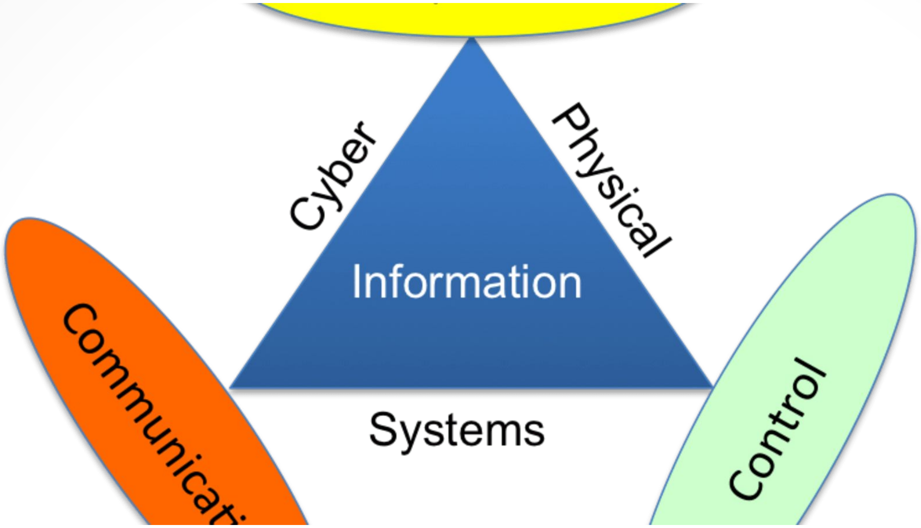
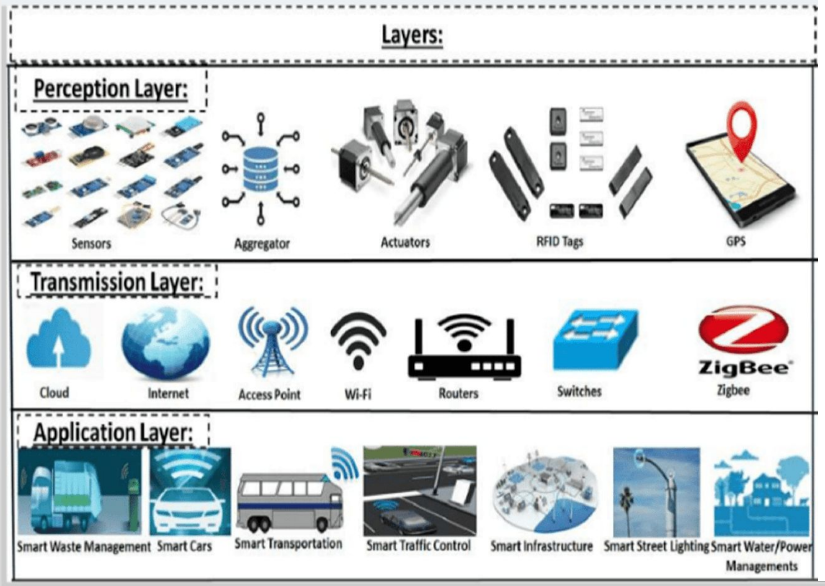
CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

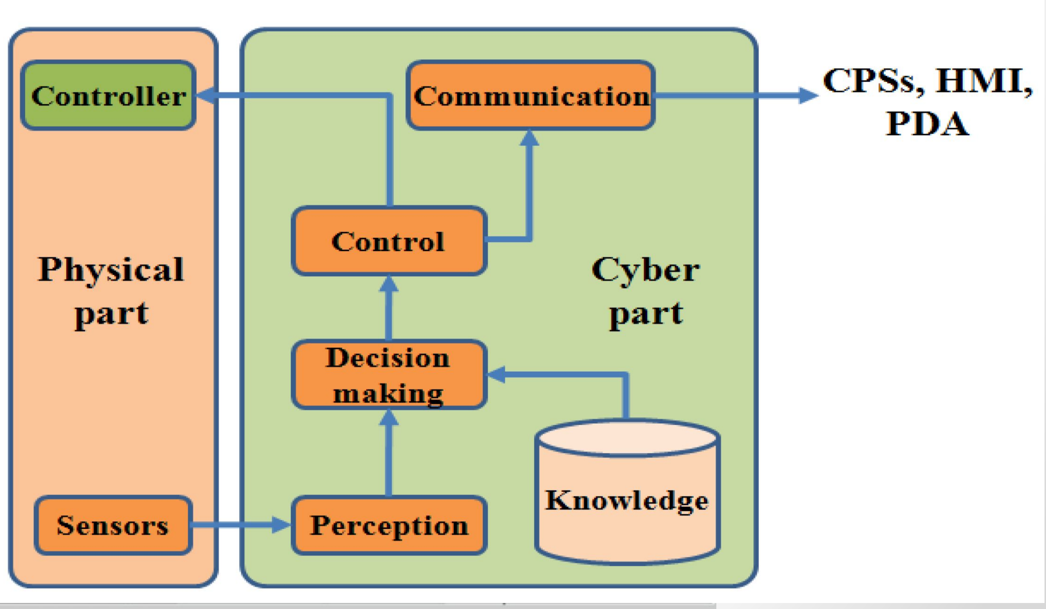
Cyber-Physical Smart Grid Security

Dr Neetesh Saxena
Associate Professor
IEEE Senior Member
DAAD and TCS Fellow Alumni
Vice Chair, DASIG – IEEE UK and Ireland Systems Council
Cardiff University, United Kingdom

