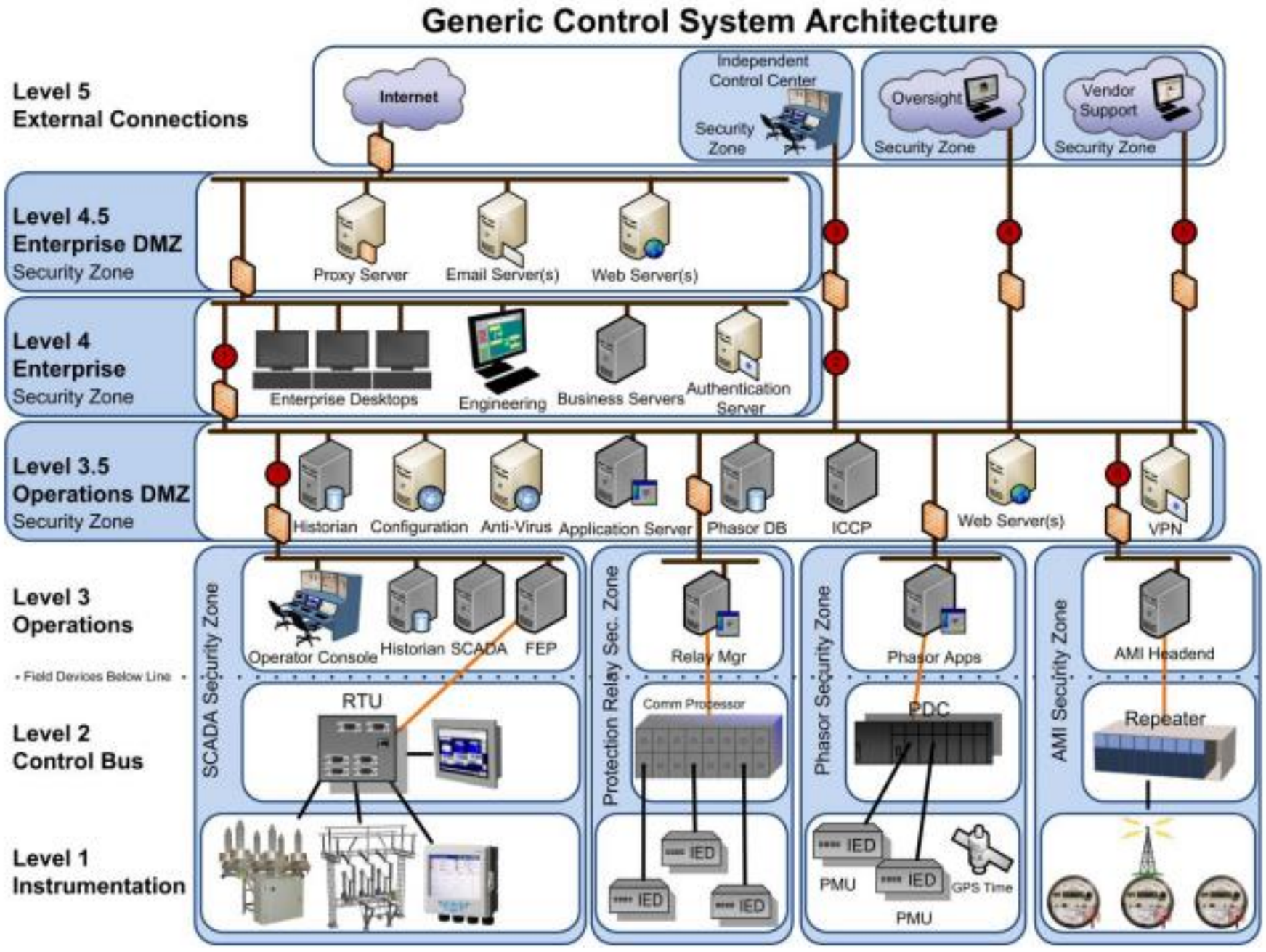
A distributed cyberattack diagnosis scheme for malicious protection operation based on IEC 61850

Md Touhiduzzaman
Pacific Northwest National Lab

Adam Hahn, Saeed Lotfifard
Washington State University (WSU)

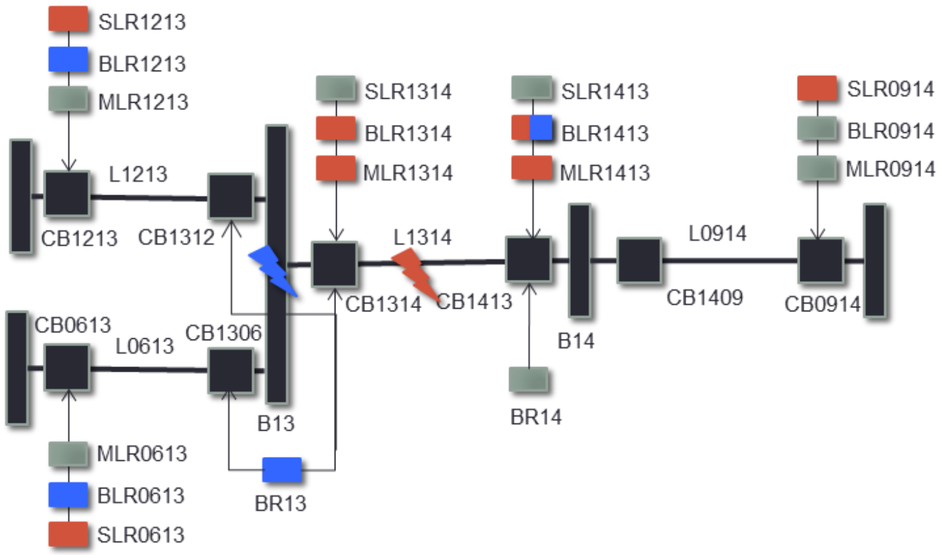
2019 Industrial Control System Security (ICSS) Workshop
December 10th 2019

