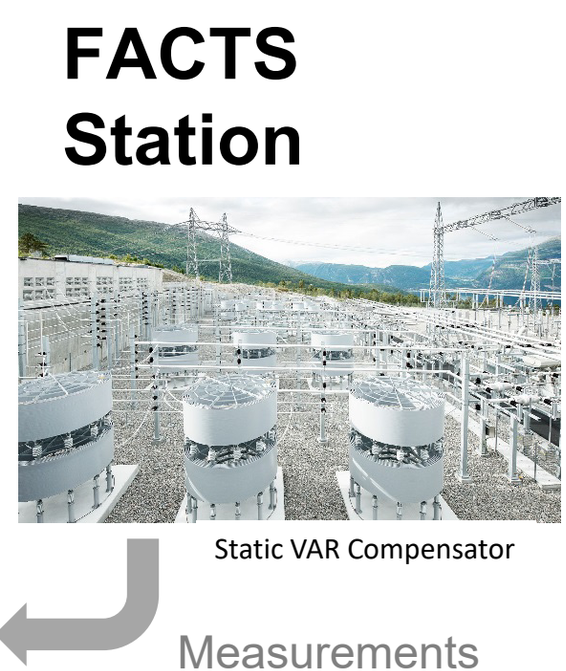
- January 2019 – Sept 2021
  - FACTS System threat models – 12/4/2019
  - Cyber defense mechanisms concepts developed and validated – 9/30/20
  - Cyber security functions prototyped and tested – 3/31/2021
  - Red Team Testing completed – 5/15/2021
  - Utility Demonstration – 8/15/2021
  - Publications, panel sessions, industry and standard engagement for knowledge dissemination – 9/30/2021

Total Value of Award:	**$ 3,235,021 ($744,241 (cost share) + $2,490,780 (federal share))**
Funds Expended to Date:	**28.8% (Total Project) [($931,240/$3,235,021) *100] 26.1% (Federal Share) [($650,915/$2,490,779) *100]**
Performer:	**ABB Inc.**
Partners:	**ABB Enterprise Solutions Inc. University of Illinois, Urbana-Champaign Iowa State University Utility (TBD)**

Advancing the State of the Art (SOA)







- State of the art in FACTS systems cyber security is largely based on IT defense tools

- Feasibility: XFACTS uses domain-based cybersecurity extensions to FACTS controllers to defend against inside threats

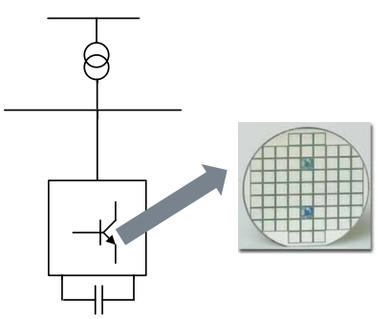
- Compared to SOA our approach is real-time, power system awareness, and capable of securing and mitigating cyber attacks, in progress, on FACTS controllers without interrupting operations.

Advancing the State of the Art (SOA)

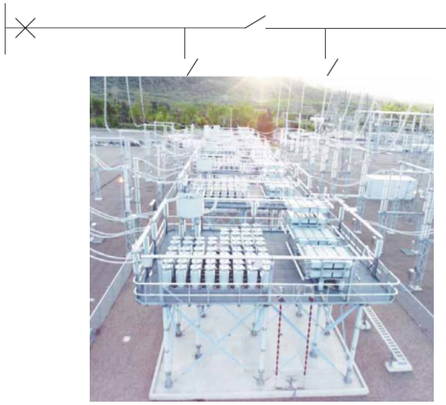
- Benefit to end user. The end users (asset owners, operators, utilities) will benefit from the increased reliability and security of FACTS operations

- Advancing Cyber Security of Energy Delivery Systems 1) increased resiliency against insider threats to FACTS systems 2) maintain FACTS continuity of service during on-going attacks 3) automatic mitigation of threats through blocking 4) increased situational awareness of cyber activities with visualization