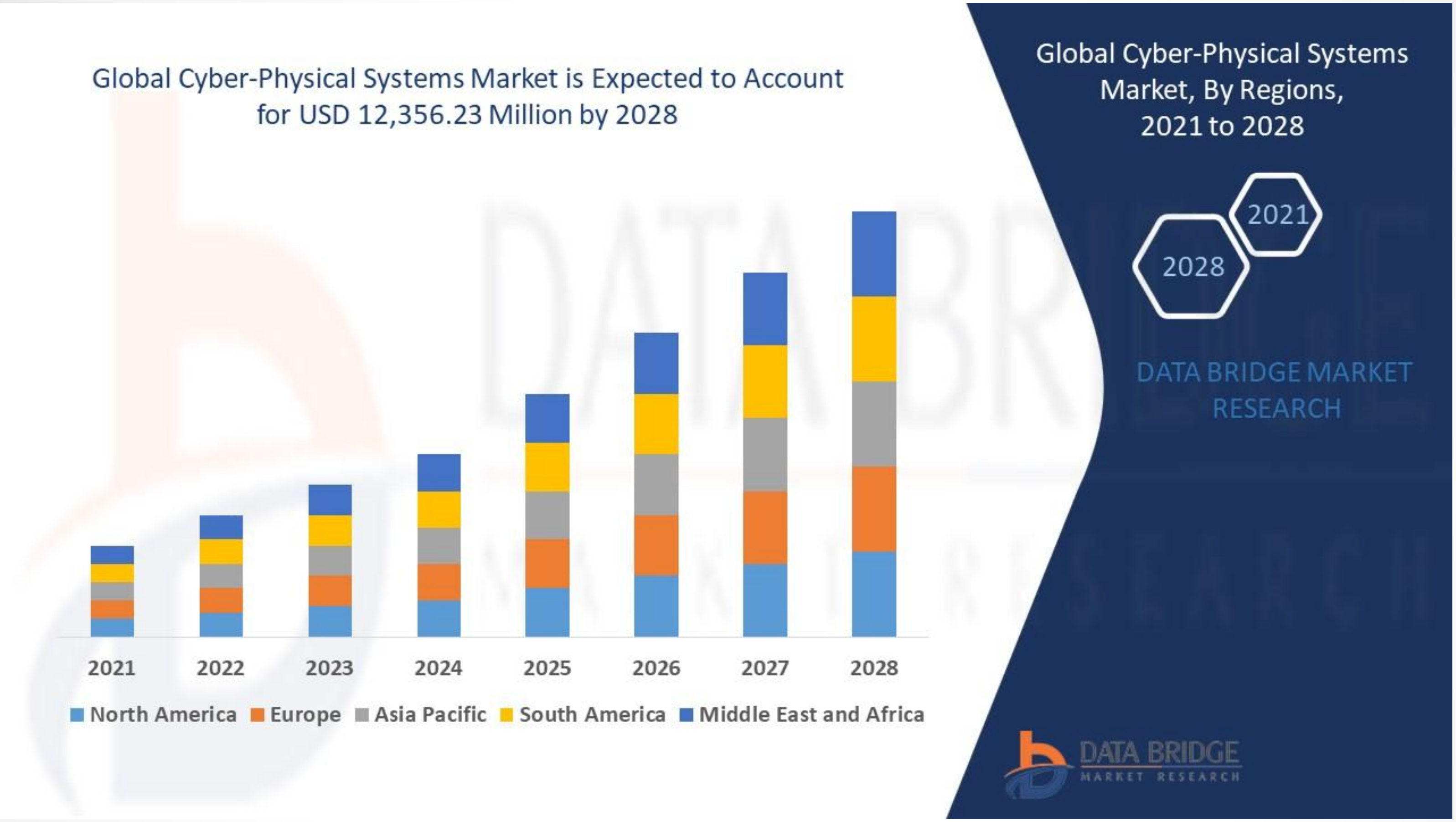
Cyber-Physical Systems







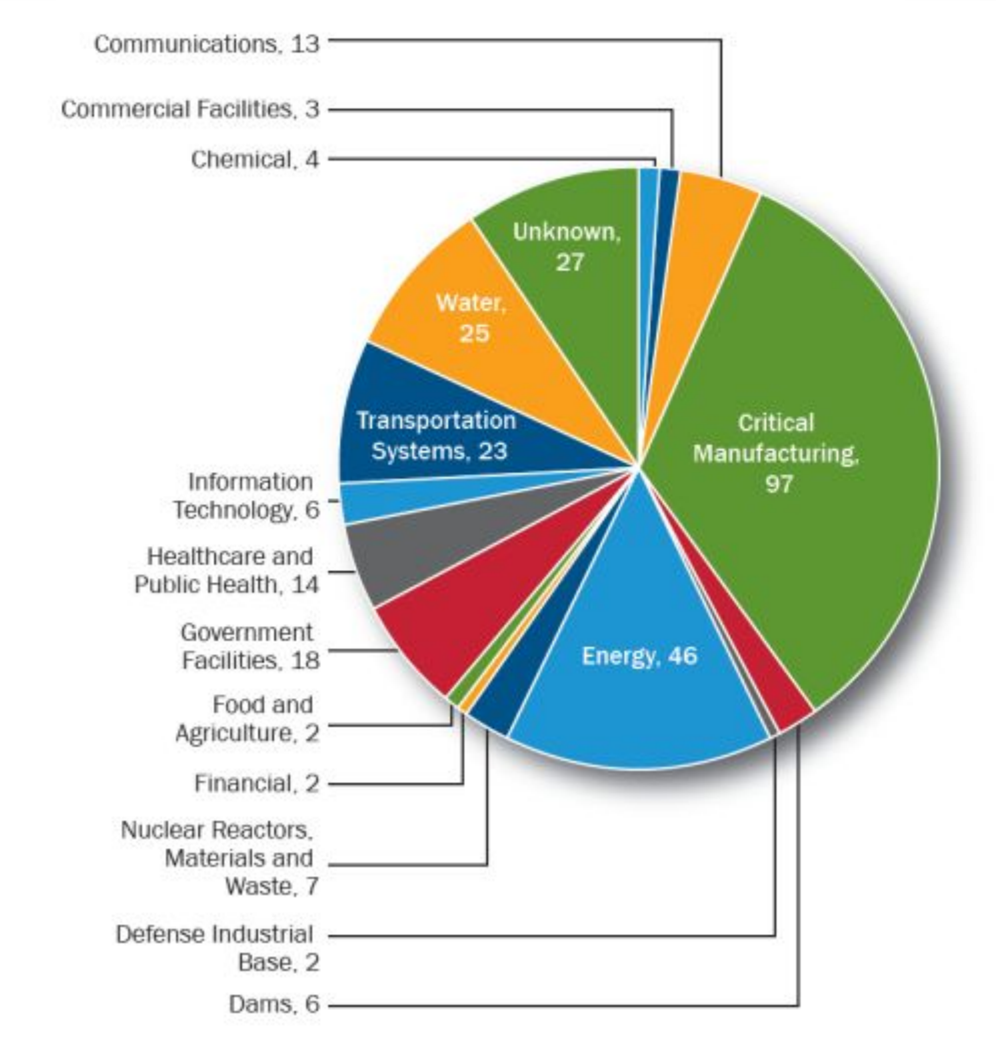
CPS Industry Market



Cyber-physical systems market will reach at an estimated value of USD 12,356.23 million by 2028 and grow at a CAGR of 10.55% in the forecast period of 2021 to 2028.

Increase in the penetration of internet acts as an essential factor driving the cyber-physical systems market.

Incidents by Sectors



https://www.osti.gov/servlets/purl/1337873

Research Interests

Critical Infrastructure Protection, Cyber Security, and Cyber-Physical System Security

Critical Systems Protection

Information Assurance

Authentication, identity and access management, availability, encryption, and non-repudiation.

Develop Strategies and Architectures

For SG
For V2G
For Cellular network and SMS
Securing Pub/Sub info
Secure wireless comm. info.

Information Privacy

Untraceability, anonymity, forward privacy.

Vulnerability Assessment

Vulnerability Identification and Detection

APT C&C malware - BlackEnergy, DoS attack, use of social engineering techniques (email).

Incident Responses

Response to cyber incidents and remediate attacks, host-based and log-based analysis.

Network Forensics

IDS, Wireshark with Jpcap, IP/TCP/ UDP/ICMP/DNP3, traffic analysis.

System Simulation

Attack Modelling and Metrics Investigation

Cyber-attacks, component criticality matrix, trust matrix.

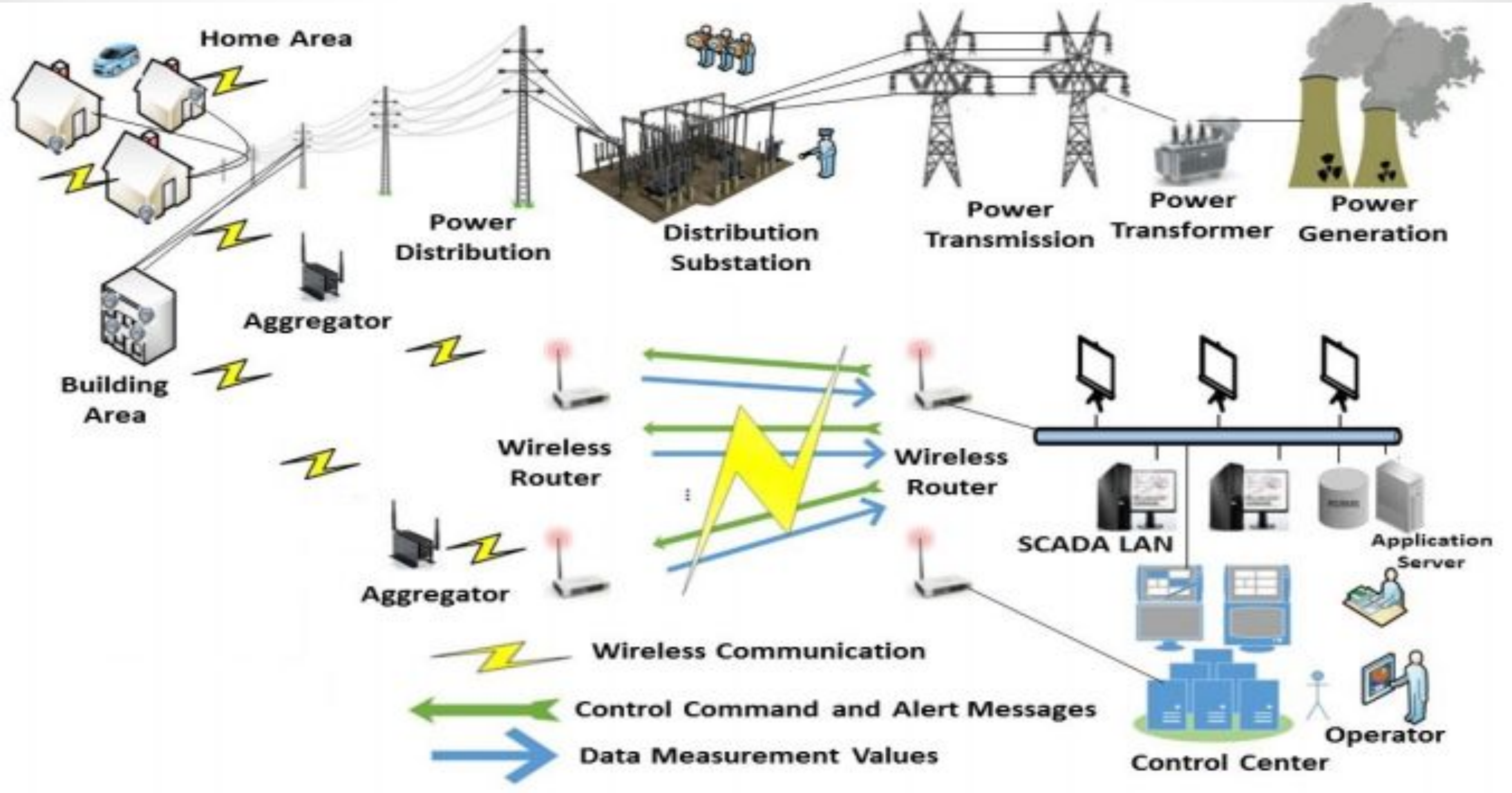
Accurate Reports and Result Analysis

CPS impact monitoring and analysis.

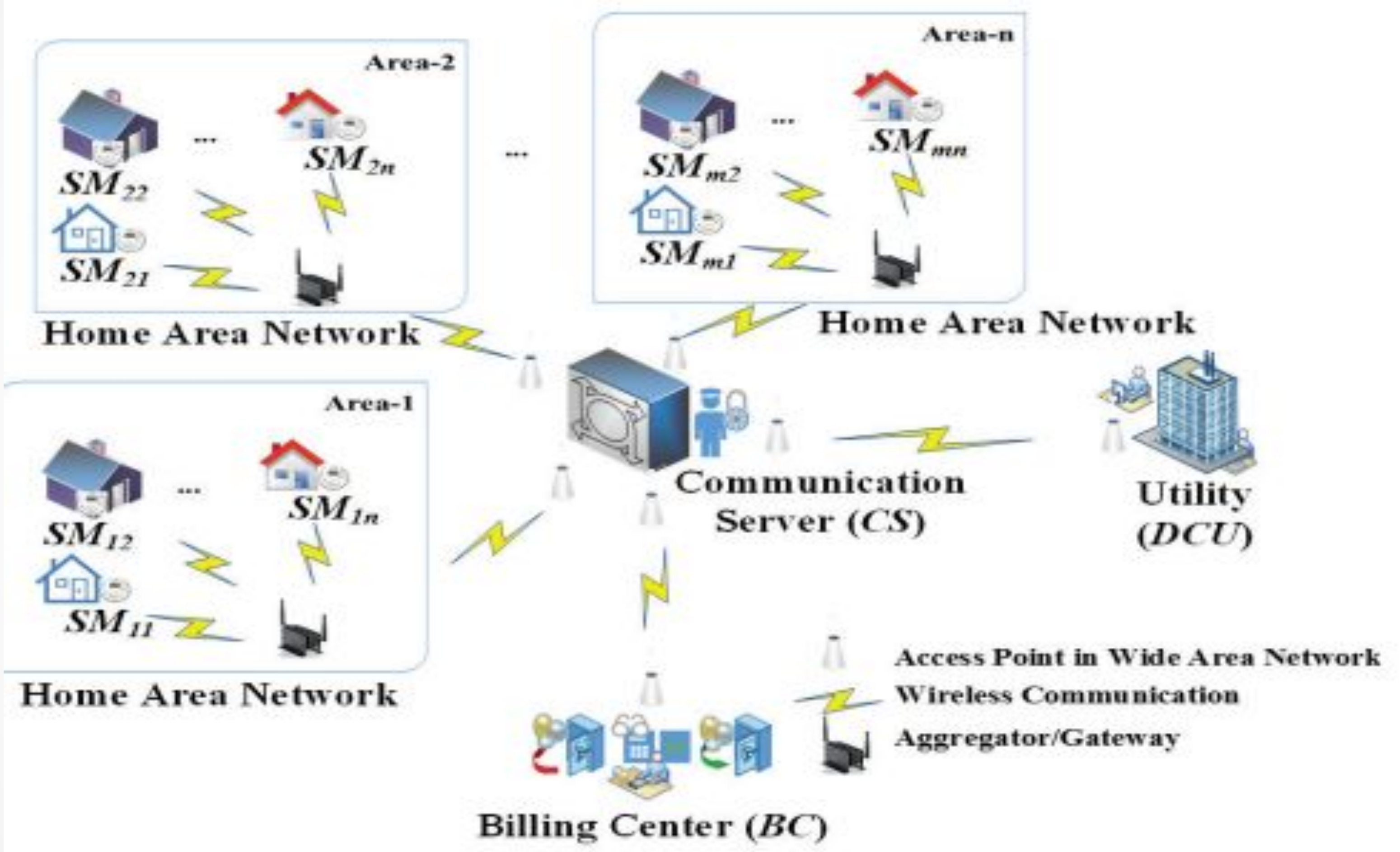
Analysis of Securing Last-Mile Communications