Smart Grid Architecture



R. Mahan et. al, “Secure Data Transfer Guidance for Industrial Control and SCADA Systems ” PNNL report 20776, 2011

Protection Overview



14 bus power system

- Line Schemes (Main, Backup, Secondary Backup)
- Bus Schemes (Bus, Secondary Backup)

Key Points

- Target multiple devices to disable
- Secondary/backup protection in neighboring substations

Scenario 1: Bus Fault

IEC 61850

Messages:

1. Pickup Fault
   - BR13
   - BLR1413
   - BLR0613
   - BLR1213

→ 2. Operate
   - BR13

Scenario 2: Line Fault

IEC 61850

Messages:

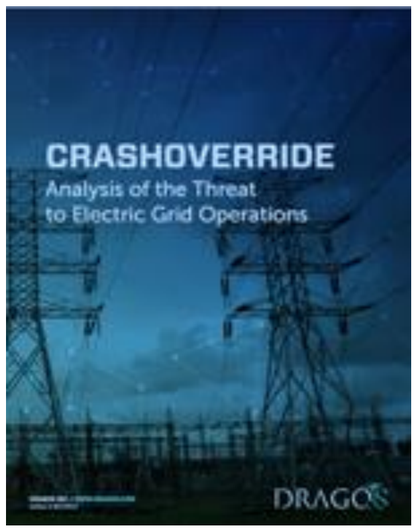
1. Pickup Fault
   - MLR1314
   - MLR1413
   - BLR1314
   - BLR1413
   - SLR0914
   - SLR1213
   - SLR06013

→ 2. Operate
   - MLR1314
   - MLR1413

X. Luo and M. Kezunovic. Implementing fuzzy reasoning Petri-nets for fault section estimation. Power Delivery, IEEE Transactions on, 23(2):676–685, Apr. 2008.

INDUSTROYER/ CRASHOVERRIDE

Anton Cherepanov. WIN32/INDUSTROYER: A new threat for industrial control systems, ESET. June 12, 2017.



CRASHOVERRRIDE: Analysis of the Threat to Electric Grid Operations. Dragos. Version: 2.20170613.

CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack By Joe Slowik, Dragos Inc. *August 15, 2019.*

Modules

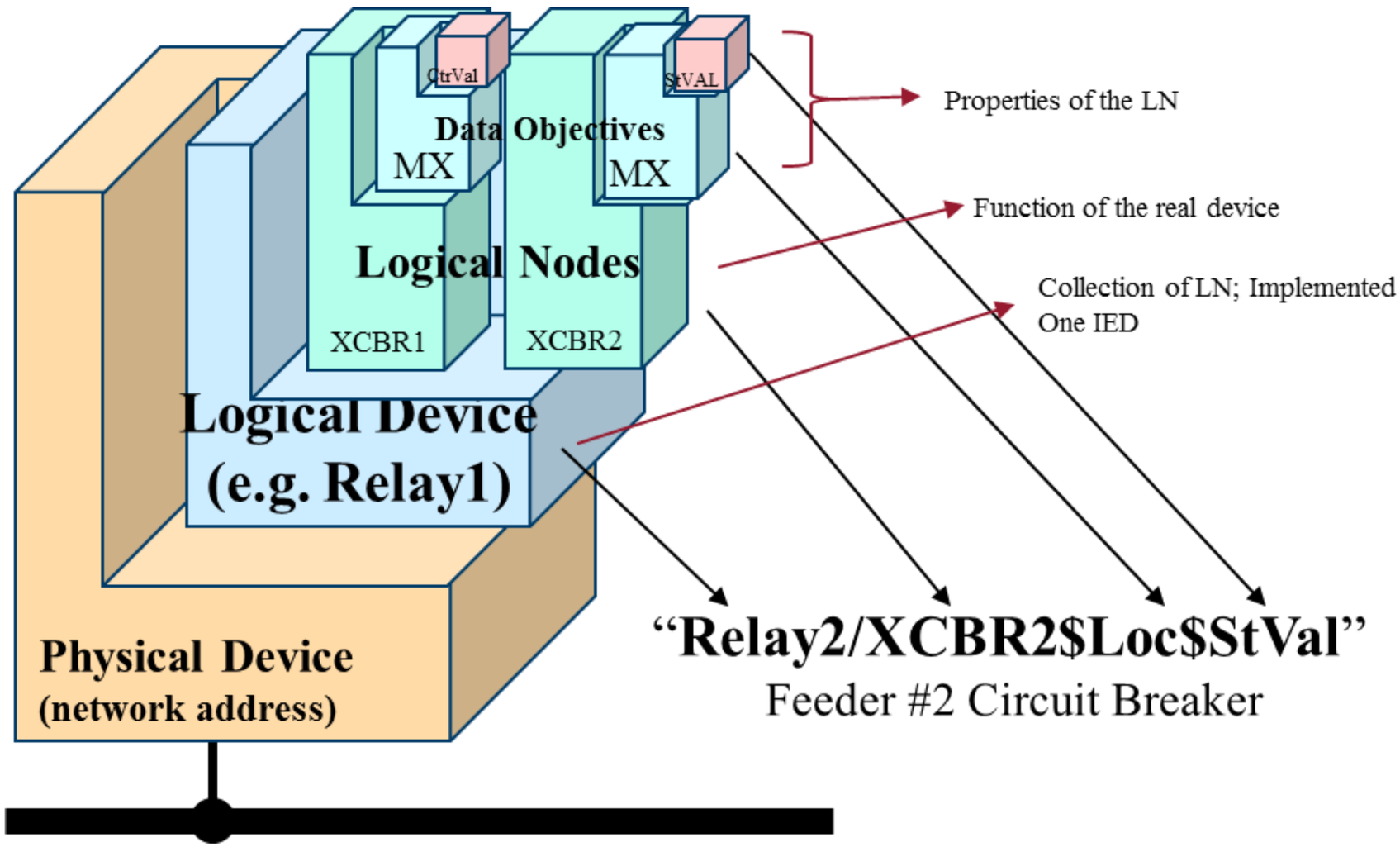
Protocols:
- IEC 60870-5-101
- IEC 60870-5-104
- IEC 61850 (MMS)
- OPC

