

CAPER

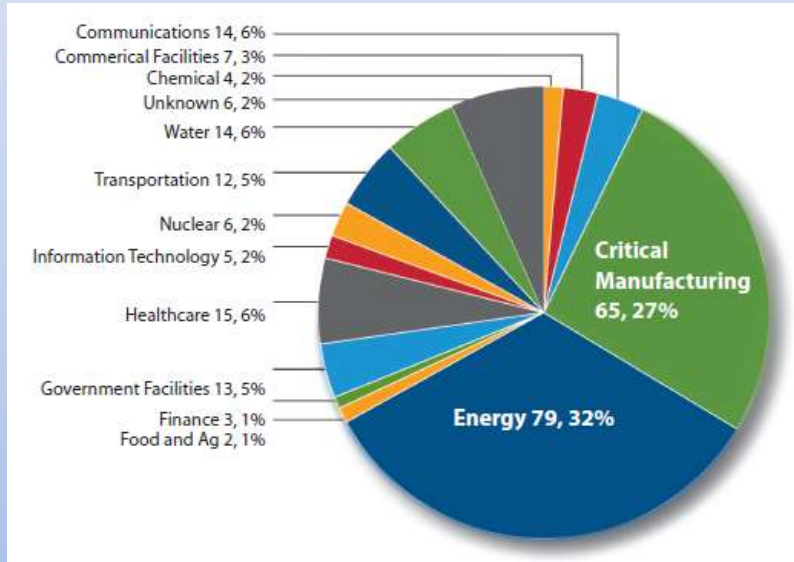
Integrated Data Management for Anomaly
Detection and Cyber Vulnerability Assessment
(Sub-area: Data Management, Analytics, and Security)

Presented By:

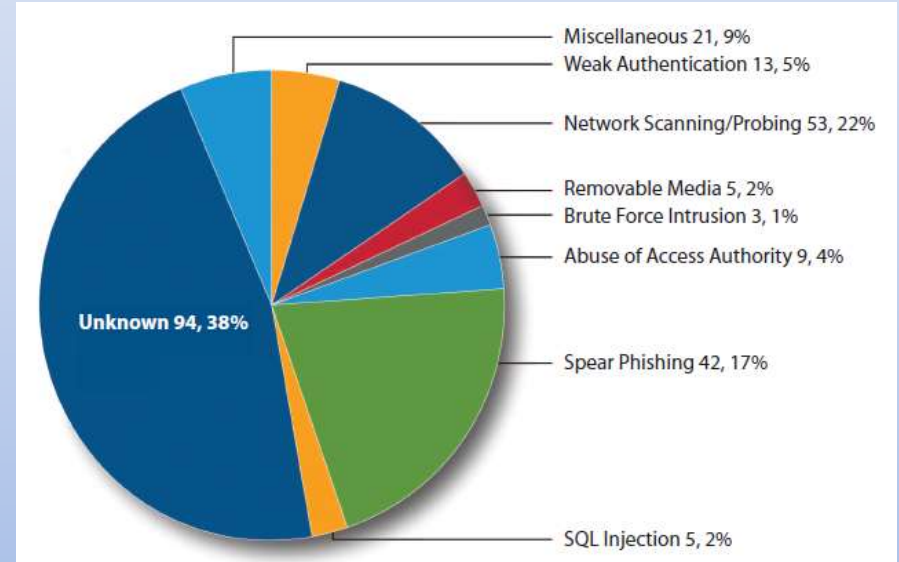
Dr. Madhav Manjrekar and Dr. Rudy Shankar
University of North Carolina – Charlotte

Dr. Ning Lu and Dr. Aranya Chakraborty
North Carolina State University

Motivation



Energy sector tops US industries under attack




ICS-CERT reported 245 incidents

Overarching Approach: More than “being compliant”

Project 2008-06 Cyber Security Order 706

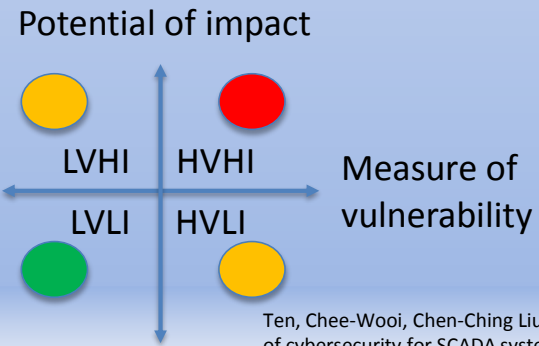
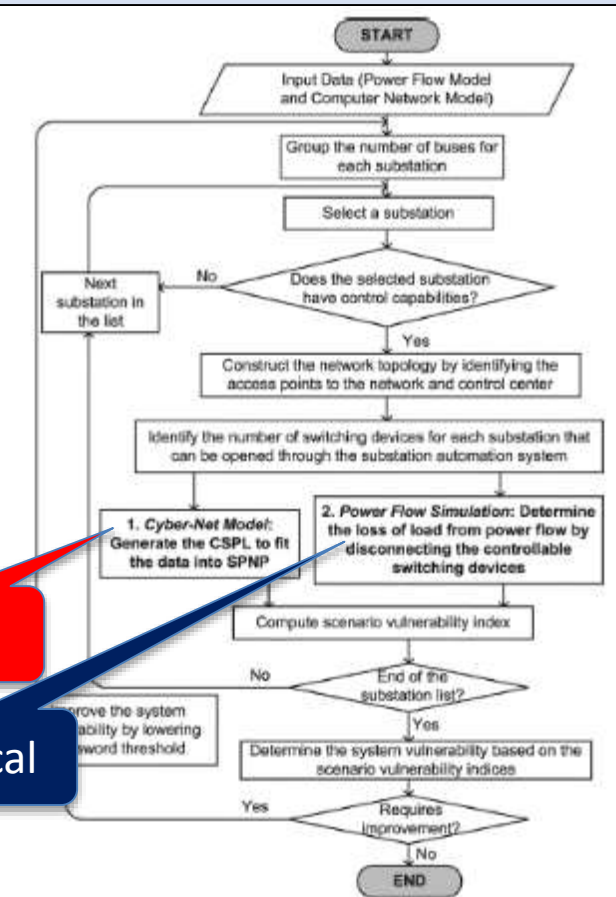
Project 2008-06 Cyber Security Order 706