Measurements, control commands and alert messages.

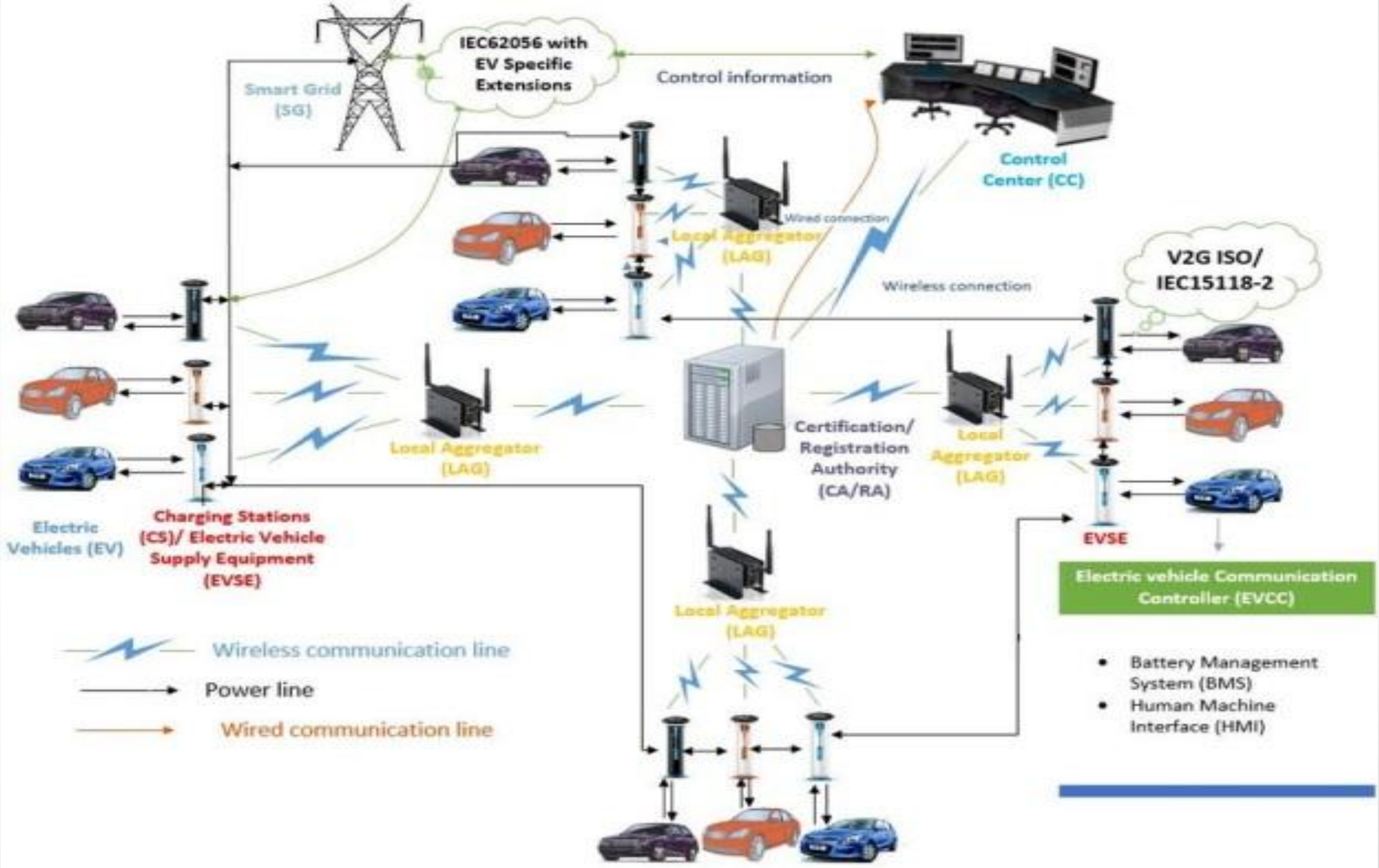
CPS Application 1



CPS Application 2



CPS Application 3


Smart Grid (SG)
IEC62056 with EV Specific Extensions
Control information
Control Center (CC)
Wired connection
Local Aggregator (LAG)
Wireless connection
V2G ISO/ IEC15118-2
Certification/ Registration Authority (CA/RA)
Local Aggregator (LAG)
Local Aggregator (LAG)
Local Aggregator (LAG)
EVSE
Electric vehicle Communication Controller (EVCC)
Electric Vehicles (EV)
Charging Stations (CS)/ Electric Vehicle Supply Equipment (EVSE)
Wireless communication line
Power line
Wired communication line
• Battery Management System (BMS)
• Human Machine Interface (HMI)

ICS – Situational Awareness

- **Last-Mile Resilient Communication –** solution for critical commands and data delivery **& Situational Awareness –** understanding impact of cyber attacks

- **Situational Awareness –** ICS
  - Life safety, monitoring, security, mass notification
    - When is it too late? - track progress
    - Detect/recommend servicing before m/c /device breaks
      - reduce production/maintenance downtime.
    - Advance alerts - handled before emergency.
    - Receive an alert if a machine/device is overheating
      - Monitor when to change devices.
    - Informing the correct people
      - Sensors added to m/c /device send alert.
    - Incorporating existing systems into a situational alerting platform
      - multifaceted security control systems.

- **ICS/OT Resilience Techniques**
  - Effective analytics monitoring
  - Adaptive responses
  - Deception
  - Diversity techniques
  - Dynamic positioning & representation
  - Coordinated defence & segmentation

Power Grid Attack: Investigation & Solutions

- Targeting cyber-attacks on Ukraine power grid – one of the most critical issues worldwide.
  - Controlled a system, opened breakers, and took 30 substations, 2 power dist. centers offline.

- **How?**
  - Had gained access to user accounts for networks and devices.
  - Wrote malicious firmware to replace the legitimate firmware.
  - Launched telephone denial-of-service attack.
  - Phishing campaign - workers clicked on the phishing attachment - enable macros.
  - Ukraine utilities were forced to bear economic losses, down reputation, left consumers in dark.

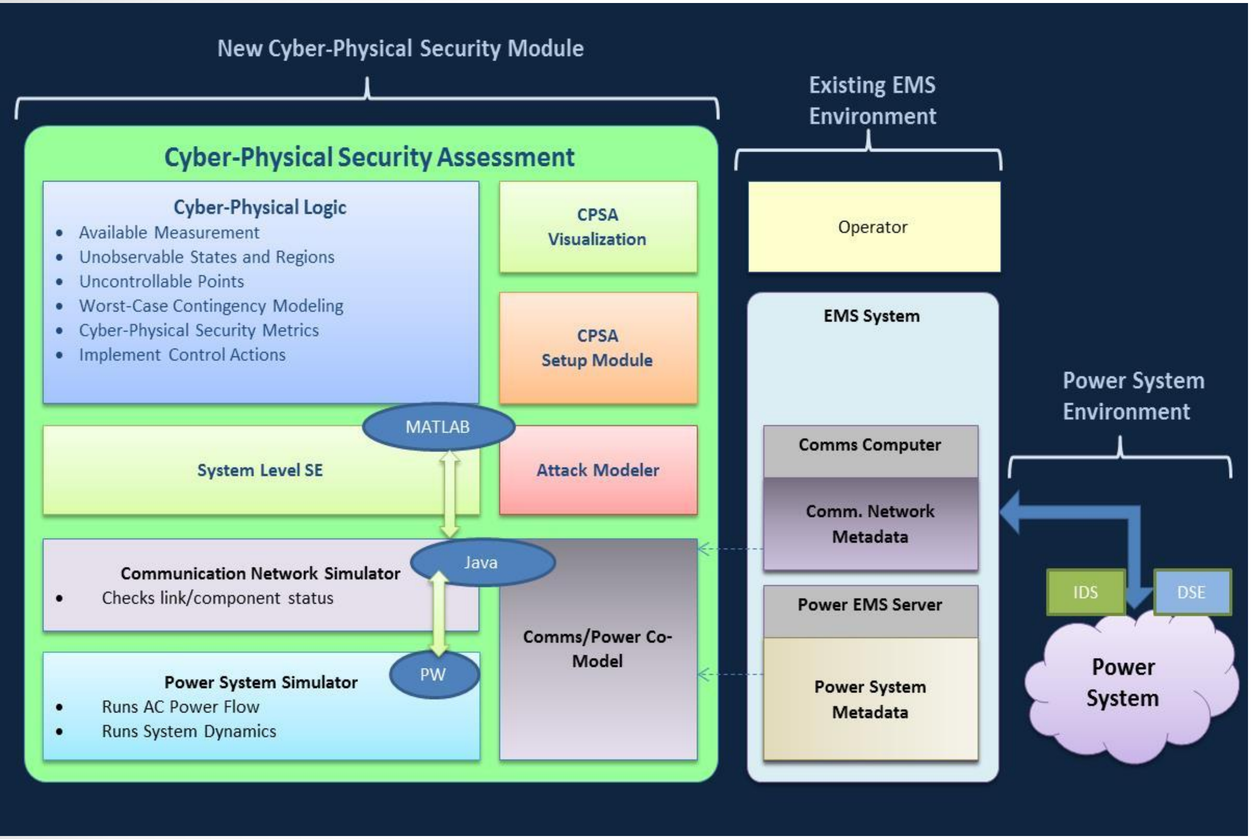
- Word/Excel enables macros - triggers BlackEnergy
  - extracts the list of proxy servers in the networks.