General:
- Backdoor/C2
- Port scanning
- DoS exploits

Modules referenced config file for target info
- attempted to enumerate IOAs

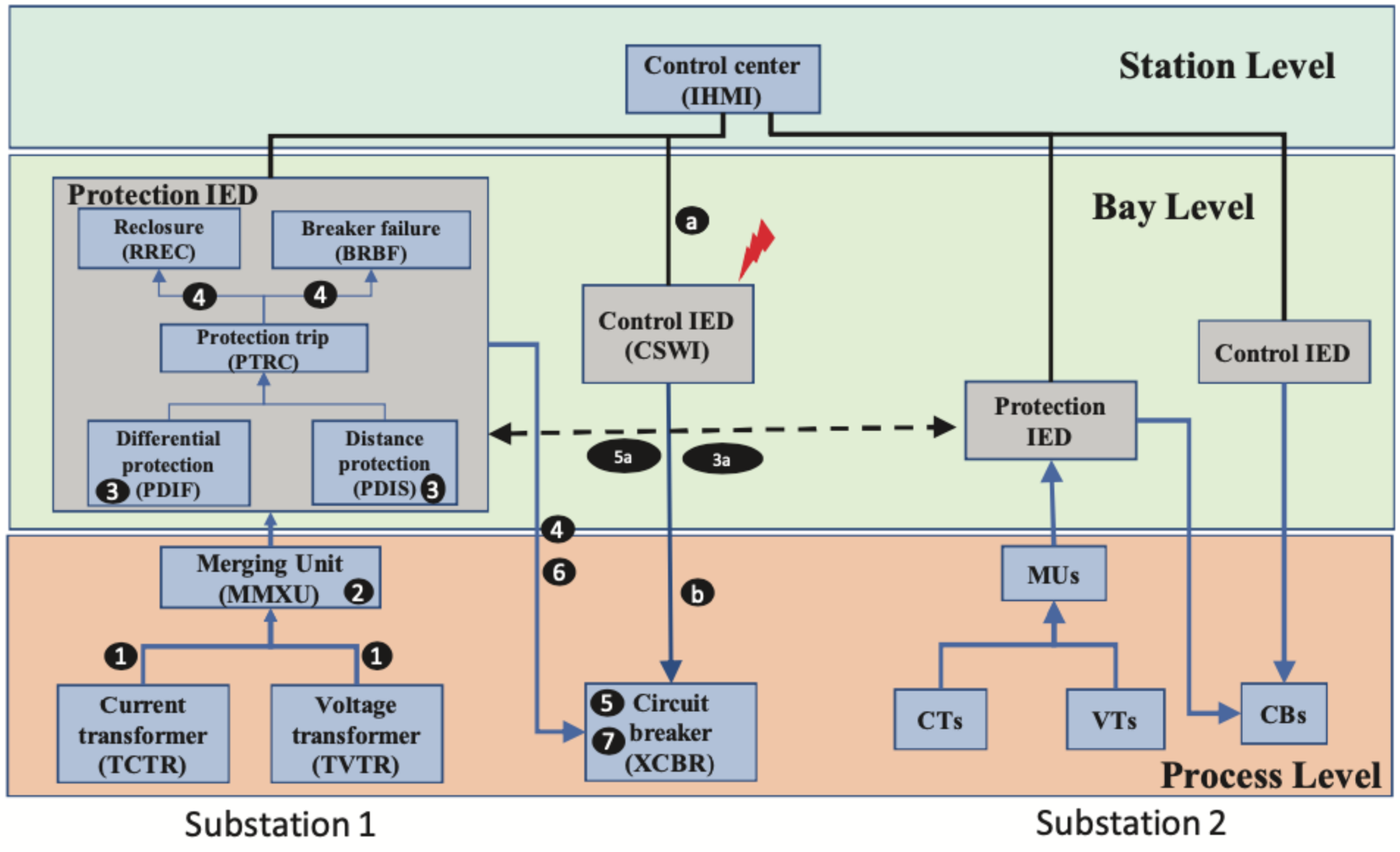
61850
- Searched for config file
- Enumerate all devices in subnet
- Identify switching/CB points (CSW)
- Operate switches:
  - (i)Continually open
  - (ii)Toggle between open/close
  - (iii)Other…