Project 2008-06. Home Related Documents & Links



Project 2008-06 Cyber Security Order 706

Link to NERC Project Page	Project 2008-06 Cyber Security Order 706
Standards Included	CIP-002-4, CIP-003-4, CIP-004-4, CIP-005-4a, CIP-005-4d, CIP-007-4, CIP-009-4, CIP-010-4, CIP-011-4, CIP-012-4, CIP-013-4, CIP-014-4, CIP-015-4, CIP-016-4, CIP-017-4, CIP-018-4, CIP-019-4, CIP-020-4, CIP-021-4, CIP-022-4, CIP-023-4, CIP-024-4, CIP-025-4, CIP-026-4, CIP-027-4, CIP-028-4, CIP-029-4, CIP-030-4, CIP-031-4, CIP-032-4, CIP-033-4, CIP-034-4, CIP-035-4, CIP-036-4, CIP-037-4, CIP-038-4, CIP-039-4, CIP-040-4, CIP-041-4, CIP-042-4, CIP-043-4, CIP-044-4, CIP-045-4, CIP-046-4, CIP-047-4, CIP-048-4, CIP-049-4, CIP-050-4, CIP-051-4, CIP-052-4, CIP-053-4, CIP-054-4, CIP-055-4, CIP-056-4, CIP-057-4, CIP-058-4, CIP-059-4, CIP-060-4, CIP-061-4, CIP-062-4, CIP-063-4, CIP-064-4, CIP-065-4, CIP-066-4, CIP-067-4, CIP-068-4, CIP-069-4, CIP-070-4, CIP-071-4, CIP-072-4, CIP-073-4, CIP-074-4, CIP-075-4, CIP-076-4, CIP-077-4, CIP-078-4, CIP-079-4, CIP-080-4, CIP-081-4, CIP-082-4, CIP-083-4, CIP-084-4, CIP-085-4, CIP-086-4, CIP-087-4, CIP-088-4, CIP-089-4, CIP-090-4, CIP-091-4, CIP-092-4, CIP-093-4, CIP-094-4, CIP-095-4, CIP-096-4, CIP-097-4, CIP-098-4, CIP-099-4, CIP-100-4
Standards to be Retired	CIP-002-3, CIP-003-3, CIP-004-3, CIP-005-3a, CIP-005-3c, CIP-007-3, CIP-008-3, CIP-010-3, CIP-011-3, CIP-012-3, CIP-013-3, CIP-014-3, CIP-015-3, CIP-016-3, CIP-017-3, CIP-018-3, CIP-019-3, CIP-020-3, CIP-021-3, CIP-022-3, CIP-023-3, CIP-024-3, CIP-025-3, CIP-026-3, CIP-027-3, CIP-028-3, CIP-029-3, CIP-030-3, CIP-031-3, CIP-032-3, CIP-033-3, CIP-034-3, CIP-035-3, CIP-036-3, CIP-037-3, CIP-038-3, CIP-039-3, CIP-040-3, CIP-041-3, CIP-042-3, CIP-043-3, CIP-044-3, CIP-045-3, CIP-046-3, CIP-047-3, CIP-048-3, CIP-049-3, CIP-050-3, CIP-051-3, CIP-052-3, CIP-053-3, CIP-054-3, CIP-055-3, CIP-056-3, CIP-057-3, CIP-058-3, CIP-059-3, CIP-060-3, CIP-061-3, CIP-062-3, CIP-063-3, CIP-064-3, CIP-065-3, CIP-066-3, CIP-067-3, CIP-068-3, CIP-069-3, CIP-070-3, CIP-071-3, CIP-072-3, CIP-073-3, CIP-074-3, CIP-075-3, CIP-076-3, CIP-077-3, CIP-078-3, CIP-079-3, CIP-080-3, CIP-081-3, CIP-082-3, CIP-083-3, CIP-084-3, CIP-085-3, CIP-086-3, CIP-087-3, CIP-088-3, CIP-089-3, CIP-090-3, CIP-091-3, CIP-092-3, CIP-093-3, CIP-094-3, CIP-095-3, CIP-096-3, CIP-097-3, CIP-098-3, CIP-099-3, CIP-100-3
Applicability Entities	RC, BA, IA, TOP, TO, GO, LSE, NERC, RE
Date FERC Approved	04/13/2012
Enforceable Date	04/01/2014 (Tentative)
SERC staff SME (Subject Matter Expert)	Tim Rowan 704-940-8230
Contact Link	Submit Feedback, Questions & Concerns



Cyber

Physical



Ten, Chee-Wooi, Chen-Ching Liu, and Govindarasu Manimaran. "Vulnerability assessment of cybersecurity for SCADA systems." Power Systems, IEEE Transactions on 23.4 (2008)