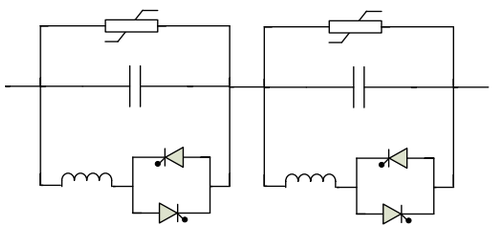
- Potential for sector adoption: 1) XFACTS addresses asset operators needs for defense-in-depth security 2) quick deployment as extensions to existing controllers 3) no additional instrumentation required 4) designed not to impede speed or dependability of FACTS controllers



STATCOM



Series Capacitor



TCSC

Progress to Date

Major Accomplishments

- Milestones achieved

- Milestone 1: NDAs with industry partners are signed – 4/1/2019
- Milestone 2: Threat model defined – 12/4/2019
- Milestone 3: Concepts for cyber defense mechanisms of FACTS Station developed and validated – 9/30/2020 (target)
- Milestone 4: . Concepts for cyber security of distributed FACTS systems developed and validated – 9/30/2020 (target)

- Key Discoveries

- Singh, Govindarasu, Nuqui *Impact Analysis of Stealthy Cyber-Attacks on FACTS-based Wide-Area Voltage Control System,* submitted to the ISGT 2021 Conference
- Singh, Govindarasu, Nuqui, *Data-Driven Attack-Resilient System for FACTS-based Wide-Area Voltage Controller,* to be submitted to the IEEE Transactions on Smart Grids

Challenges to Success

Impact of Covid-19 on timing of utility demonstration and prototyping work

- Remote connection to the hardware-in-the loop test bed.

Utility Partner

- We are currently negotiating with a utility to be our demonstration partner

Resource constraint due to resignation and/or RA students graduating

- We hired new scientists to increase resource count. Academic partners to ensure that research assistants are fully committed. Currently negotiating with the University of Idaho to join the project.

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

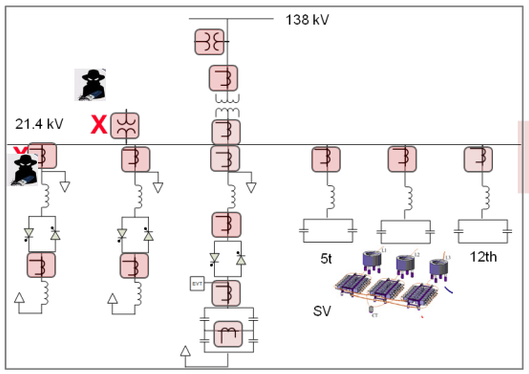
- What category is the targeted end user for the technology or knowledge? (e.g., Asset Owner, Vendor, OEM)
- The end user will be an asset owner, such as an electric utility or industrial customer, with the technology developed and sold by the FACTS vendor
- What are your plans to gain industry acceptance?
  - Demonstration set up shall consist of Real Time Digital Simulator (RTDS), FACTS controllers with prototyped cyber security functions, connected in a hardware-in-the loop to emulate performance in field installations. The testing shall be done in the partner utility's research laboratory or a FACTS substation, in the presence of cyber security and operations experts and personnel, from DOE, the utility partner, academic partners, and the vendor.
- What is the timeline for demonstration and sector adoption?
  - The demonstration is planned to be held in August 2021. Plans are in place to align the technology to the vendor's FACTS product roadmap

Next Steps for this Project

Approach for the next year or to the end of project

- Key Milestones to accomplish
- Milestone 5: Implemented and prototyped cyber defense mechanisms for FACTS station – 3/30/2021
- Milestone 6: Implemented and prototyped cyber security functions of distributed FACTS systems – 3/30/2021
- Milestone 8: . Red team testing completed – 5/15/2021
- Milestone 9: Utility demonstration finished – 8/16/2021
- Upcoming significant events
  - Demonstration is planned to be held in August 2021

Cybersecurity of sensor data in FACTS stations



Measurement placement in an SVC station

1. State Estimator

FACTS Digital Model

State Estimation Engine

$$\boldsymbol{I} = \boldsymbol{h}(\boldsymbol{V}) + \boldsymbol{e}$$

$$(\boldsymbol{H}^T(\boldsymbol{x}^v)\boldsymbol{R}_z^{-1}\boldsymbol{H}(\boldsymbol{x}^v))\Delta\hat{\boldsymbol{x}}^v = \boldsymbol{H}^T(\boldsymbol{x}^v)\boldsymbol{R}_z^{-1}\Delta\mathbf{z}(\boldsymbol{x}^v)$$