IEC 61850 Overview



LN	Definition
XCBR	Switch with circuit breaker
MMXU	measurement sampling through merging unit
TCVR	Voltage measurement
TCTR	Current measurement
CSWI	Circuit breaker control
PDIS	Distance fault identification
PDIF	Differential fault identification
PTRC	Protection trip conditioning
BRBF	Breaker failure function
RREC	Re-closer function

IEC 61850
Protection (1)



GOOSE messages for the substation event

1. CT and VT measurement (TCTR. Amp. instMag and TVTR. Op. general)
2. Sampling the measurement (MMXU. MX. Amp or vol)
3. Distance or differential protection Operation (PDIS. Op. general or PDIF. Op. general)

3a. For distance send command to zonal substations

4. Protection scheme operation
   - Send command to XCBR LN (XCBR. Pos.ctlVal)
   - Send command to RREC LN(RREC. Op. general)
   - Send command to BRBF LN (BRBF. OpLn)
5. Circuit breaker open

5a. Local breaker fail to open, Re-trip backup breaker (RBRF.OpEx)

6. CB reclosure signal
7. CB reclosed

a. Initiate CB command from IMHI (IHMI.Mod.stVal)

b. CWSI LN request the XCBR LN to operate (CSWI.Pos.ctlVal)

IEC 61850 Protection (2)