- **Detection**
  - Designed a Tool - Event Logs and Host-Based Monitoring.
    - **Centralized Timeline analysis:** log files access, registry data, Internet history files.
    - **Communication network log files:** start/stop activity time, ACK status, comm. parameters.
    - **Other logs:** attempts of wrong password/change settings of the device, temporal anomalies.

  - Extract macros without running Excel/Word - *oledump* (object linking and embedding tool).

  - **Network Forensics and IPS/IDS Rules Formation** – **Suricata**, **DNP3** and **Wireshark**.
    - **Block** - malicious URLs and masks, botnet C&C URLs + IP addresses and port#.
    - Compute and block - MD5/SHA **hashes of malicious objects/files database**.
      - OWASP – File Hash Repository

Cyber-Physical Situational Awareness



Component	Physical	Cyber	Other	Total	Last Time
Bus					
Generator					
Load					
Transformer					
Other					

Component Trust Matrix

Component	V. Low	Low	Moderate	High	Critical
Bus					
Generator					
Load					
Transformer					
Other					

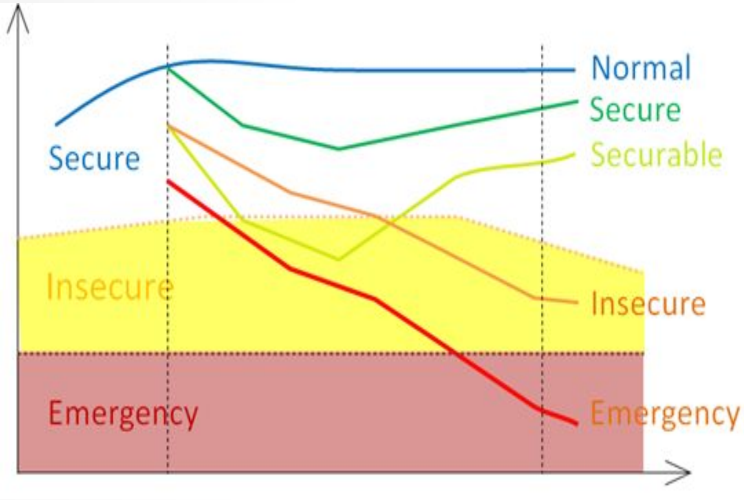
Component Criticality Matrix

Co-simulator with modelling of cyber attacks

- **Objectives**
  - System-level cyber-security assessment.
  - Steady-state cyber-attack impact assessment.
  - Cyber-security state estimator with system-level comm. topology.

Situational Awareness: Effects of Cyber Attacks

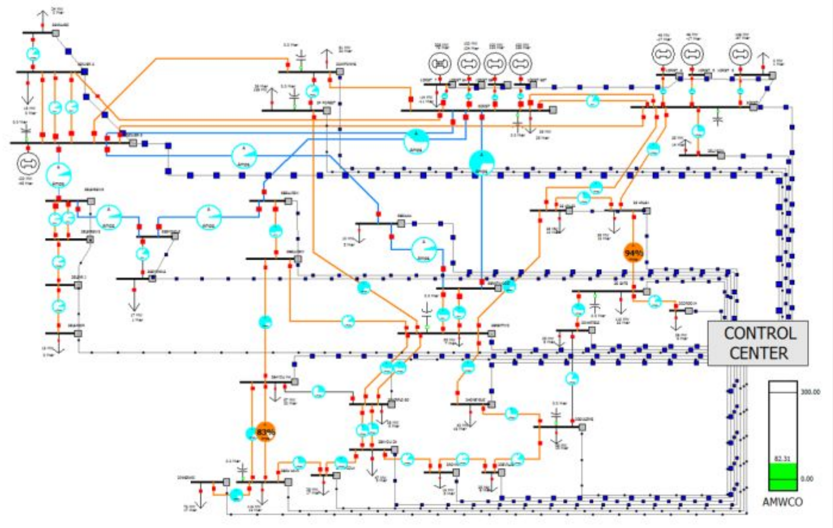
Evaluate system behavior with cyber-attacks scenarios.
Evaluate system behavior with future demands scenarios.
30 iterations- next half an hour with varying load.



Understanding cyber-physical effects.

▯ **“Under Attack” Scenario:**

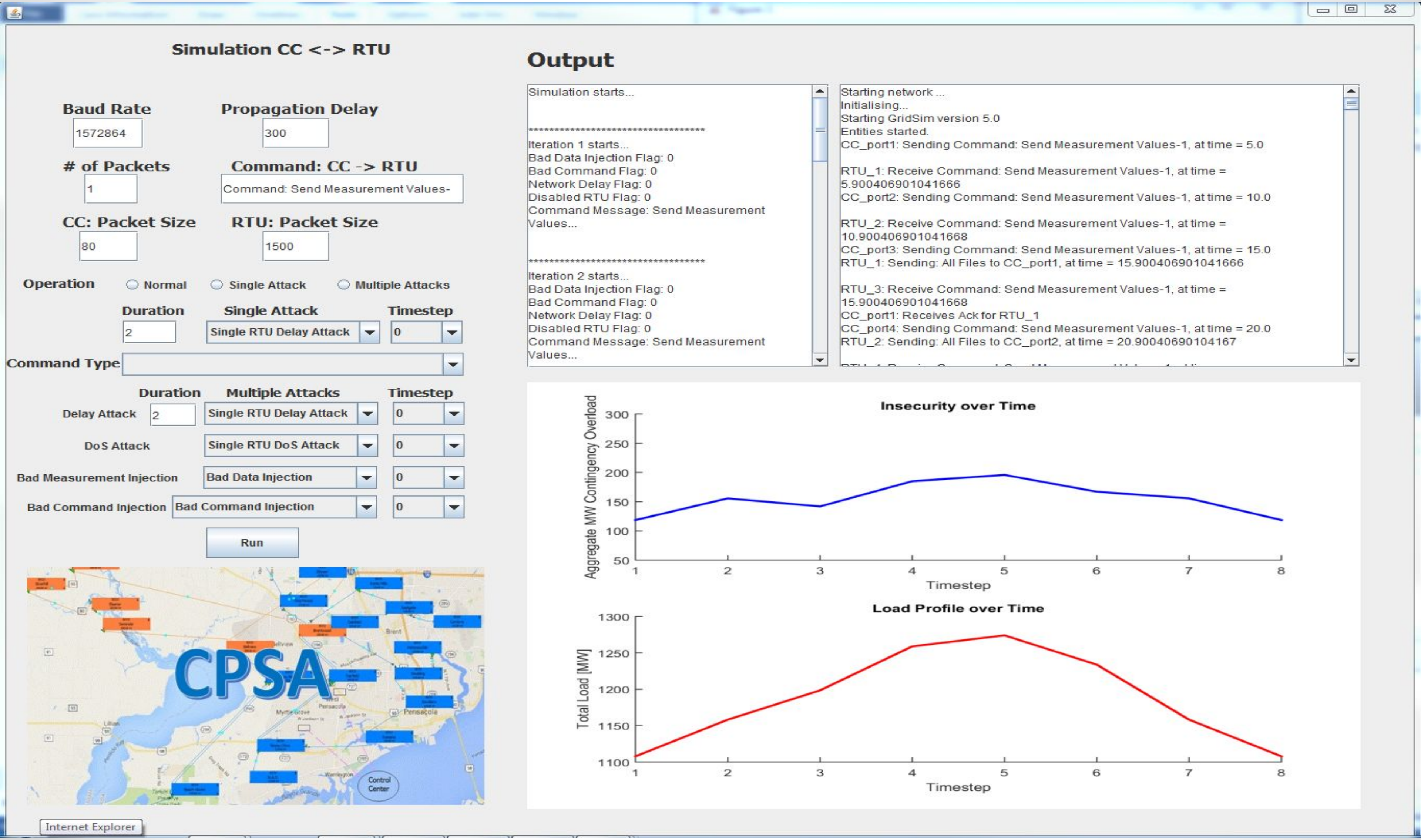
- System recovery from a critical security issue
  - frequent generation of dynamic secrets and secret keys recover the system.
- Situational awareness



Effects of Cyber and Physical Events

Event	Type
Altered Measurement	Cyber
RTU stream blocked	Cyber
Unexpected load increase	Physical
Altered control command	Cyber

CPSA



Simulation CC <-> RTU

Baud Rate: 1572864

Propagation Delay: 300

# of Packets: 1

Command: CC -> RTU: Command: Send Measurement Values-

CC: Packet Size: 80

RTU: Packet Size: 1500

Operation ○ Normal ○ Single Attack ○ Multiple Attacks

Duration	Single Attack	Timestep
2	Single RTU Delay Attack	0

Command Type:

	Duration	Multiple Attacks	Timestep
Delay Attack	2	Single RTU Delay Attack	0
DoS Attack		Single RTU DoS Attack	0
Bad Measurement Injection		Bad Data Injection	0
Bad Command Injection		Bad Command Injection	0