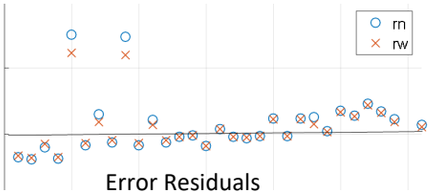
$$\hat{\boldsymbol{x}}^{v+1} = \hat{\boldsymbol{x}}^{v+1} + \Delta\hat{\boldsymbol{x}}^v$$

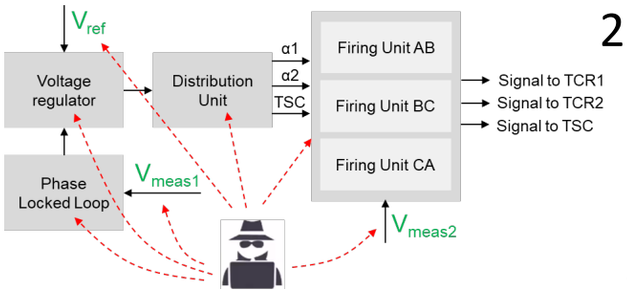
Hypothesis testing

Malicious measurements → X

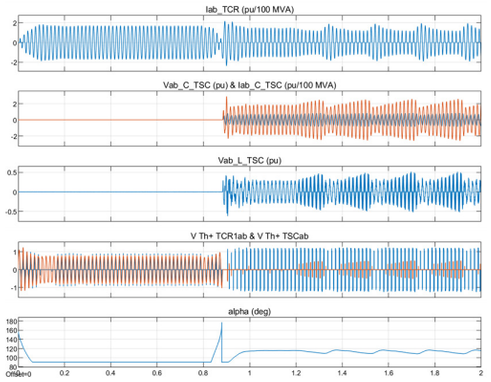
X

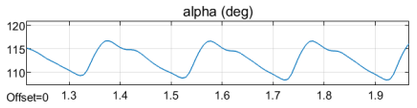
Faulty measurements





2. Thyristor Misfiring Security





- Periodic α change could be an indicator of stealth attack;
- α sis an input to the cyber security function

Repetitive mild attack (stealth attack) on the voltage measurement:

- Can cause overcurrent or overvoltage on SVC components
- Repetitive stealth attack could over stress SVC components and expedite their degradation, resulting in an unexpected failure of the components and/or station outage

Attack vectors: false data injection, malware, controller configuration attack. Attacks are stealthy and could not be detected by controller

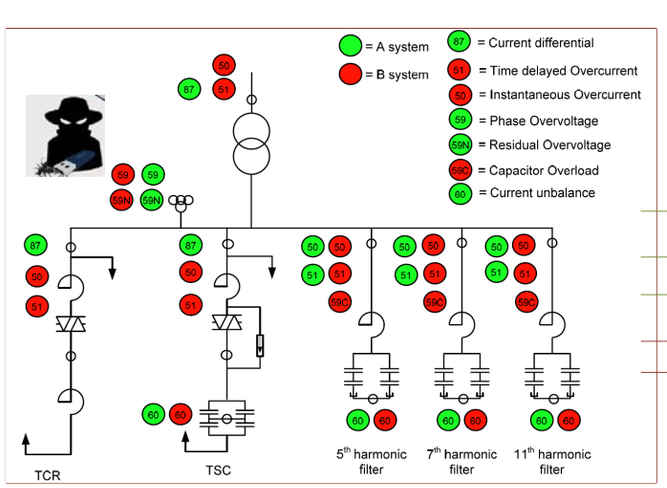
Our solution: 1) Real time streaming state estimation to identify singular or simultaneous attacks on control data, 2) consistency of the firing angle with system conditions