Sequence of GOOSE messages for different substation operation

(*i*) Protection operation

1 2 3 3a 4 5 6 7

(*ii*) Breaker failure operation

1 2 3 4 5a

(*iii*) Control operation

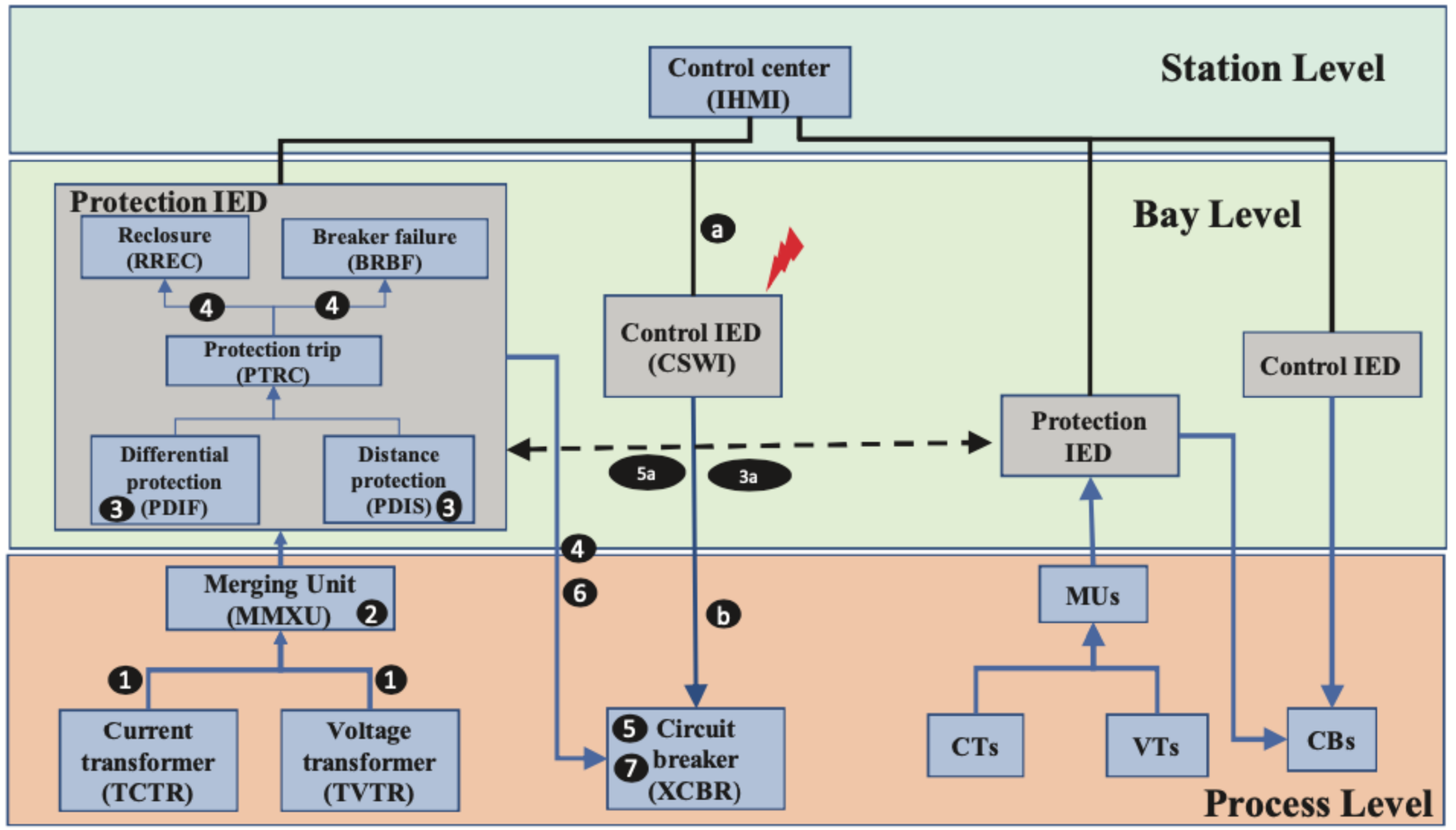
a b 5 6 7

Sequence of GOOSE messages for CRASHOVERRIDE malware

b 5

Bi-directional communication

Uni directional communication



Question

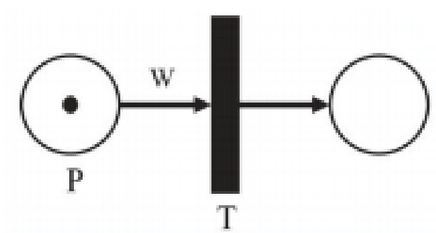
Can we detect malicious IEC 61850 communication sequences?

Petri Net

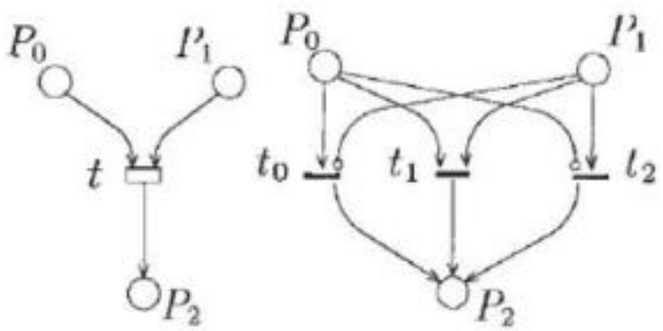
- Agent oriented bipartite graph that defined as

$$N = (Place, transition, flow, weight) = (P, T, F, W)$$

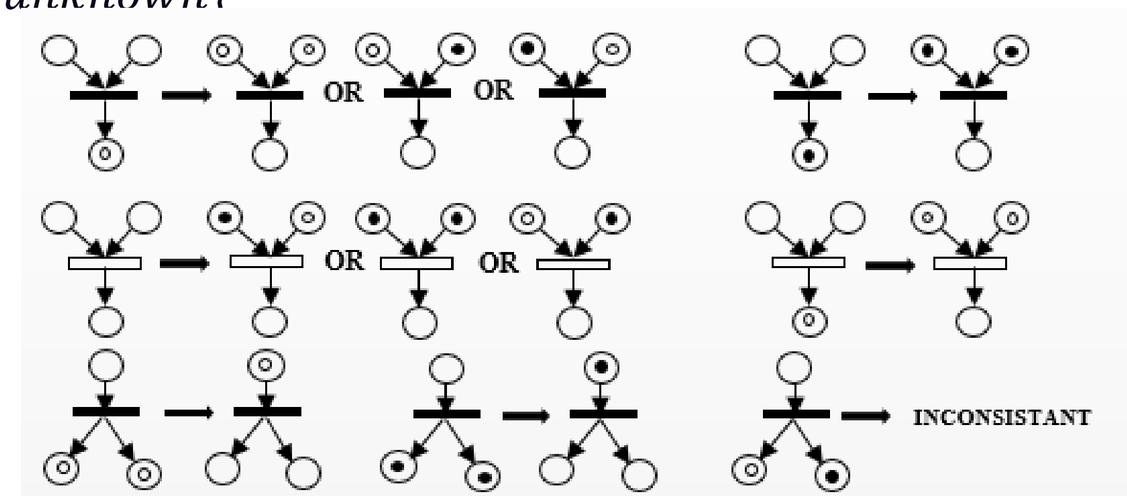
- Extended by introducing inhibitor arc (act as reverse logic of input)
- Backward reachability analysis: Diagnosis incorrect behavior by analyzing the firing rule in backward manner
  - Three logical value are considered $\{truth, false, unknown\}$