Summary of Previous Work

- Hardware-in-the-loop Network Analysis for Critical Infrastructure Protection (UNC Charlotte)
- Multi-layer Data-driven Reasoning Tool for Anomaly Detection and Causality Analysis (NC State)

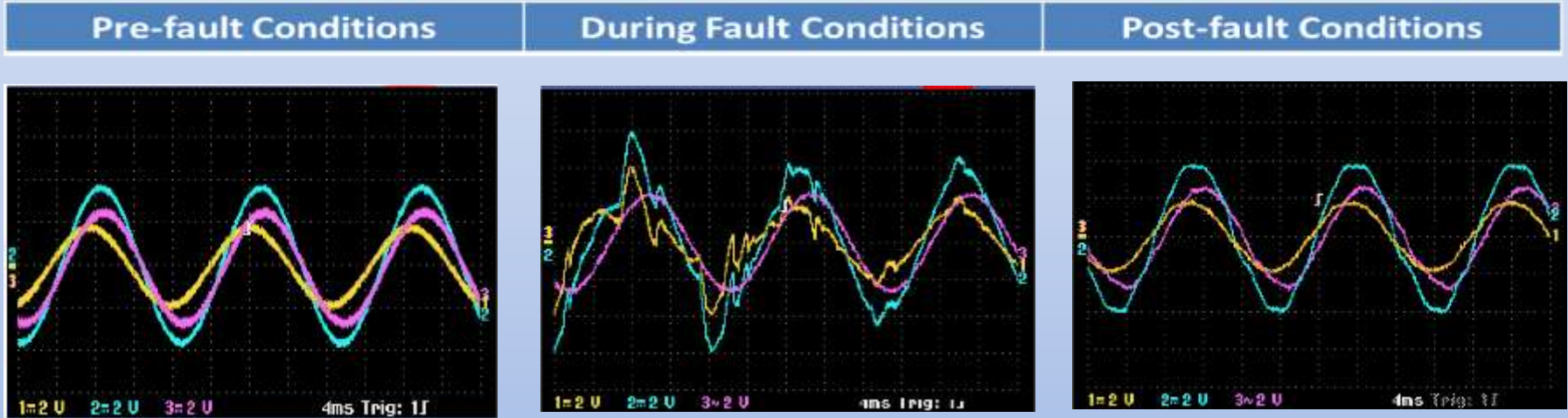
List of Assets and Control Levers



Item	Asset	Description	Specifications	Control Levers
1	SRCDOR	Dorsey generation	230kV, 4350MVA	
2	DORTRF1	Dorsey single phase auto transformer 1 with static capacitor compensation on 46kV side	230/46/500kV, 1200MVA, 138 μ F	Transformer breaker control
3	DORTRF2	Dorsey single phase auto transformer 2 with static capacitor compensation on 46kV side	230/46/500kV, 1200MVA, 138 μ F	Transformer differential protection
4	D602 and D602PRE	Dorsey main breaker and pre-insertion resistor	500kV, 600 Ω	Breaker control
5	LINE REACTOR	Dorsey line reactor	1111 Ω + 425 Ω , 225MVA _r	
6	dorros	Dorsey to Roseau transmission line	3.74 + j76.59 Ω , $X_c = 912\Omega$, 226km	
7	SCAPROS	Roseau series capacitor	31.9 μ F, 50% series compensation	Metal Oxide Varistor (MOV) and bypass switch
8	rosfor	Roseau to Forbes transmission line	5.23 + j110 Ω , $X_c = 688\Omega$, 311km	
9	MPL230	Forbes generation	230kV	
10	FORTRF1	Forbes single phase transformer 1 with series resistance load on 34.5kV	230/34.5/500kV, 600MVA, 2000 Ω	

Fault Simulation Results with RTDS

Fault is located at Roseau causing the Dorsey side distance relay protection to activate



Yellow: 230kV bus at Dorsey

Blue: 500kV bus at Forbes

Pink: 345kV bus at Chisago

Power Flow Analysis Results with RTDS

- Operate under light load, bypass series capacitors and overcompensate
- Operate under heavy load, undercompensate, request higher voltage