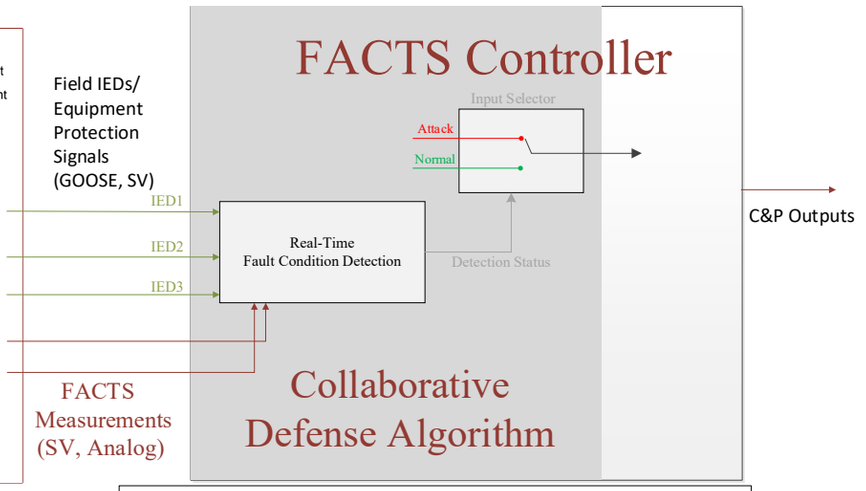
Feasibility: The functions are realized as algorithm extensions to the existing FACTS controllers. Thus, they can be deployed as simple software upgrade to the FACTS control systems

U.S. DEPARTMENT OF ENERGY
OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Security against malicious commands and measurements in FACTS stations

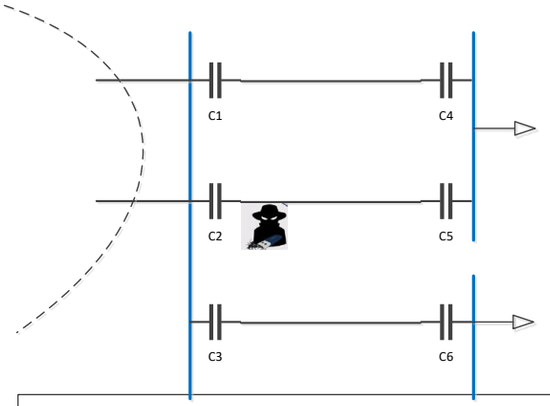
1. Collaborative defense of FACTS in IEC 61850 environment

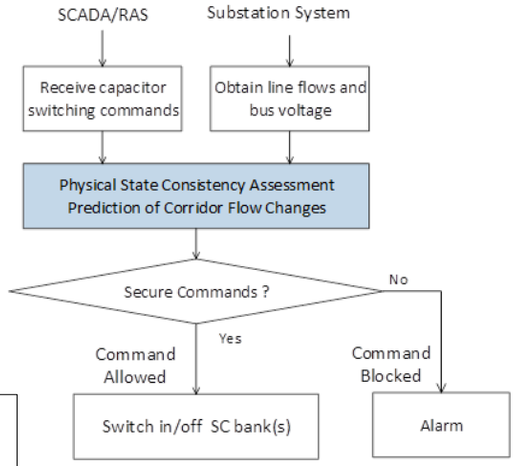




External trip commands are independently confirmed using other measurements in the FACTS station

2. Security of Series Capacitors





Security enhancement of series compensated transmission corridor

a. *Capacitor bypass commands will be blocked if power flow in remaining monitored line(s) is predicted to exceed operational thresholds*