Simple Petri net model

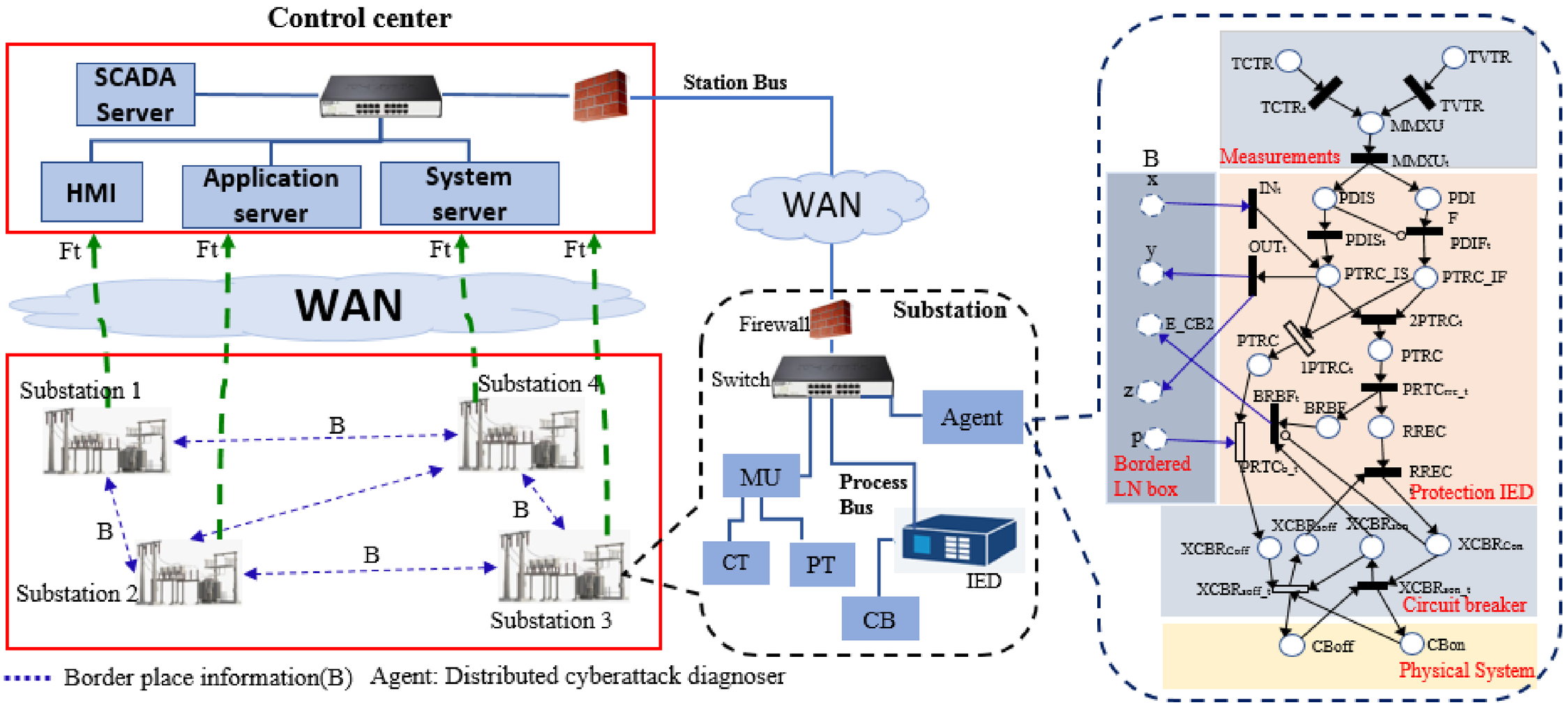


OR-transition



Backward firing rules

Hierarchical behavioral petri net (BPN) model for substation



Distributed Cyberattack Diagnosis Solution (DCDS)

- The DCDS for substation i is defined as:

$$DCDS_i = \{N_i, B_i, Ft_i, (\gamma_i^+, \gamma_i^-), \zeta\}$$

Here, N is the BPN model, B is the set of border place, Ft is the set of possible fault event, (γ_i^+, γ_i^-) initial local observation and ζ is the final local observation

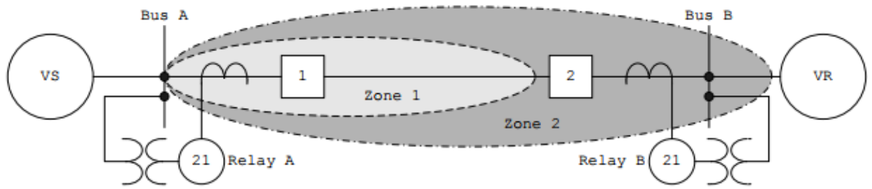
- The list of possible event scenarios are:

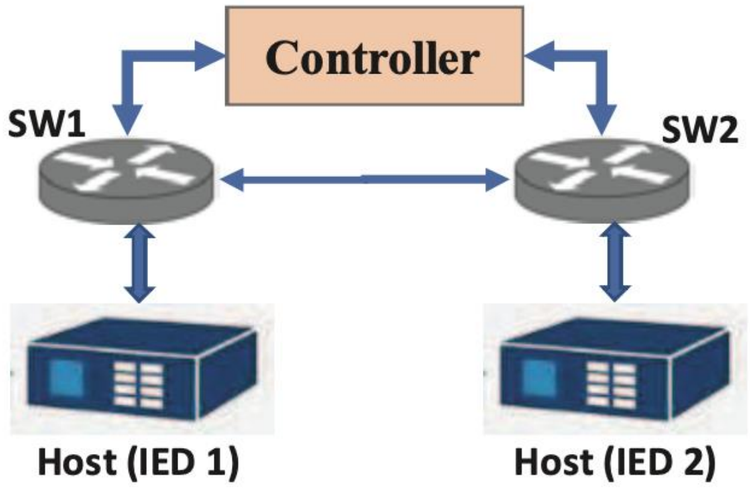
$$\begin{aligned}\zeta = \zeta(Ft, B) = \zeta(Ft_{dis}, Ft_{dif}, f^+, f^-,) \\ = S_1(f^+, Ft_{dis}) + S_2(f^-, Ft_{dis}) + \\ S_3(f^+, Ft_{dif}) + S_4(f^-, Ft_{dif})\end{aligned}$$

- Backward reachability algorithms used to detect whether event sequence consistent with normal event/fault