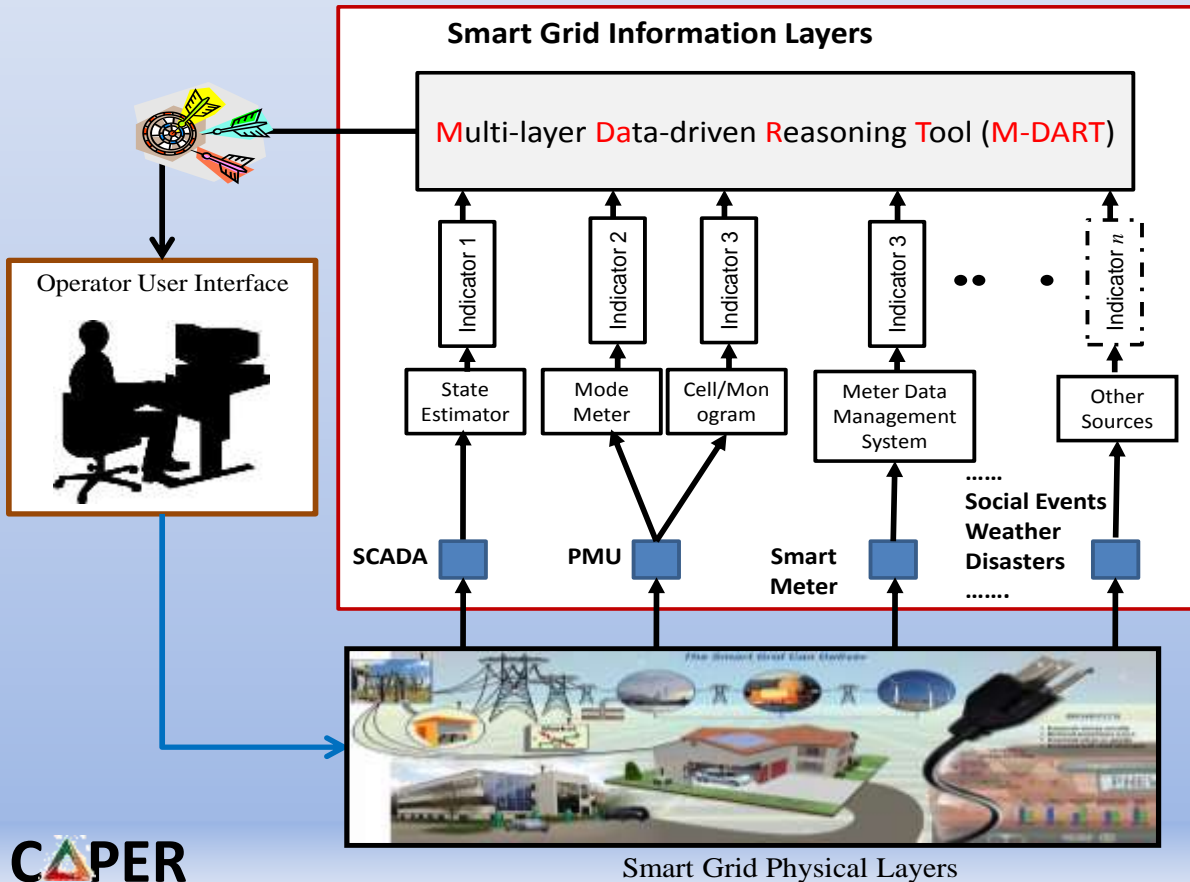
Real Power Demand	100MW	300MW	500MW
Shunt + Series Compensation	Very High Compensation	High Compensation	Optimal Compensation
Only Series (No Shunt) Compensation	High Compensation	Optimal Compensation	Low Compensation
No Compensation	<u>Medium High twist in system voltages</u> Voltages at Roseau above 8% over-voltage limit. Voltages at Chisago below 3% under-voltage limit.	<u>Medium Low twist in system voltages</u> Voltages at Roseau above 7% over-voltage limit. Voltages at Chisago below 2% under-voltage limit.	<u>Low twist in system voltages</u> Voltages at Roseau above 5% over-voltage limit. Voltages at Chisago below 1% under-voltage limit.
Only Shunt (No Series) Compensation	<u>High twist in system voltages</u> Voltages at Roseau above 10% over-voltage limit. Voltages at Chisago below 6% under-voltage limit.	<u>Medium High twist in system voltages</u> Voltages at Roseau above 9% over-voltage limit. Voltages at Chisago below 5% under-voltage limit.	<u>Medium Low twist in system voltages</u> Voltages at Roseau above 8% over-voltage limit. Voltages at Chisago below 4% under-voltage limit.

Real Power Demand	100MW	300MW	500MW
Variable Shunt + Series Compensation	$V_{LL} = 0.86$	$V_{LL} = 0.86$	$V_{LL} = 0.84$
	$V_{UL} = 1.04$	$V_{UL} = 1.02$	$V_{UL} = 1.00$
Only Variable Shunt (No Series) Compensation	$V_{LL} = 0.88$	$V_{LL} = 0.88$	$V_{LL} = 0.86$
	$V_{UL} = 1.10$	$V_{UL} = 1.04$	$V_{UL} = 1.06$

Summary of Previous Work

- Hardware-in-the-loop Network Analysis for Critical Infrastructure Protection (UNC Charlotte)
- Multi-layer Data-driven Reasoning Tool for Anomaly Detection and Causality Analysis (NC State)