b. *Interlocking scheme blocks successive bypass and insertion operations.*

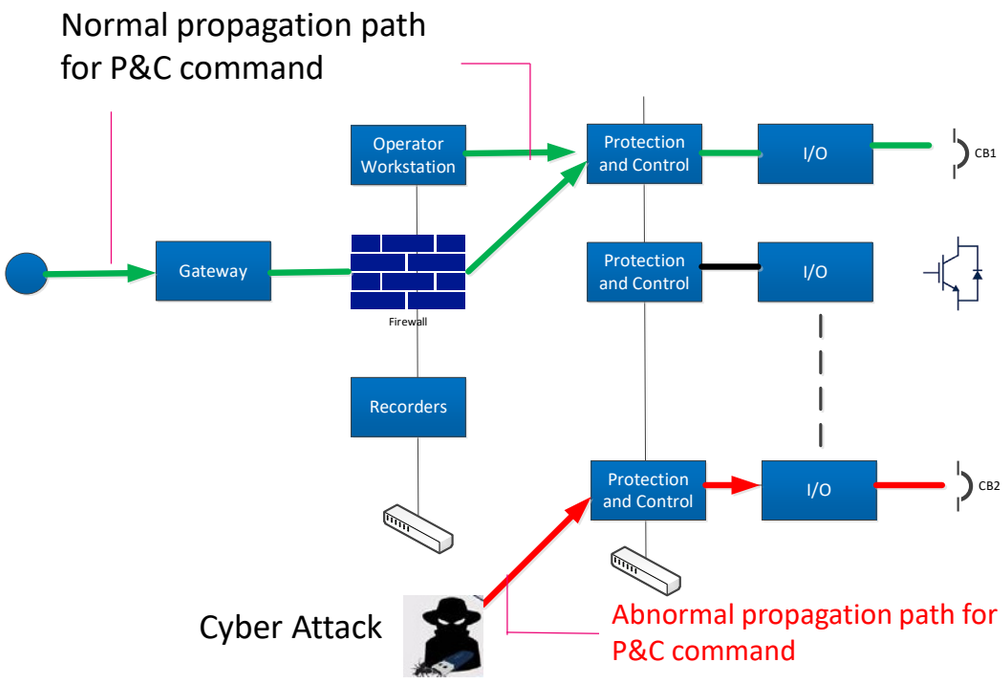
Attack vectors: Attacks are stealthy and could not be detected by existing FACTS controllers

1. False data injection, malicious trip commands, malicious GOOSE.
2. malicious capacitor switching command

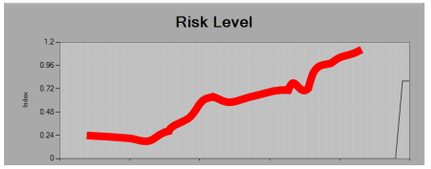
Feasibility: Deployment as simple software upgrade to the FACTS control systems

1. The collaborative defense functions are realized as algorithm extensions to the existing IEC 61850 compatible FACTS controllers.
2. The blocking and interlocking schemes could be realized as extensions to existing FACTS controllers