Output

```
Simulation starts...


************************************
Iteration 1 starts...
Bad Data Injection Flag: 0
Bad Command Flag: 0
Network Delay Flag: 0
Disabled RTU Flag: 0
Command Message: Send Measurement
Values...


************************************
Iteration 2 starts...
Bad Data Injection Flag: 0
Bad Command Flag: 0
Network Delay Flag: 0
Disabled RTU Flag: 0
Command Message: Send Measurement
Values...
```

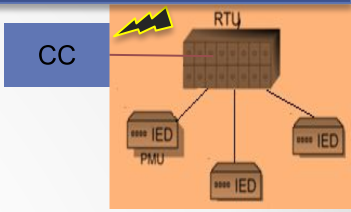
```
Starting network ...
Initialising...
Starting GridSim version 5.0
Entities started.
CC_port1: Sending Command: Send Measurement Values-1, at time = 5.0

RTU_1: Receive Command: Send Measurement Values-1, at time =
5.900406901041666
CC_port2: Sending Command: Send Measurement Values-1, at time = 10.0

RTU_2: Receive Command: Send Measurement Values-1, at time =
10.900406901041668
CC_port3: Sending Command: Send Measurement Values-1, at time = 15.0
RTU_1: Sending: All Files to CC_port1, at time = 15.900406901041666

RTU_3: Receive Command: Send Measurement Values-1, at time =
15.900406901041668
CC_port1: Receives Ack for RTU_1
CC_port4: Sending Command: Send Measurement Values-1, at time = 20.0
RTU_2: Sending: All Files to CC_port2, at time = 20.90040690104167
```

Bad Measurement Injection & Malicious Command Injection

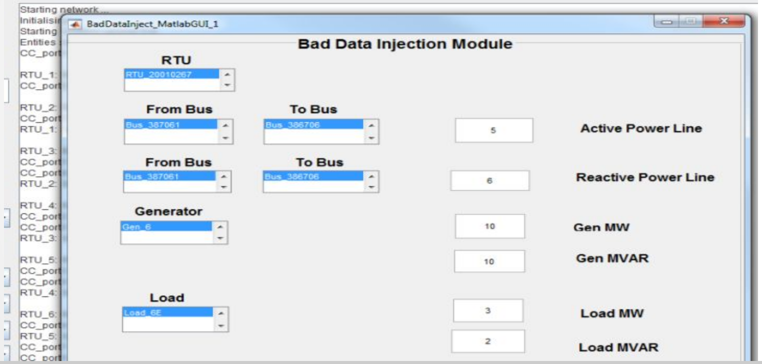


Scenario: Case 1

- Attacker manipulates raw measurements at RTU.
- RTU sends bad measurements to the CC.
- IDS/DSE provides an alert of suspicious data.

Scenario: Case 2

- Attacker intercepts a legitimate command, alters it.
- IDS identifies bad command based on its rules.
- IDS notifies to the CC and asks for confirmation.
- Operator simulates - confirms or rejects command.



```
Starting network ...
Initialisi
Starting
Entities
CC_port
RTU_1:
CC_port
RTU_2:
CC_port
RTU_1:
RTU_3:
CC_port
CC_port
RTU_2:
RTU_4:
CC_port
CC_port
RTU_3:
RTU_5:
CC_port
CC_port
RTU_4:
RTU_6:
CC_port
RTU_5:
CC_port
CC_port
```

Bad Data Injection Module

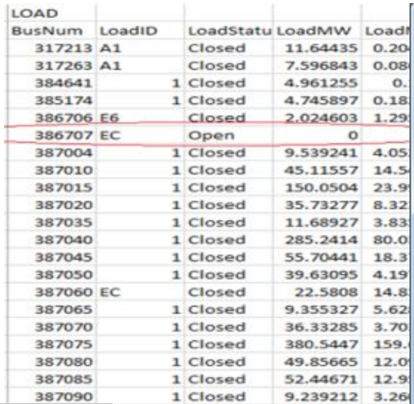
RTU: RTU_20010267

From Bus: Bus_387061 To Bus: Bus_386706 — 5 Active Power Line

From Bus: Bus_387061 To Bus: Bus_386706 — 6 Reactive Power Line

Generator: Gen_6 — 10 Gen MW; 10 Gen MVAR

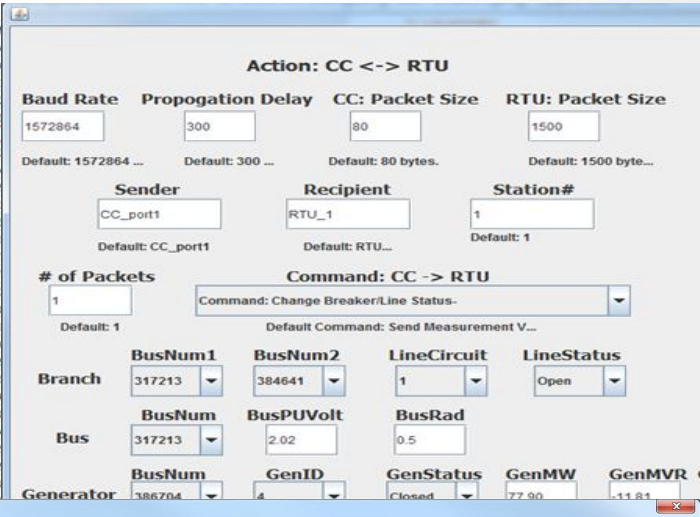
Load: Load_6E — 3 Load MW; 2 Load MVAR



LOAD

BusNum	LoadID	LoadStatu	LoadMW	LoadM
317213	A1	Closed	11.64435	0.20
317263	A1	Closed	7.596843	0.08
384641	1	Closed	4.961255	0.
385174	1	Closed	4.745897	0.18
386706	E6	Closed	2.024603	1.29
386707	EC	Open	0	
387004	1	Closed	9.539241	4.05
387010	1	Closed	45.11557	14.5
387015	1	Closed	150.0504	23.9
387020	1	Closed	35.73277	8.32
387035	1	Closed	11.68927	3.83
387040	1	Closed	285.2414	80.0
387045	1	Closed	55.70441	18.3
387050	1	Closed	39.63095	4.19
387060	EC	Closed	22.5808	14.8
387065	1	Closed	9.355327	5.62
387070	1	Closed	36.33285	3.70
387075	1	Closed	380.5447	159.
387080	1	Closed	49.85665	12.0
387085	1	Closed	52.44671	12.9
387090	1	Closed	9.239212	3.26
	1	Closed	33.00498	9.32
	1	Closed	74.60045	29.8
	1	Closed	61.41096	18.1
	1	Closed	7.658389	2.60
	1	Closed	9.992132	2.51
	1	Closed		

2016-04-08-15-28



Action: CC <-> RTU

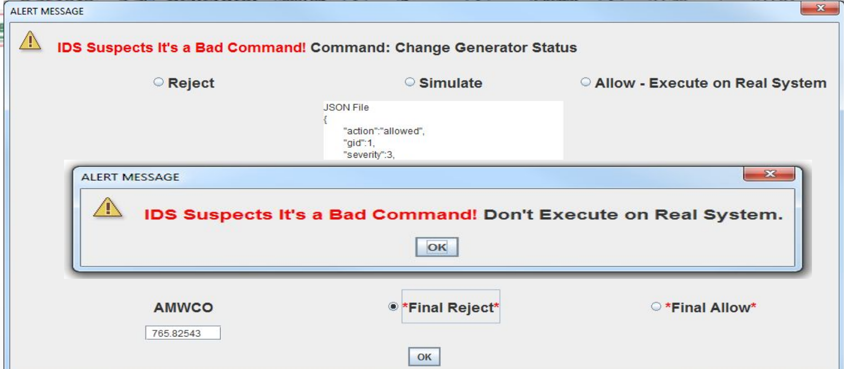
Baud Rate	Propogation Delay	CC: Packet Size	RTU: Packet Size
1572864	300	80	1500
Default: 1572864 ...	Default: 300 ...	Default: 80 bytes.	Default: 1500 byte...

Sender	Recipient	Station#
CC_port1	RTU_1	1
Default: CC_port1	Default: RTU...	Default: 1

# of Packets: 1 (Default: 1)

Command: CC -> RTU: Command: Change Breaker/Line Status- (Default Command: Send Measurement V...)

	BusNum1	BusNum2	LineCircuit	LineStatus	
Branch	317213	384641	1	Open	
	BusNum	BusPUVolt	BusRad		
Bus	317213	2.02	0.5		
	BusNum	GenID	GenStatus	GenMW	GenMVR
Generator	386704	4	Closed	77.90	-11.81



ALERT MESSAGE

IDS Suspects It's a Bad Command! Command: Change Generator Status

○ Reject ○ Simulate ○ Allow - Execute on Real System

JSON File

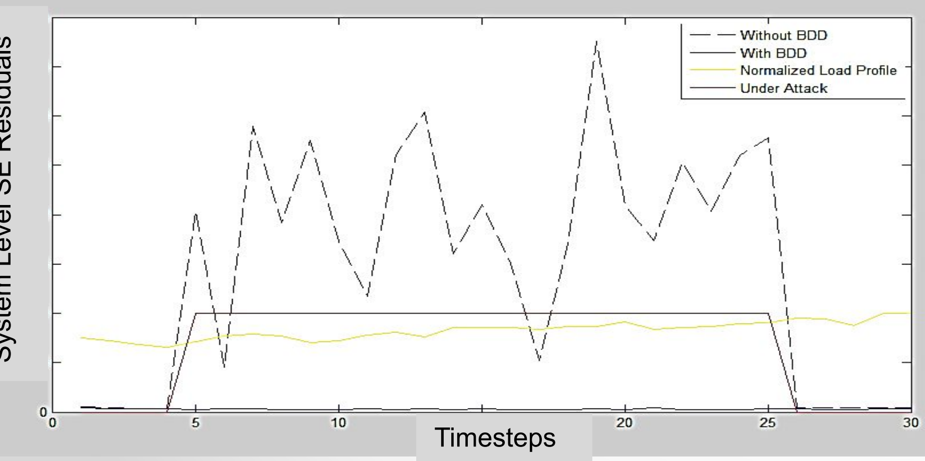
{
"action":"allowed",
"gid":1,
"severity":3,

ALERT MESSAGE

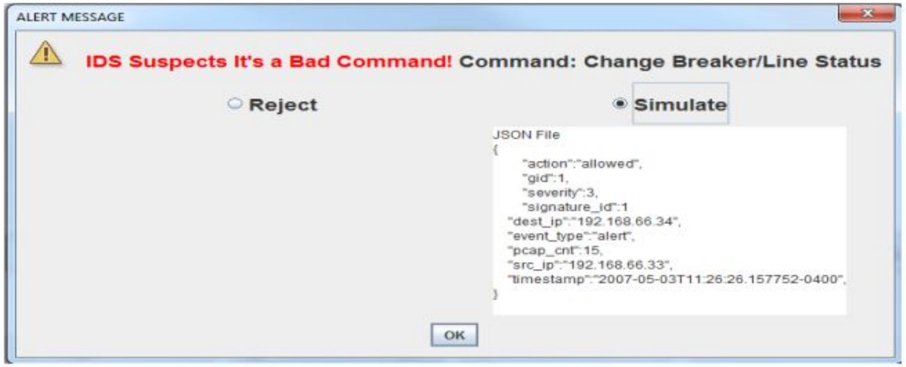
IDS Suspects It's a Bad Command! Don't Execute on Real System.