M-DART Project: Multi-layer Data Anomaly Analysis

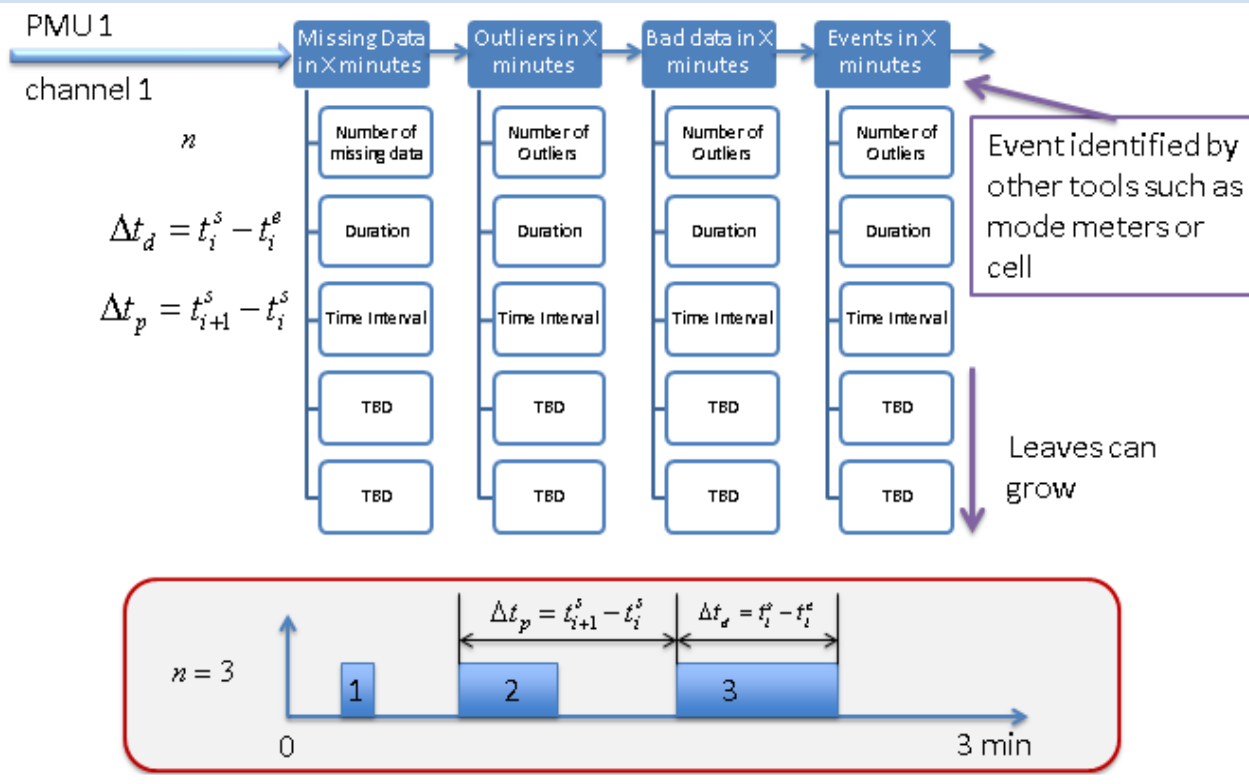


Data has “finger prints” too. There are certain signatures for abnormal data streams.

Device malfunctions, faults caused by natural events, man-made errors, cyber-attacks have different signatures.

Data collected from different sources can be used to verify each other.

Step 1. Data Quality Quantification for Each Data Stream



What is unique in DQQ?

Pay special attention to:

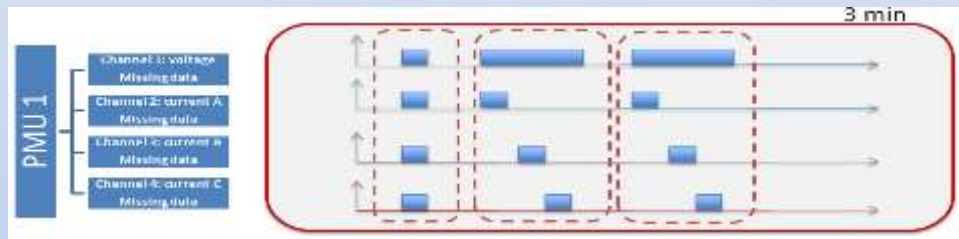
- Missing data
- Outliers
- Bad data

“Good data sets” are selected for analysis so they don’t contaminate results.

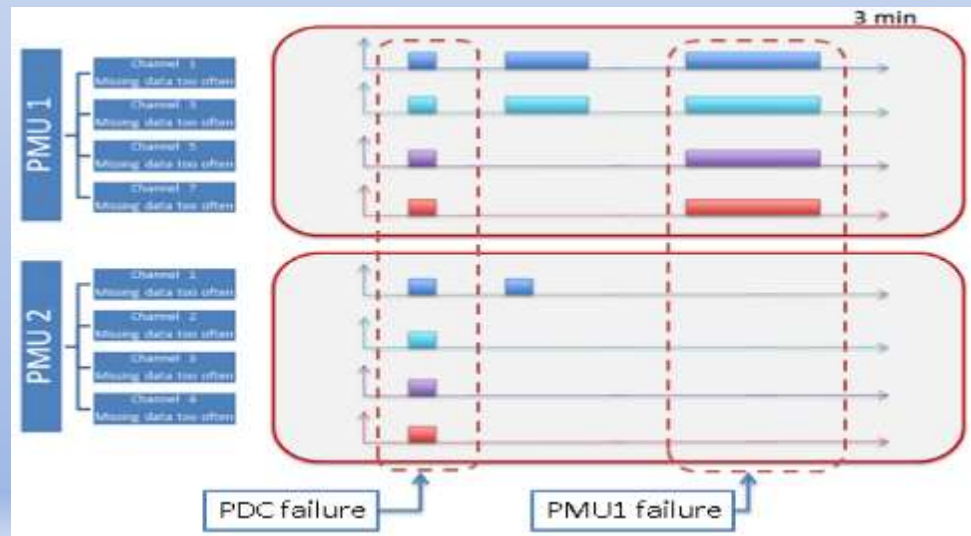
“Bad data sets” reveals more information from cyber security perspective.