Cyber monitoring and failure prognosis in FACTS Stations

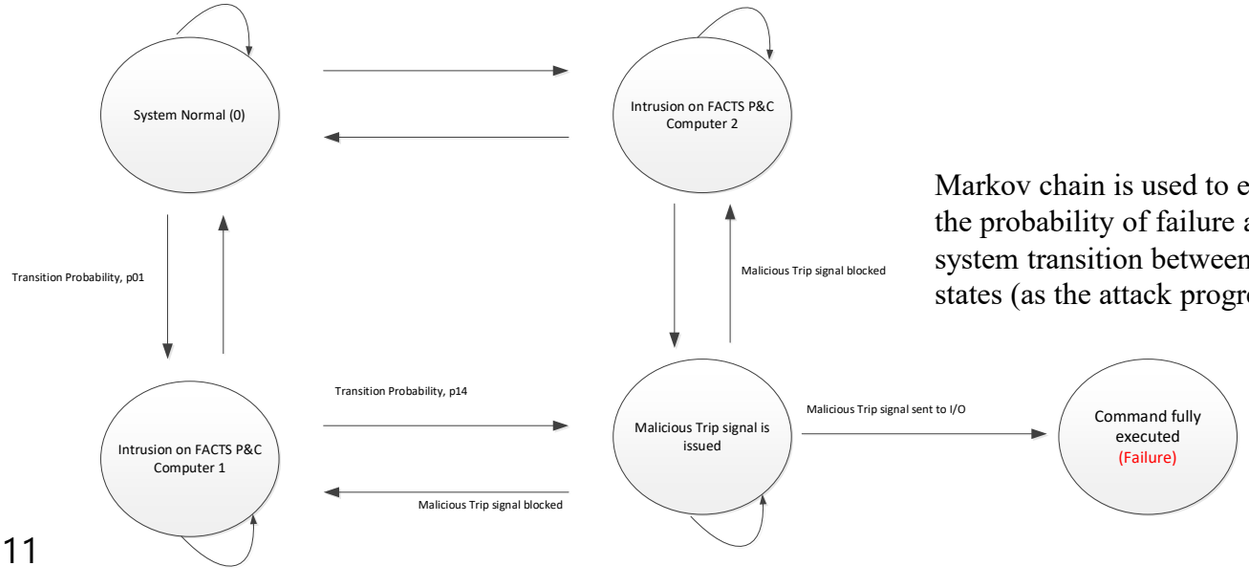


Risk level of intrusion is updated as the malicious command is propagated towards the I/O devices.



The propagation path is mapped into a Time Failure Propagation Graph

If the command does not follow a defined propagation path, it will generate a discrepancy between normal operation and flagged as a cyber intrusion.



Markov chain is used to estimate the probability of failure as the system transition between the states (as the attack progresses)

Attack vectors: Attack on FACTS control and/or protection signals

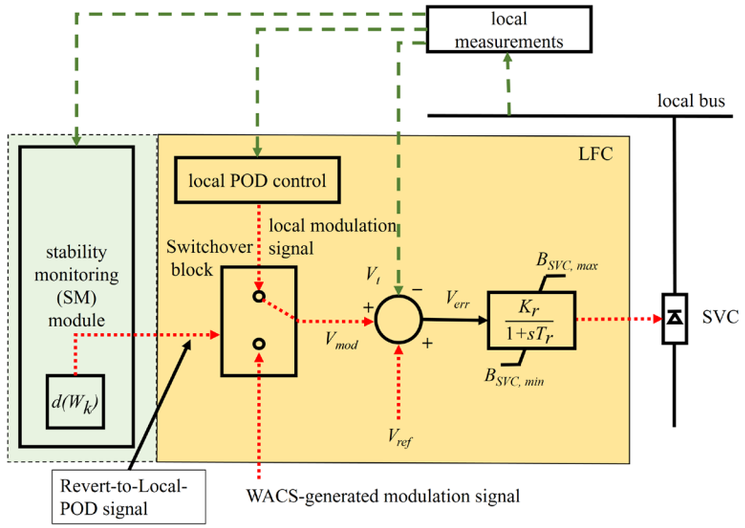
Our solution: 1) Consistency of command propagation paths using time failure propagation graphs. Markov models for describing risk propagation and failure prognosis

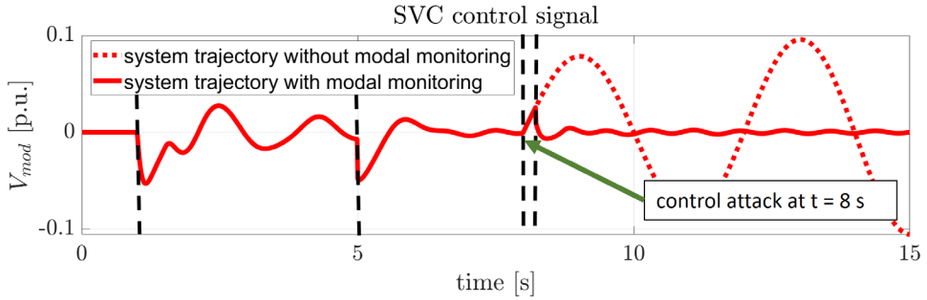
Feasibility: The functions could be deployed as extensions to the station security monitoring system and extensions to the existing FACTS controllers.

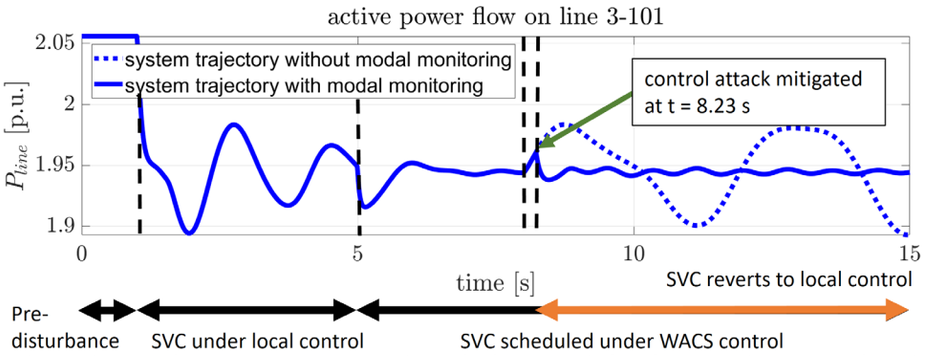
Secured Power Damping in Wide Area Controlled FACTS – University of Illinois at Urbana Champaign