AMWCO: 765.82543

● *Final Reject* ○ *Final Allow*



Malicious Command Injection



ALERT MESSAGE

⚠ **IDS Suspects It's a Bad Command!** Command: Change Breaker/Line Status

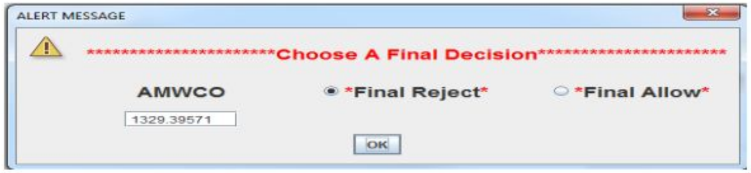
○ Reject ● Simulate

JSON File

```
{
      "action":"allowed",
      "gid":1,
      "severity":3,
      "signature_id":1
  "dest_ip":"192.168.66.34",
  "event_type":"alert",
  "pcap_cnt":15,
  "src_ip":"192.168.66.33",
  "timestamp":"2007-05-03T11:26:26.157752-0400",
}
```

OK

An alert message sent from the RTU to the CC.



ALERT MESSAGE

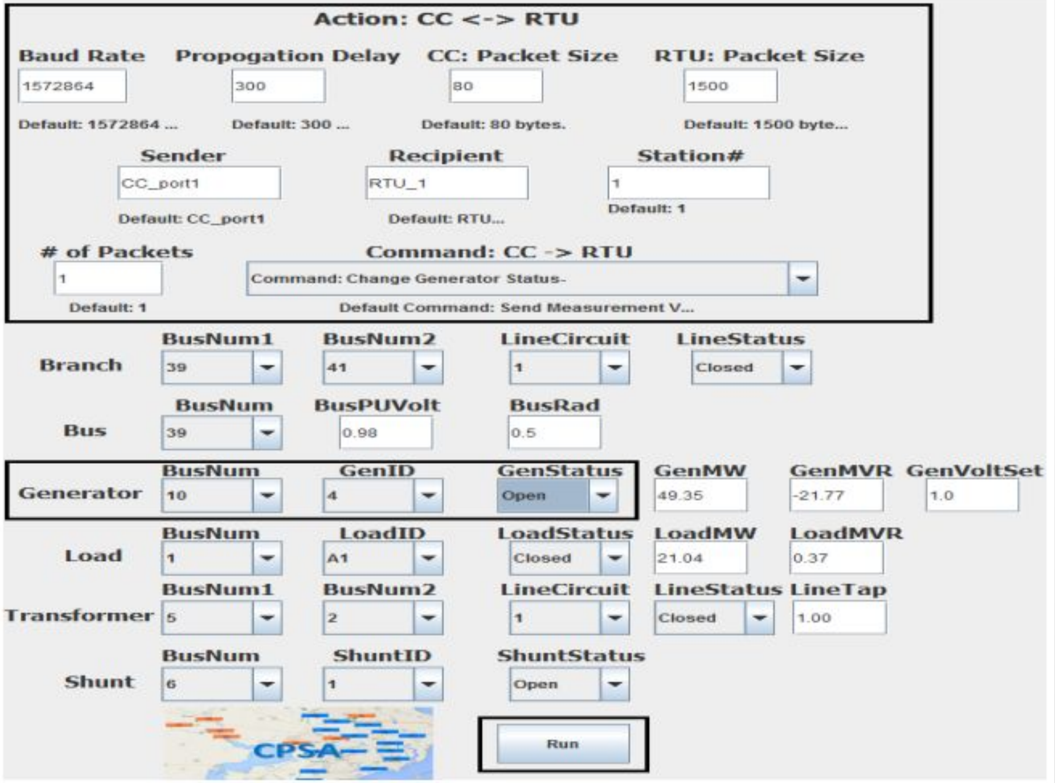
⚠ *************************Choose A Final Decision*************************

AMWCO 1329.39571

● *Final Reject* ○ *Final Allow*

OK

Final decision to accept or reject the command.



Action: CC <-> RTU

Baud Rate	Propogation Delay	CC: Packet Size	RTU: Packet Size
1572864	300	80	1500
Default: 1572864 ...	Default: 300 ...	Default: 80 bytes.	Default: 1500 byte...

Sender	Recipient	Station#
CC_port1	RTU_1	1
Default: CC_port1	Default: RTU...	Default: 1

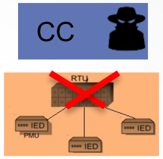
# of Packets	Command: CC -> RTU
1	Command: Change Generator Status- ▾
Default: 1	Default Command: Send Measurement V...

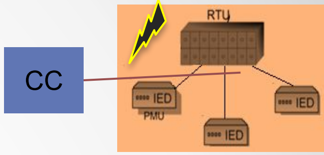
	BusNum1	BusNum2	LineCircuit	LineStatus		
Branch	39 ▾	41 ▾	1 ▾	Closed ▾		
	BusNum	BusPUVolt	BusRad			
Bus	39 ▾	0.98	0.5			
	BusNum	GenID	GenStatus	GenMW	GenMVR	GenVoltSet
Generator	10 ▾	4 ▾	Open ▾	49.35	-21.77	1.0
	BusNum	LoadID	LoadStatus	LoadMW	LoadMVR	
Load	1 ▾	A1 ▾	Closed ▾	21.04	0.37	
	BusNum1	BusNum2	LineCircuit	LineStatus	LineTap	
Transformer	5 ▾	2 ▾	1 ▾	Closed ▾	1.00	
	BusNum	ShuntID	ShuntStatus			
Shunt	6 ▾	1 ▾	Open ▾			

Run

A command simulation GUI at the CC.

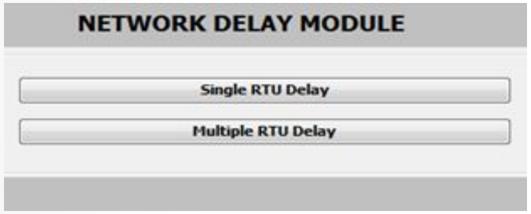
Communication Network Delay & Disabled RTU

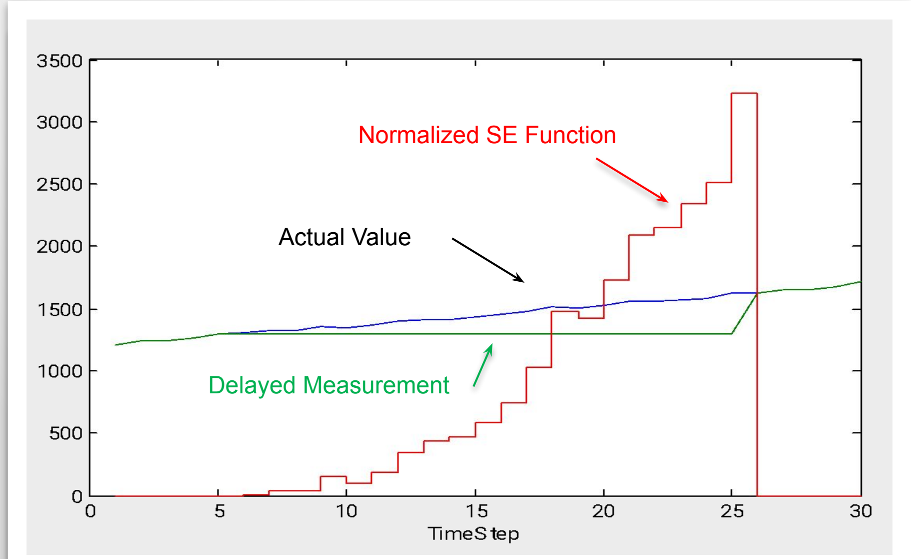




Scenario: Case 3

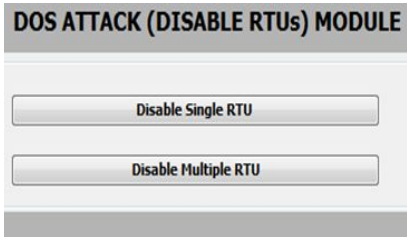
- Attacker floods network with useless packets delaying measurements from RTU to CC.
- Delay is detectable by the SE, which sees increase in measurement residuals.
- If delay persists, SE function increases beyond a threshold and CPSA logic is invoked.