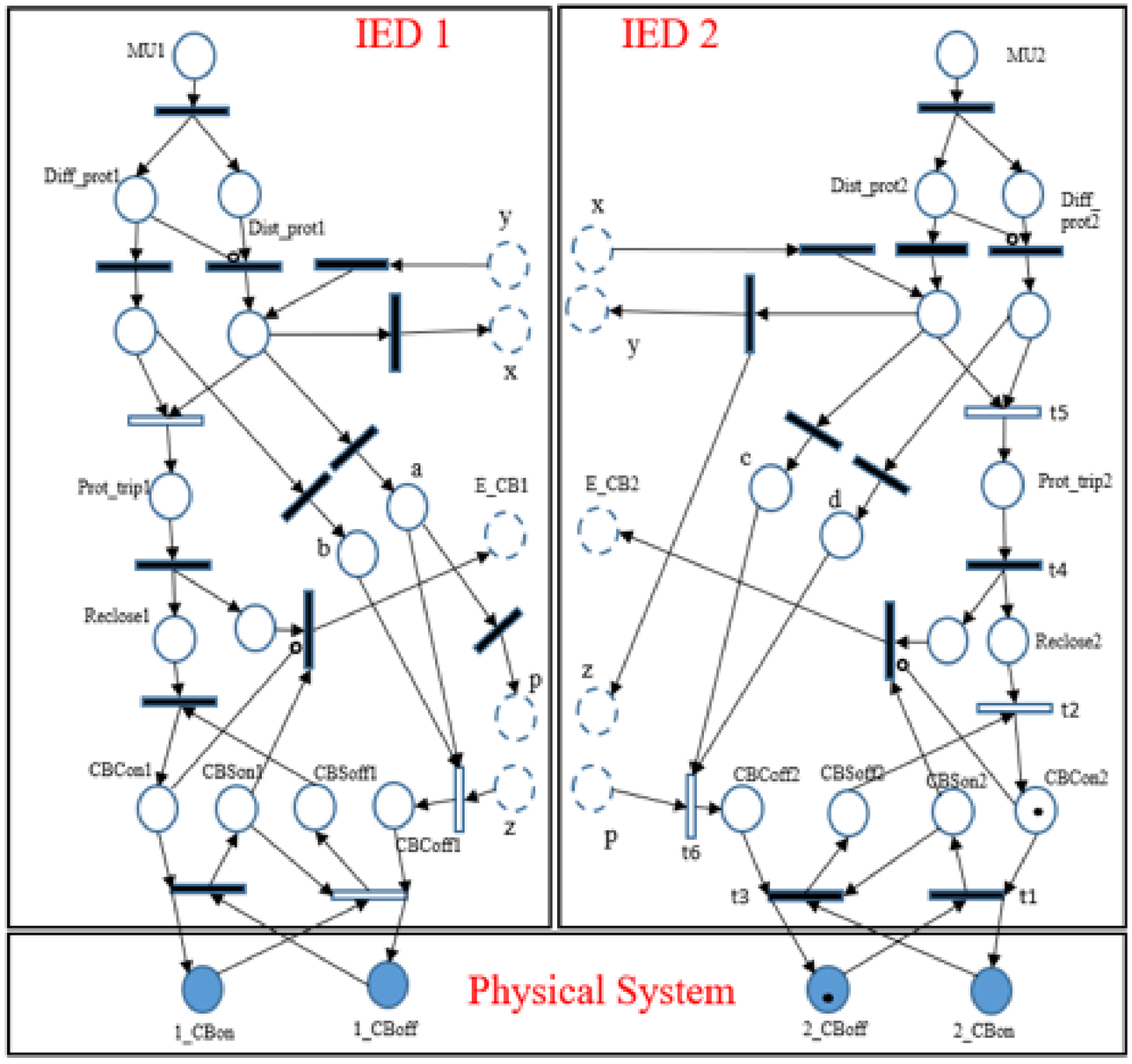
Case Study

2-bus system model





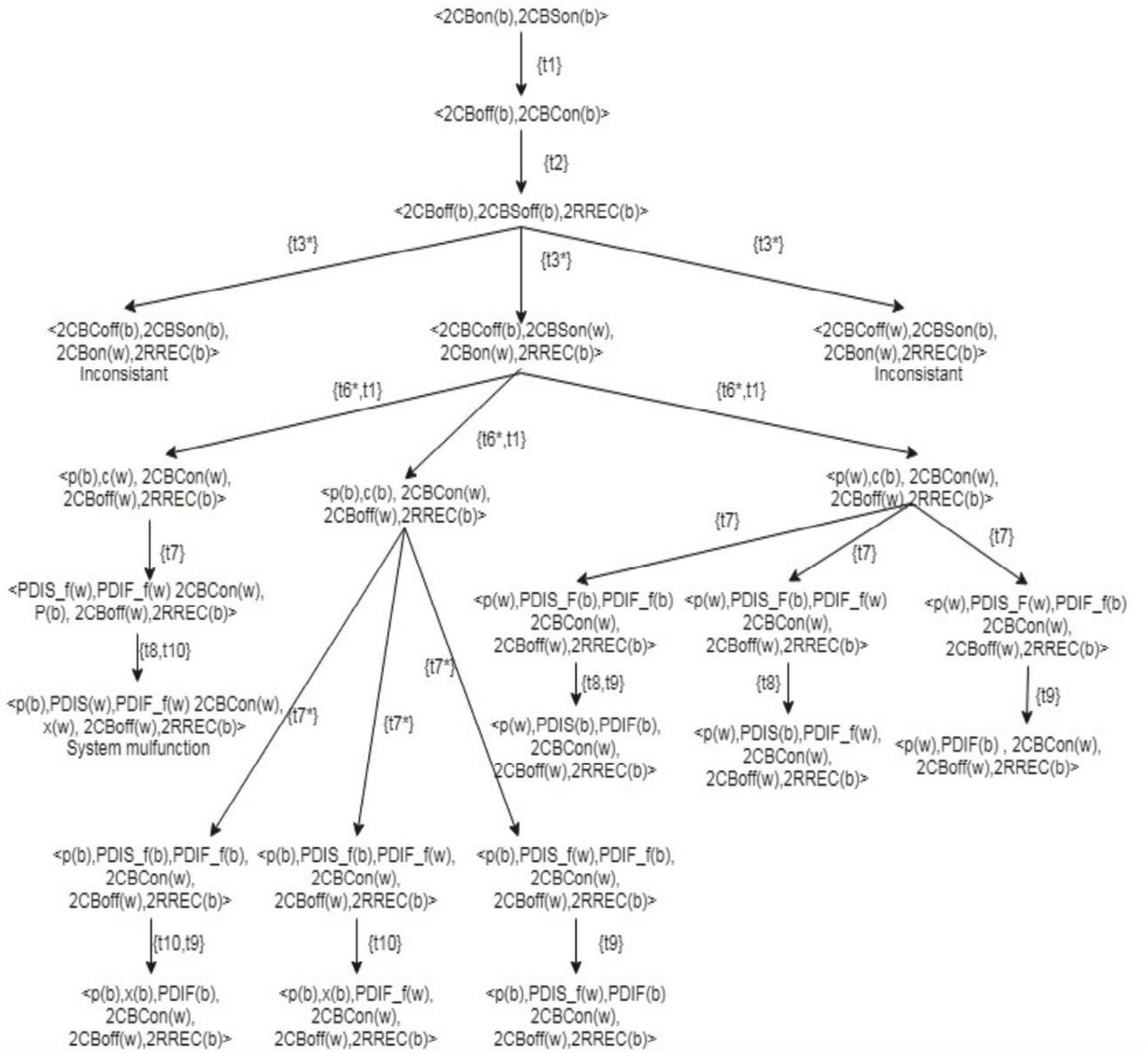
Mininet simulation topology



BPN model for 2-bus system

Results

Event: Substation 2 CB trips, deter set of valid sequences



Backward reachability graph

B-W analysis for 2-bus system

	< p, x>	<PDIF, PDIS>	State
<2CBC$_{off}$(b),2CBS$_{on}$(b), 2CB$_{on}$(w),2RREC(b)>	< ∅, ∅ >	< ∅, ∅ >	Inconsistency (cyber-attack)
<2CBC$_{off}$(w),2CBS$_{on}$(b), 2CBon(w),2RREC(b)>	< ∅, ∅ >	< ∅, ∅ >	Inconsistcncy (cyber-attack)
<p(b),PDIS(w),PDIF_f(w), 2CBC$_{on}$(w), x(w), 2CB$_{off}$(w),2RREC(b)>	< b, w>	< w, ∅>	System malfunction
<p(w),PDIS(b),PDIF(b), 2CBC$_{on}$(w), 2CBoff(w),2RREC(b)>	< w, ∅>	< b, b>	Bus 2 & line fault(z1 for sub2)
<p(w),PDIS(b),PDIF_f(w), 2CBC$_{on}$(w), 2CB$_{off}$(w),2RREC(b)>	< w, ∅>	< b, ∅>	Line fault
<p(w),PDIF(b) , 2CBC$_{on}$(w), 2CB$_{off}$(w),2RREC(b)>	< w, ∅>	< ∅, b>	Bus 2 fault
<p(b),x(b),PDIF(b), 2CBC$_{on}$(w), 2CB$_{off}$(w),2RREC(b)>	< b, b>	< ∅, ∅>	Bus 2 & line fault(z1 for sub2)
<p(b),x(b),PDIF_f(w), 2CBC$_{on}$(w), 2CB$_{off}$(w),2RREC(b)>	< b, b>	< ∅, ∅>	Line fault