1. SVC damping controller with SM security extension

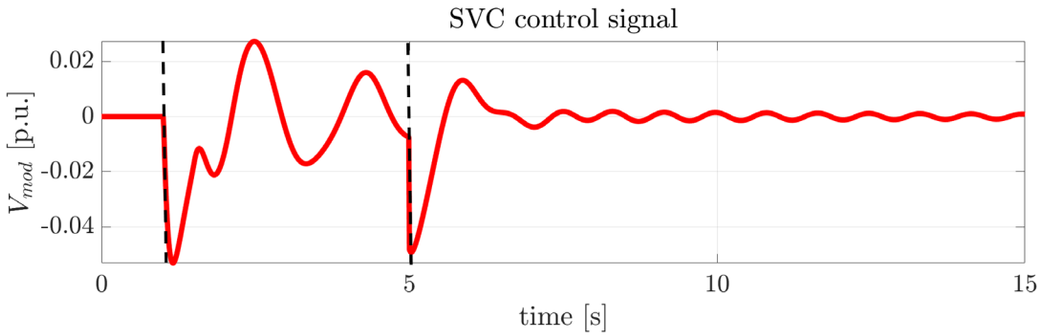
Man-in-middle attacks directed at the modulation signal of FACTS that are controlled by Wide Area Control (WAC) Systems