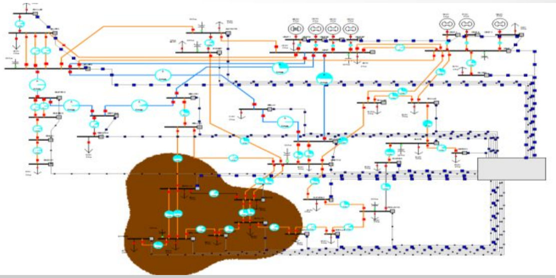

NETWORK DELAY MODULE

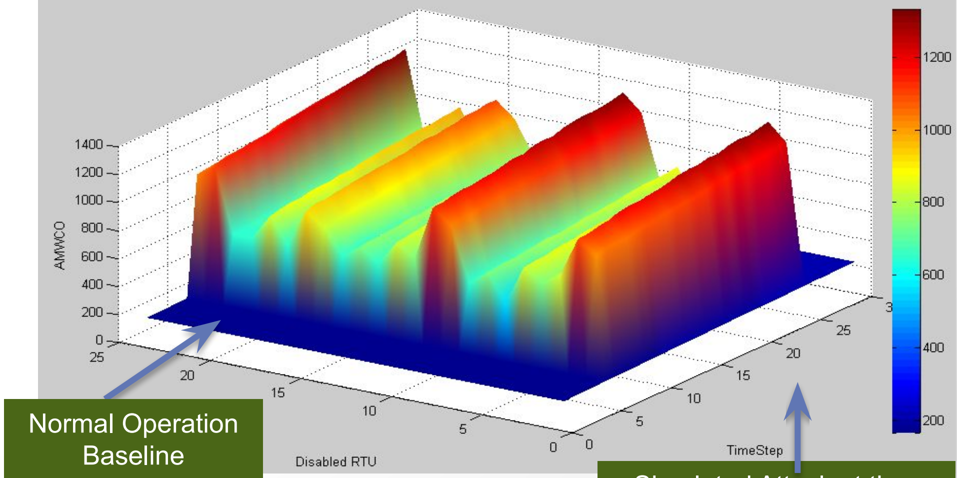


Scenario: Case 4

- Attacker disables CC-RTU link.
- CC cannot receive data from RTU or execute commands.
- Observability analysis identifies unobservable parts.
- Uncontrollable points are identified.
- CPSA simulates attacker worst-case actions.


DOS ATTACK (DISABLE RTUs) MODULE

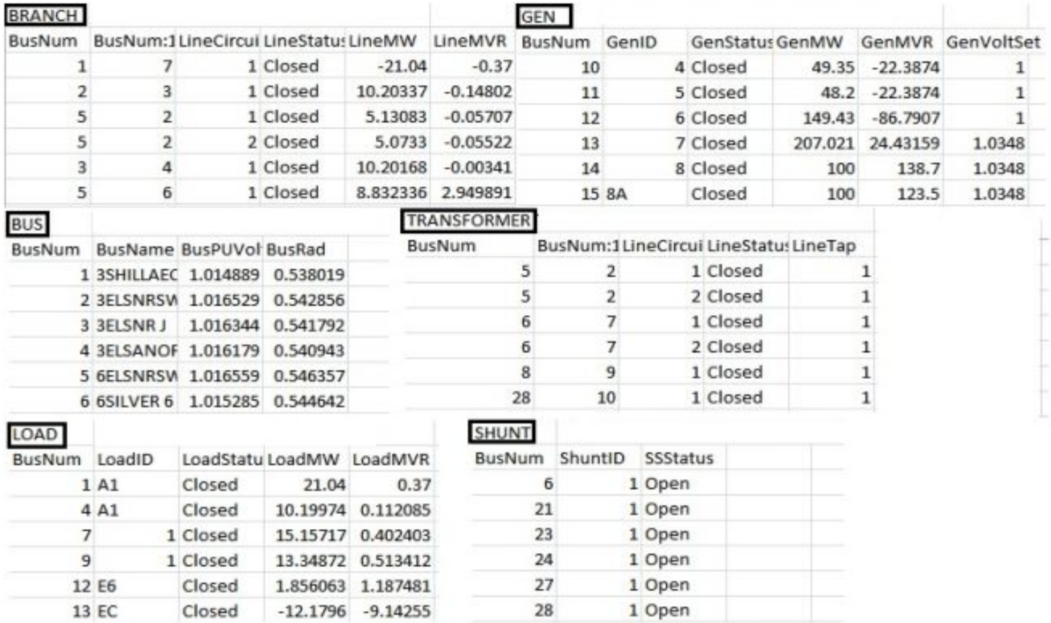




Normal Operation Baseline

Simulated Attack at time steps 5 to 25

Results Monitoring



BRANCH

BusNum	BusNum:1	LineCircui	LineStatus	LineMW	LineMVR
1	7	1	Closed	-21.04	-0.37
2	3	1	Closed	10.20337	-0.14802
5	2	1	Closed	5.13083	-0.05707
5	2	2	Closed	5.0733	-0.05522
3	4	1	Closed	10.20168	-0.00341
5	6	1	Closed	8.832336	2.949891

GEN

BusNum	GenID	GenStatus	GenMW	GenMVR	GenVoltSet
10	4	Closed	49.35	-22.3874	1
11	5	Closed	48.2	-22.3874	1
12	6	Closed	149.43	-86.7907	1
13	7	Closed	207.021	24.43159	1.0348
14	8	Closed	100	138.7	1.0348
15	8A	Closed	100	123.5	1.0348

BUS

BusNum	BusName	BusPUVol	BusRad
1	3SHILLAEC	1.014889	0.538019
2	3ELSNRSW	1.016529	0.542856
3	3ELSNR J	1.016344	0.541792
4	3ELSANOF	1.016179	0.540943
5	6ELSNRSW	1.016559	0.546357
6	6SILVER 6	1.015285	0.544642

TRANSFORMER

BusNum	BusNum:1	LineCircui	LineStatus	LineTap
5	2	1	Closed	1
5	2	2	Closed	1
6	7	1	Closed	1
6	7	2	Closed	1
8	9	1	Closed	1
28	10	1	Closed	1

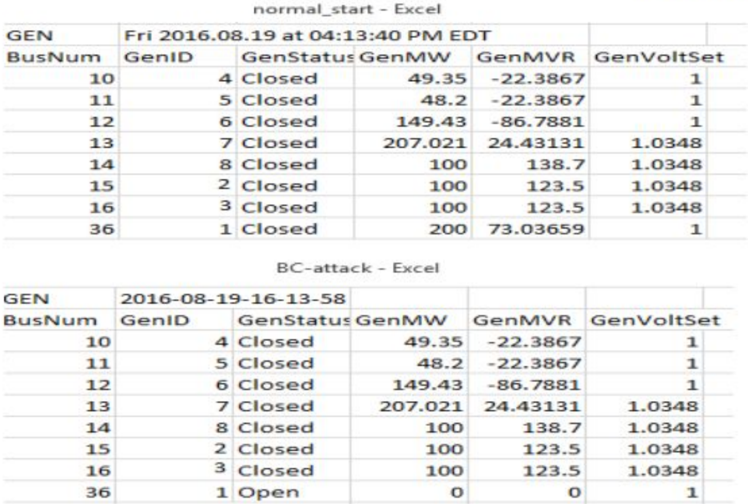
LOAD

BusNum	LoadID	LoadStatu	LoadMW	LoadMVR
1	A1	Closed	21.04	0.37
4	A1	Closed	10.19974	0.112085
7	1	Closed	15.15717	0.402403
9	1	Closed	13.34872	0.513412
12	E6	Closed	1.856063	1.187481
13	EC	Closed	-12.1796	-9.14255

SHUNT

BusNum	ShuntID	SSStatus
6	1	Open
21	1	Open
23	1	Open
24	1	Open
27	1	Open
28	1	Open

A sample meta-data of the power system components.



normal_start - Excel

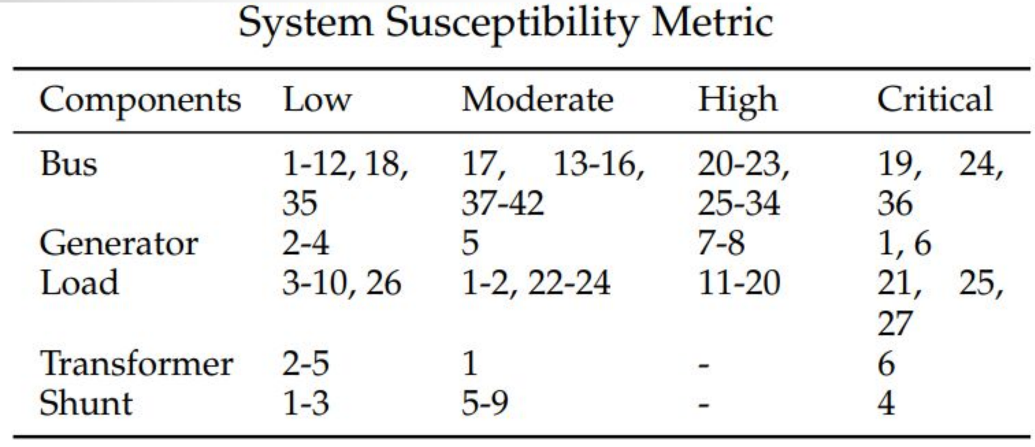
GEN	Fri 2016.08.19 at 04:13:40 PM EDT				
BusNum	GenID	GenStatus	GenMW	GenMVR	GenVoltSet
10	4	Closed	49.35	-22.3867	1
11	5	Closed	48.2	-22.3867	1
12	6	Closed	149.43	-86.7881	1
13	7	Closed	207.021	24.43131	1.0348
14	8	Closed	100	138.7	1.0348
15	2	Closed	100	123.5	1.0348
16	3	Closed	100	123.5	1.0348
36	1	Closed	200	73.03659	1

BC-attack - Excel

GEN	2016-08-19-16-13-58				
BusNum	GenID	GenStatus	GenMW	GenMVR	GenVoltSet
10	4	Closed	49.35	-22.3867	1
11	5	Closed	48.2	-22.3867	1
12	6	Closed	149.43	-86.7881	1
13	7	Closed	207.021	24.43131	1.0348
14	8	Closed	100	138.7	1.0348
15	2	Closed	100	123.5	1.0348
16	3	Closed	100	123.5	1.0348
36	1	Open	0	0	1

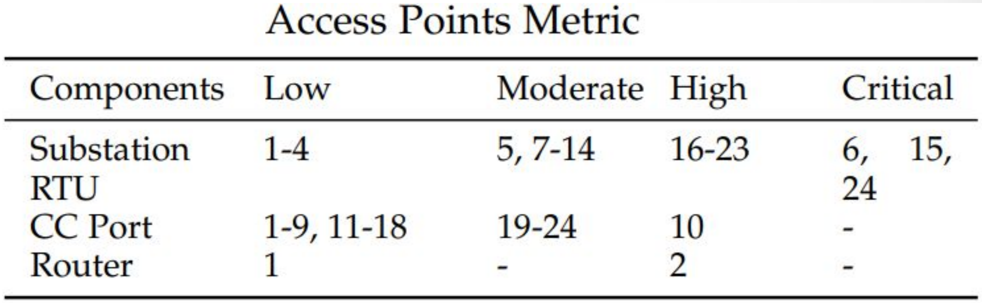
Legitimate vs. malicious command to open
a generator breaker (Bus number 36, generator ID 1).