Step 2: Pattern Recognition for Multiply Data Stream and Data Sources

Multiple Channels
from the same PMU

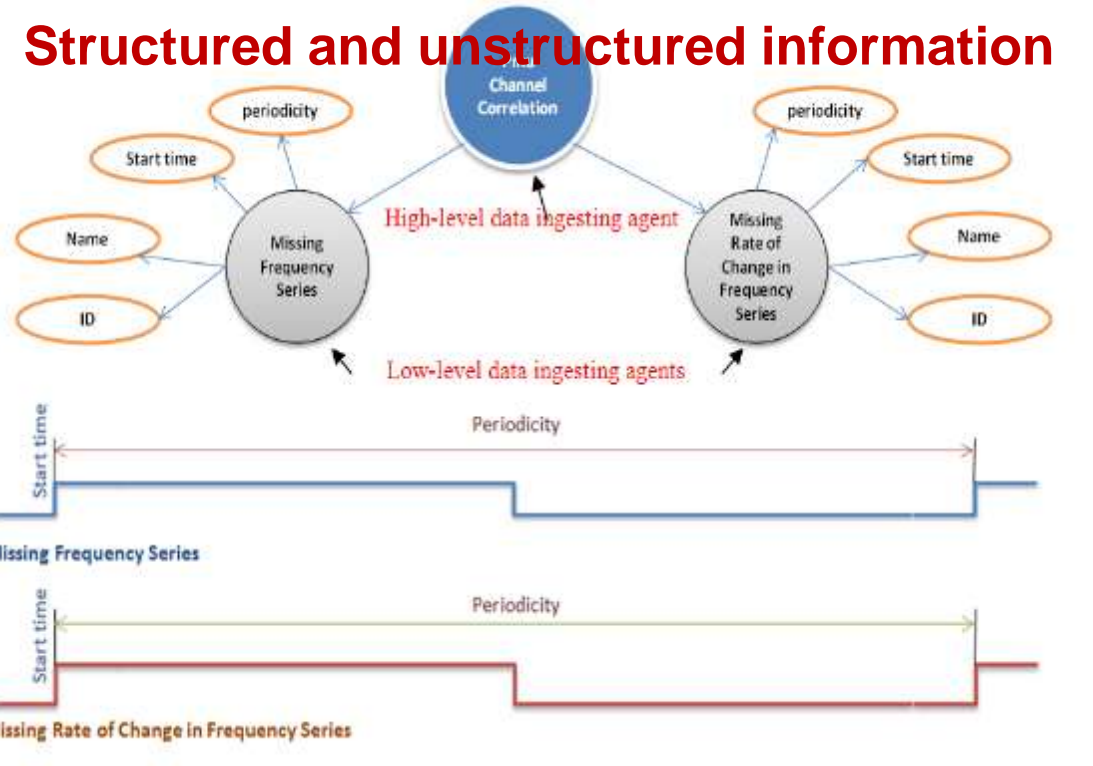


Multiple Channels
from multiple PMUs



Step 3: Correlate Patterns and Signatures → Knowledge base

Structured and unstructured information



Why an experienced operator can identify causes of an event much quicker than an inexperienced operator?

They can derive information from seemingly unrelated events by

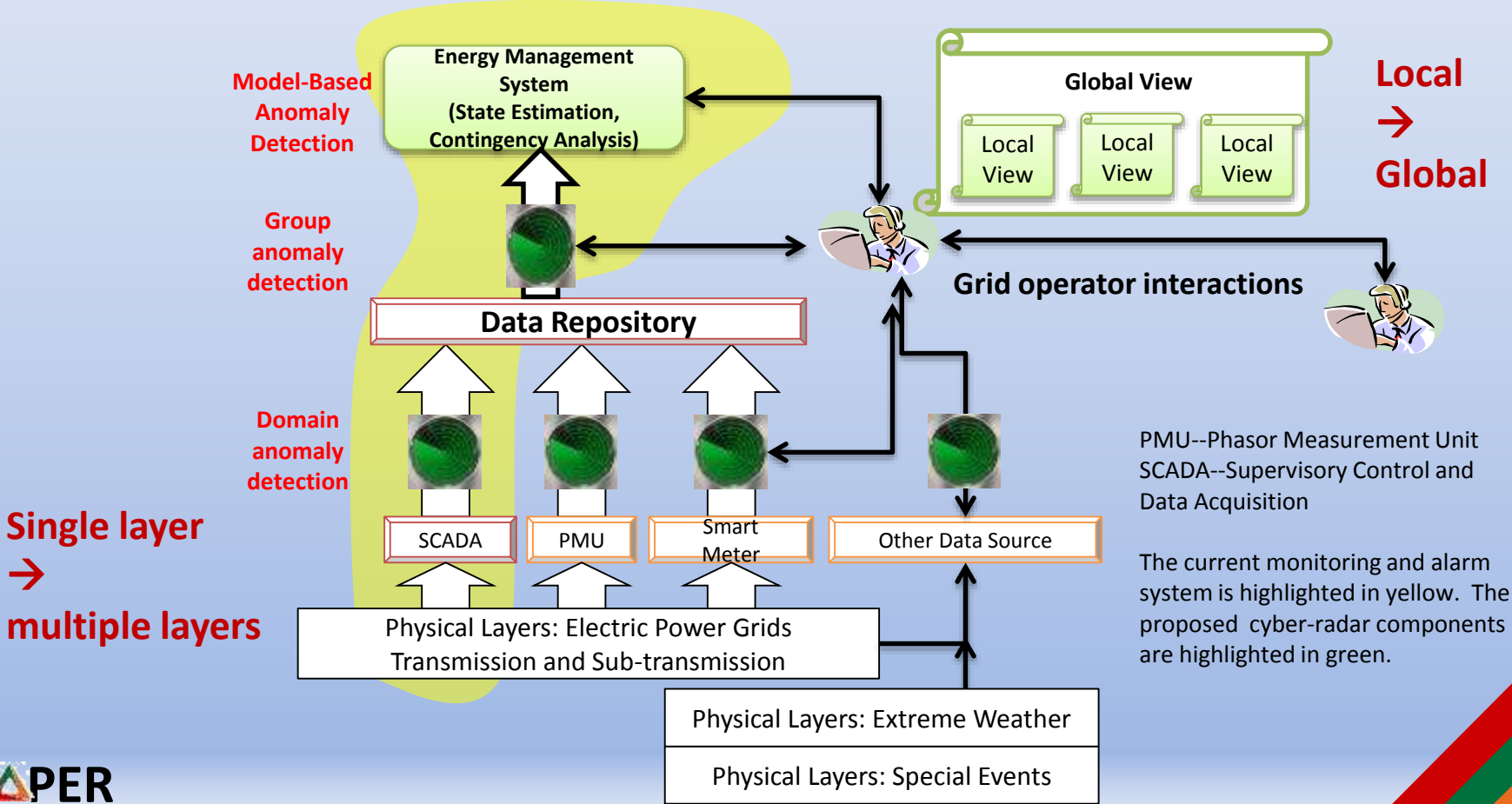
- Detect the hidden patterns
- Assess the strong and weak correlations based on situations
- Access additional information for making better judgements