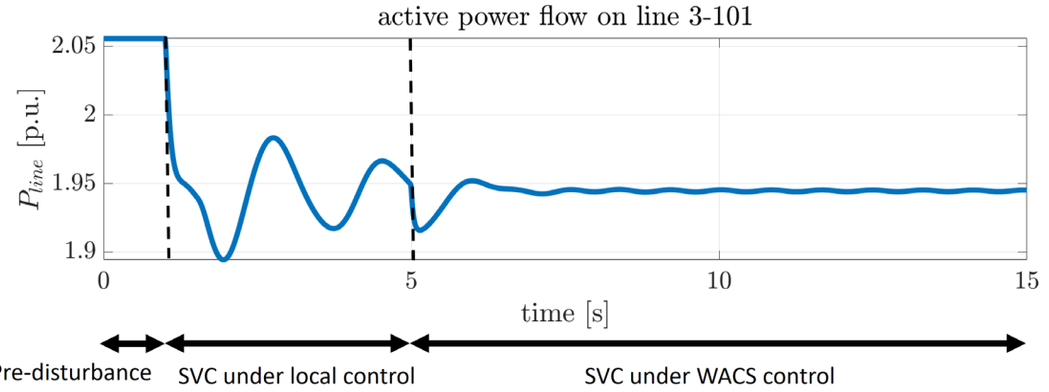






3. POD when compromised, but with detection and mitigation





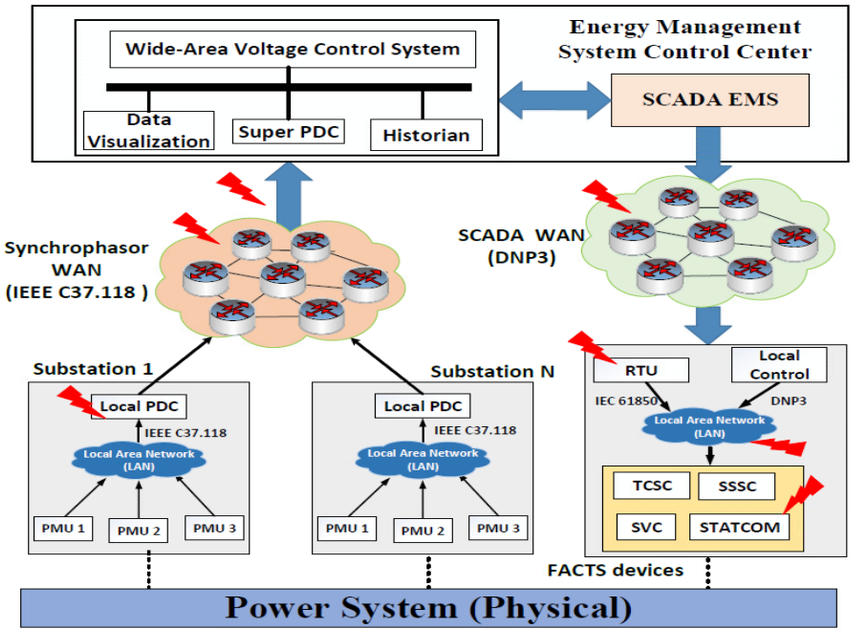
2. POD when uncompromised

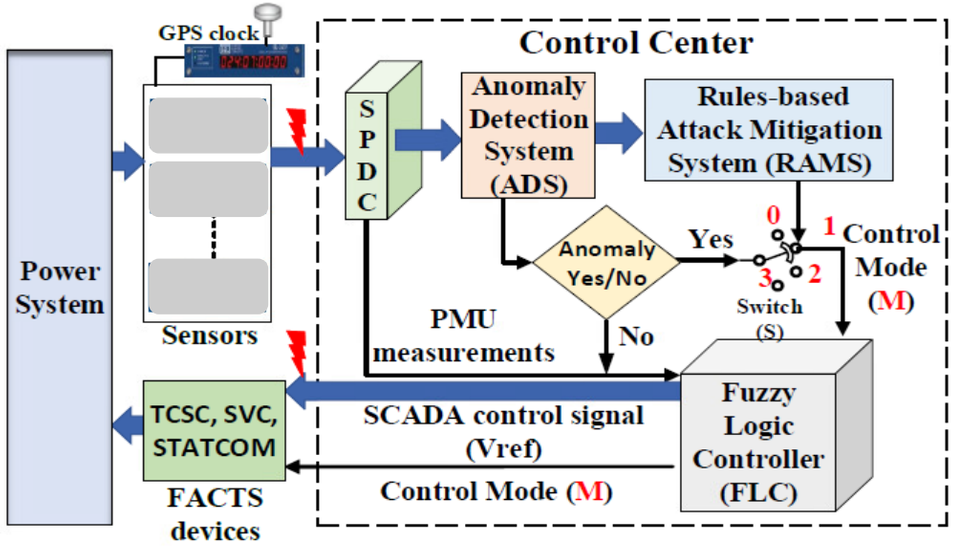
- Modal monitoring of 0.5 s data window
- Detection achieved in 0.23 s from injection

This approach is localized, does not carry the risk of opening more attack surfaces, and implementable at each FACTS device on an individual basis.

Attack-Resilient Wide Area Voltage Control with FACTS - Iowa State University (ISU)

Attack surface in FACTS-based WAVCS





13 **Proposed attack-resilient architecture for WAVCS**

Proposed Attack-Resilient Algorithm

- A Data-Driven Attack-Resilient System (DARS) is proposed by integrating machine learning-based anomaly detection system (ADS) with rules-based attack mitigation system (RAMS).
- Anomaly detection system (ADS): A novel methodology is proposed by applying variational mode decomposition (VMD) technique with decision tree (DT) algorithm using PMU measurements.
- Rules-based attack mitigation system (RAMS): Defines different mode of operations (local or replay mode) to provide necessary mitigations.
- The proposed DARS operates in inline with the fuzzy logic-based WAVCS in real time.

Performance of different machine learning classifiers

Classifier	Accuracy (%)	Processing Time (microseconds/PMU frame)
Decision Tree (J48)	97.4518	6.2
SVM	80.085	10.27

Key Results

The proposed ADS (decision tree) shows an **accuracy rate of 97.45%** while exhibiting a small processing time (6.2 microseconds/per frame).
Also, the proposed RAMS showing promising performance in mitigating disturbances during attacks.