<p(b),PDIS_f(w),PDIF(b) 2CBC$_{on}$(w), 2CB$_{off}$(w),2RREC(b)>	< b, ∅ >	< ∅, b>	System malfunction

Simulation

- Four different scenario was emulated through Mininet and analyze GOOSE publish/subscribe bit pattern.
- Use ***libiec61850*** package
- Check how many sequences are required to open the CB
- In border place operation, P and X should subscribe simultaneously

BPN model verification by analyzing events

LN (IED2)	Case 1: Normal Operation		Case 2: Differential Fault		Case 3: system Malfunction		Case 4: Cyber Attack	
	Sequence	Bit	Sequence	Bit	Sequence	Bit	Sequence	Bit
MMXU	1	1	1	1	1	1	1	1
PDIF	-	0	2	**1**	-	0	-	**0**
PDIS	-	0	-	0	-	0	-	**0**
X	-	0	-	0	-	**0**	-	**0**
Y	-	0	-	0	-	0	-	**0**
Z	-	0	-	0	-	0	-	**0**
P	-	0	-	0	1	**1**	-	**0**
PTRC	--	0	3	1	2	1	2	1
RREC	-	0	3	1	-	0	2	1
BRBF	-	0	3	1	-	0	2	1
XCBR	-	0	4	1	3	1	3	1

Conclusion

Protection key to grid operations

Increased target for attack

IEC 61850 introduces complex control sequences

Need techniques to monitor spatial and temporal aspect of communications

Distributed Petri net models used to detect malicious behavior

Attacks introduce anomalous communication sequences

thank you.

a.hahn@wsu.edu