Proposed Work

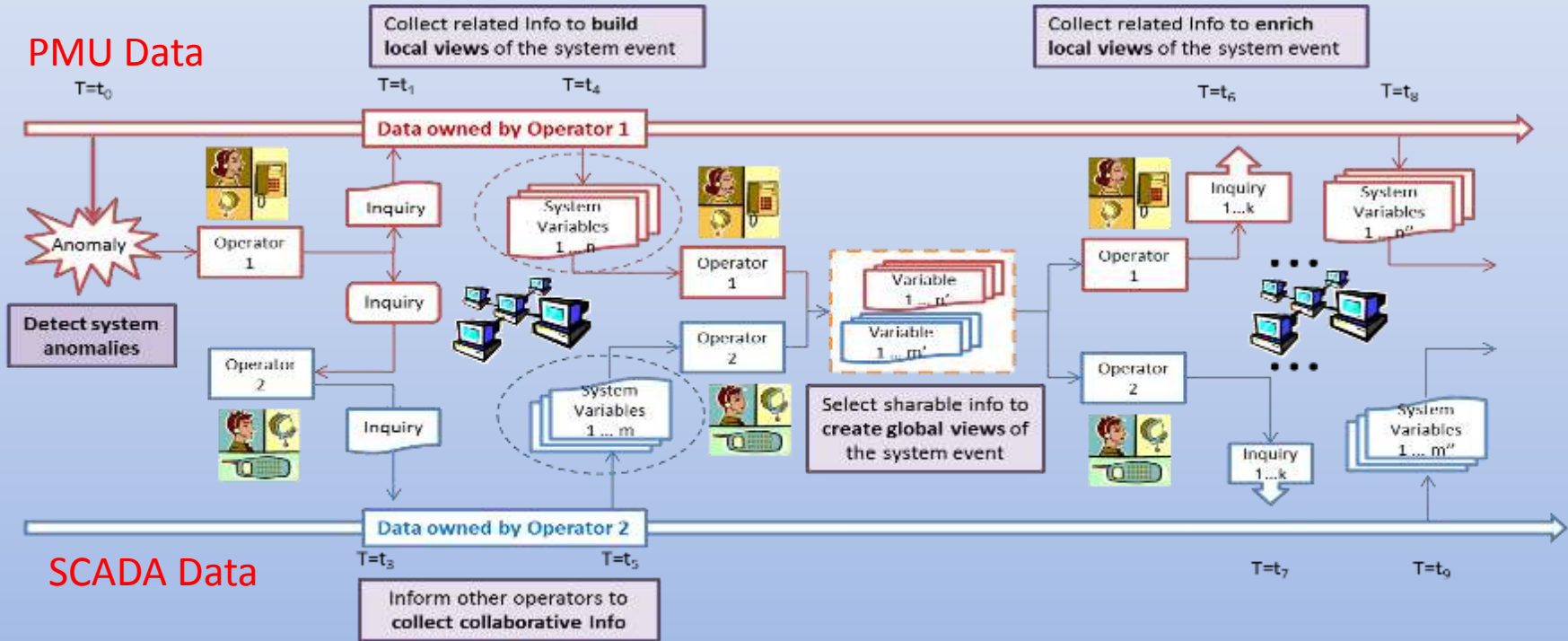
Integrated Data Management for Anomaly Detection and Cyber Vulnerability Assessment

(**Sub-area:** Data Management, Analytics, and Security)

Goal: Integrated Data Management



An illustration of the Anomaly Detection Process



Proposed Approach

- Analyze information from multiple data sources
- Capture subject-matter expertise in ontological model-based representation
- Update knowledge base using real-time data and correlate data sources
- Further reveal the nature of the anomaly and show that if the anomaly is caused by nature events, man-made error or malicious attack
- Assess the impact of the anomaly
- Determine the severity (triaging of threat level)
- Determine the level of response (from “do nothing” to “enter emergency operation”)
- Provide guidance to utility operators on recommended steps (Enable alternate power flow mechanisms? Shut down service? Block access to certain users? Throw away the problematic data sets? Harden protection of certain devices?)
- Ensure stable and reliable operation of the grid through the cyber-event

Power Flow Analysis Results with RTDS

- Operate under light load, bypass series capacitors and overcompensate
- Operate under heavy load, undercompensate, request higher voltage



Real Power Demand	100MW	300MW	500MW
Shunt + Series Compensation	Very High Compensation	High Compensation	Optimal Compensation
Only Series (No Shunt) Compensation	High Compensation	Optimal Compensation	Low Compensation
No Compensation	<u>Medium High twist in system voltages</u> Voltages at Roseau above 8% over-voltage limit. Voltages at Chisago below 3% under-voltage limit.	<u>Medium Low twist in system voltages</u> Voltages at Roseau above 7% over-voltage limit. Voltages at Chisago below 2% under-voltage limit.	<u>Low twist in system voltages</u> Voltages at Roseau above 5% over-voltage limit. Voltages at Chisago below 1% under-voltage limit.
Only Shunt (No Series) Compensation	<u>High twist in system voltages</u> Voltages at Roseau above 10% over-voltage limit. Voltages at Chisago below 6% under-voltage limit.	<u>Medium High twist in system voltages</u> Voltages at Roseau above 9% over-voltage limit. Voltages at Chisago below 5% under-voltage limit.	<u>Medium Low twist in system voltages</u> Voltages at Roseau above 8% over-voltage limit. Voltages at Chisago below 4% under-voltage limit.