Results Monitoring



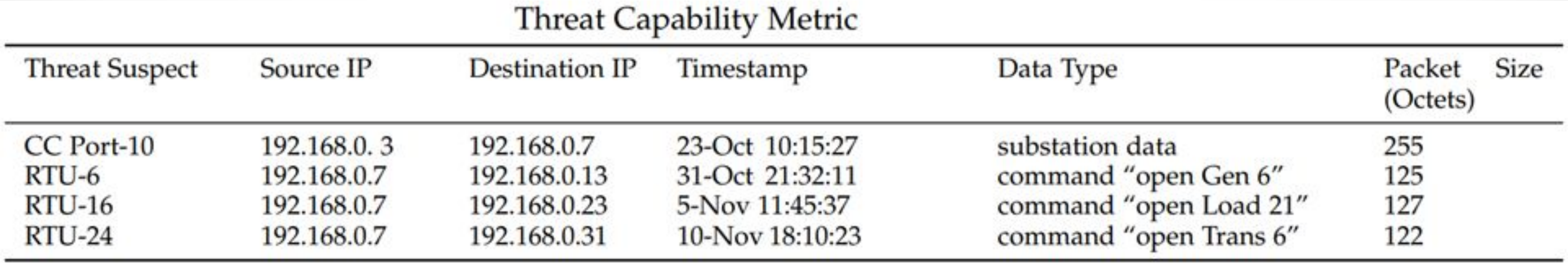
System Susceptibility Metric

Components	Low	Moderate	High	Critical
Bus	1-12, 18, 35	17, 13-16, 37-42	20-23, 25-34	19, 24, 36
Generator	2-4	5	7-8	1, 6
Load	3-10, 26	1-2, 22-24	11-20	21, 25, 27
Transformer	2-5	1	-	6
Shunt	1-3	5-9	-	4



Access Points Metric

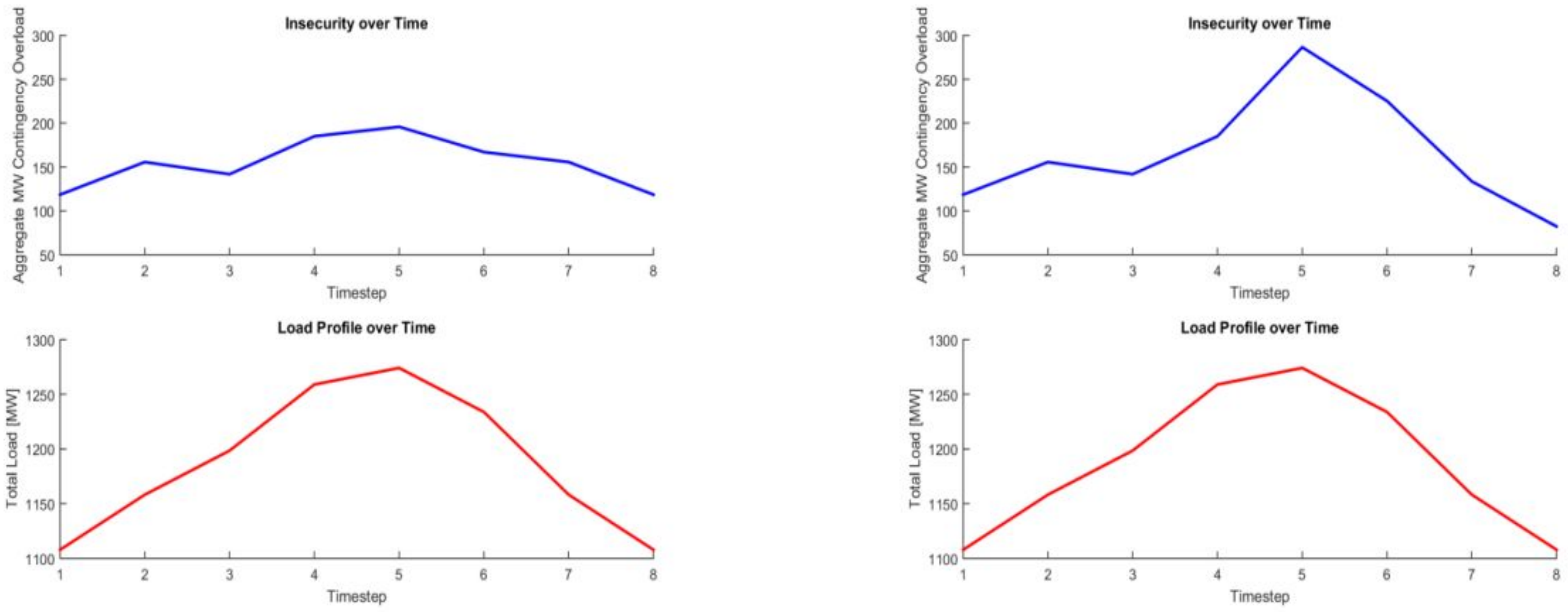
Components	Low	Moderate	High	Critical
Substation RTU	1-4	5, 7-14	16-23	6, 15, 24
CC Port	1-9, 11-18	19-24	10	-
Router	1	-	2	-



Threat Capability Metric

Threat Suspect	Source IP	Destination IP	Timestamp	Data Type	Packet Size (Octets)
CC Port-10	192.168.0. 3	192.168.0.7	23-Oct 10:15:27	substation data	255
RTU-6	192.168.0.7	192.168.0.13	31-Oct 21:32:11	command "open Gen 6"	125
RTU-16	192.168.0.7	192.168.0.23	5-Nov 11:45:37	command "open Load 21"	127
RTU-24	192.168.0.7	192.168.0.31	10-Nov 18:10:23	command "open Trans 6"	122

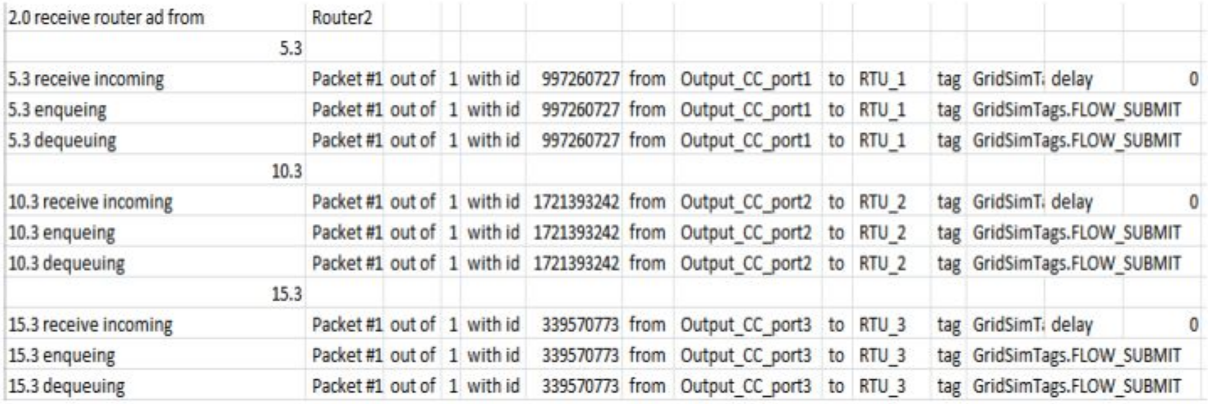
Malicious Command Impact Monitoring



(a) Normal operation.

(b) Malicious command injection operation.

Detecting malicious operation at timestep 5 by comparing the SysAMWCO



2.0 receive router ad from	Router2												
5.3													
5.3 receive incoming	Packet #1	out of	1	with id	997260727	from	Output_CC_port1	to	RTU_1	tag	GridSimTa	delay	0
5.3 enqueing	Packet #1	out of	1	with id	997260727	from	Output_CC_port1	to	RTU_1	tag	GridSimTags.FLOW_SUBMIT		
5.3 dequeuing	Packet #1	out of	1	with id	997260727	from	Output_CC_port1	to	RTU_1	tag	GridSimTags.FLOW_SUBMIT		
10.3													
10.3 receive incoming	Packet #1	out of	1	with id	1721393242	from	Output_CC_port2	to	RTU_2	tag	GridSimTa	delay	0
10.3 enqueing	Packet #1	out of	1	with id	1721393242	from	Output_CC_port2	to	RTU_2	tag	GridSimTags.FLOW_SUBMIT		
10.3 dequeuing	Packet #1	out of	1	with id	1721393242	from	Output_CC_port2	to	RTU_2	tag	GridSimTags.FLOW_SUBMIT		
15.3													
15.3 receive incoming	Packet #1	out of	1	with id	339570773	from	Output_CC_port3	to	RTU_3	tag	GridSimTa	delay	0
15.3 enqueing	Packet #1	out of	1	with id	339570773	from	Output_CC_port3	to	RTU_3	tag	GridSimTags.FLOW_SUBMIT		
15.3 dequeuing	Packet #1	out of	1	with id	339570773	from	Output_CC_port3	to	RTU_3	tag	GridSimTags.FLOW_SUBMIT		

Event logs maintained at the intermediate routers.

Thank You
☺