Real Power Demand	100MW	300MW	500MW
Variable Shunt + Series Compensation	$V_{LL} = 0.86$	$V_{LL} = 0.86$	$V_{LL} = 0.84$
	$V_{UL} = 1.04$	$V_{UL} = 1.02$	$V_{UL} = 1.00$
Only Variable Shunt (No Series) Compensation	$V_{LL} = 0.88$	$V_{LL} = 0.88$	$V_{LL} = 0.86$
	$V_{UL} = 1.10$	$V_{UL} = 1.04$	$V_{UL} = 1.06$

Proposed Tasks and Milestones

- ~~Creation of a power flow simulation model of candidate transmission line with embedded synchrophasors~~
- ~~Creation of distributed communication network model for synchrophasors~~
- ❖ ~~Analysis of distributed phasor state estimation algorithms under normal conditions~~
- ~~Insertion of series of threats at vulnerable points at different threat levels~~
- ❖ ~~Analysis of distributed phasor state estimation algorithms under threat conditions~~
- ❖ ~~Quantify~~
 - ~~ability of algorithms to converge and provide accurate state~~
 - ~~ability of algorithms to locate and “triage” severity threats~~
 - ~~ability of algorithms to reconfigure and reroute data to isolate compromised assets~~

Proposed Tasks and Milestones

- Task 1: Data Requests (NCSU + UNCC)
 - Request PMU, SCADA, or smart meter data for baseline data quality quantification
 - Request PMU, SCADA, or smart meter data before, during, and after a system outage for anomaly detection
 - Interview with grid operation engineers for events detection procedures

Milestones:

- 1) Identify the system event detection scenarios
- 2) Deliver training data sets associate with the baseline and the system event identified

- Task 2: Benchmark the Signature (NCSU)
 - Establish the baseline data signatures for each data stream
 - Establish the baseline data patterns for multiple data stream and multiple data sources
 - Establish the knowledge base for detection a group of specified grid events

Milestones:

Deliver a signature database and a knowledge database for the target grid event (**depending on which data sets we can get from sponsors.**)

- Task 3: Anomaly Detection (NCSU)
 - Identify the indicators/precursors of a target system event
 - Develop an algorithm for automating the process
 - Implement the anomaly detection module and test them on RTDS

Proposed Tasks and Milestones

- Task 4: Hard-ware-in-the-loop simulation for identifying the threat levels and impacts (UNCC)
 - Build an RTDS model for the selected system
 - Integrate RTDS model with hardware control and protection components
- Task 5: Impact Study (UNCC)
 - Insertion of series of identified threats into the system model to evaluate impact at different threat levels
 - ability of algorithms to converge and validate the threats
 - ability of algorithms to locate and “triage” severity threats
 - ability of algorithms to reconfigure and reroute data to isolate compromised assets
- Task 6: Identify mitigation methods (UNCC+ NCSU)

Lead Principal Investigators



Dr. Madhav Manjrekar, Associate Professor, University of North Carolina in Charlotte, led technology and innovation teams in the areas of green energy and power systems for the past 15 years. Prior to joining academia in 2012, Dr. Manjrekar was the VP of Global Research and Innovation at Vestas (the wind turbine company), and previously has held various leadership and management positions at Siemens, Eaton and ABB. His research interests are in utility applications of power electronics, renewable power integration, energy storage, smart grids, and cyber vulnerability of electrical infrastructure.



Dr. Lu has over 19 years of experience in electric power engineering. From 2003 to 2012, Dr. Ning Lu was a senior research engineer with Pacific Northwest National Laboratory. She has conducted and managed research projects in modeling and analysis of power system load behaviors, wide area energy storage management systems, renewable integration, climate impact on power grids, and smart grid modeling and diagnosis. Dr. Lu is a senior member of the Institute of Electrical and Electronics Engineers. She has authored or co-authored more than 60 publications, including journal articles, conference proceedings, and technical reports.



NC STATE

Proposed Budget

PI	2016	2017	Total
Madhav Manjrekar	\$36.2K	\$36.2K	\$72.4K
Ning Lu	\$36.2K	\$36.2K	\$72.4K
	\$72.4K	\$72.4K	\$144.8K

Budget Amount	2016	2017	Total
	1 GA UNCC 1 GA at NC State	1 GA UNCC 1 GA at NC State	
Salaries	\$36,000	\$36,000	\$72,000
Fringe Benefits	\$4,958	\$4,958	\$9,916
Tuition Remission	\$17,128	\$17,128	\$34,256
Equipment	\$2,500	\$2,500	\$5,000
Travel	\$4,000	\$4,000	\$8,000
Materials & Supplies	\$1,250	\$1,250	\$2,500
Contract Support			
Overhead (10%)	\$6,584	\$6,584	\$13,168
TOTAL	\$72,420	\$72,420	\$144,840