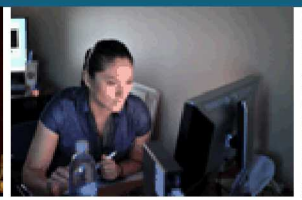
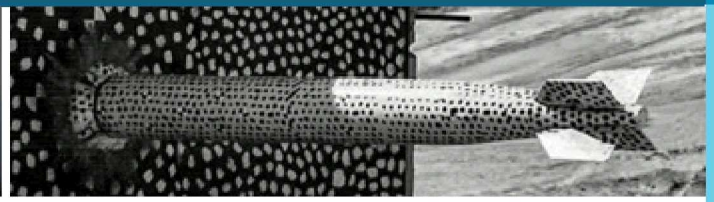
SAND2018-8932C

Measurement and Analysis of Cyber Resilience in Control Systems: An Illustrative Example





PRESENTED BY

Nicholas Jacobs, Shamina Hossain-McKenzie, Eric Vugrin

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2018-XXXX XX

Outline

What is Cyber Resilience?

Load Frequency Control Example

Modeling Cyber in a Control System

Measuring Cyber Impact

- Security
- Resilience

Scenarios

Results and Discussion

What is Cyber Resilience?

Increasing calls for cyber resilience:

- PPD-21
- EO 13636 – among others
- DOD DSB Task Force on Cyber Deterrence (February 2017)
- DHS & DOE Quadrennial Reviews

But how do we achieve it in a measurable way?

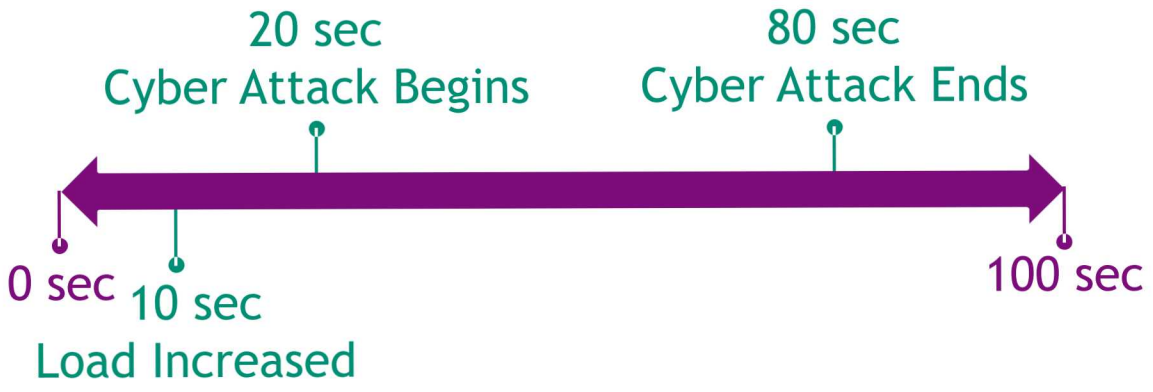
- Quantitative
- Efficacy and performance of option A vs option B vs option C?

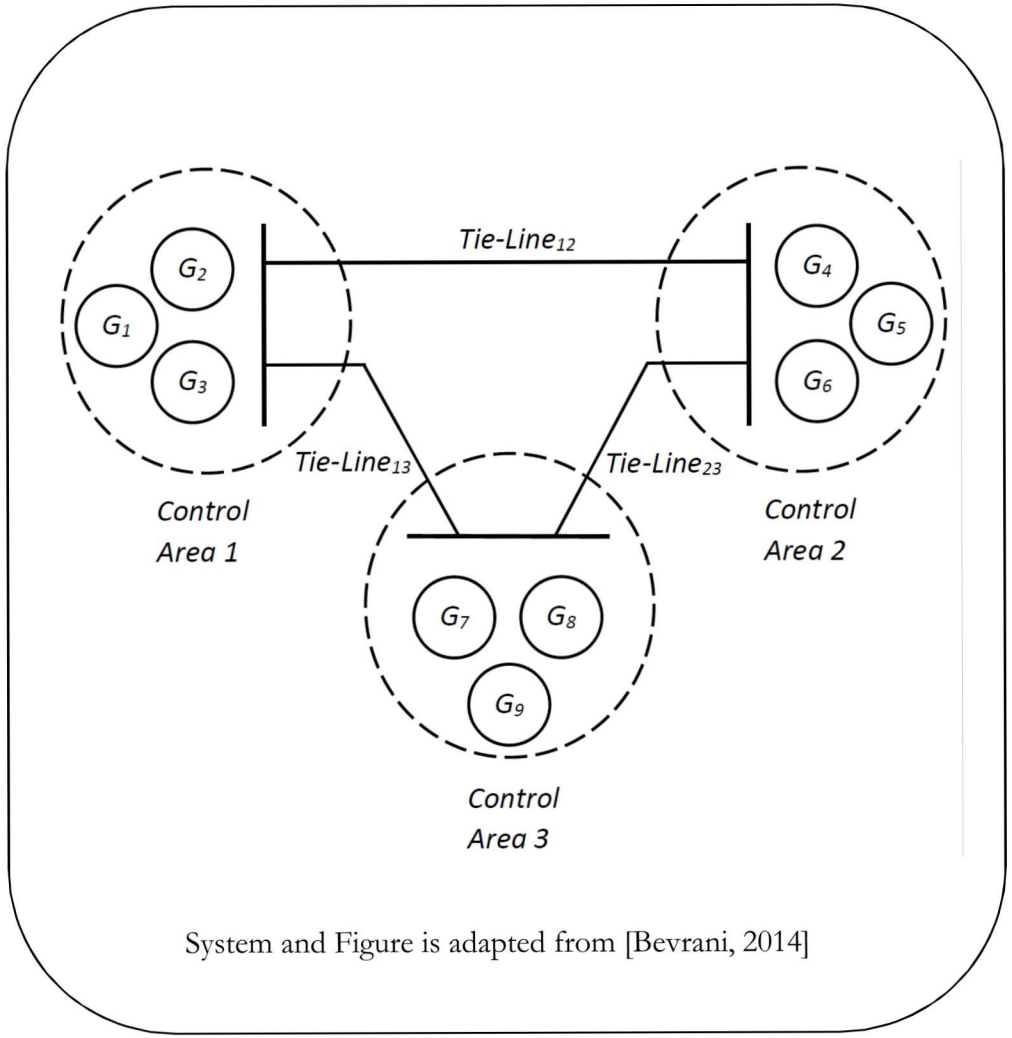
Informally, cyber resilient systems are able to execute required mission parameters despite an hostile cyber-threat environment.

Case Study: Load Frequency Control (LFC)

LFC provides secondary regulation of generation with respect to system frequency error

Timeline





System and Figure is adapted from [Bevrani, 2014]

Source: H. Bevrani "*Robust Power System Frequency Control, 2nd Edition,*" 2014.

Modeling the System

General form:

$$\dot{x}(t) = \mathbf{A}x(t) + \mathbf{B}u(t) + w(t)$$
$$y(t) = \mathbf{C}x(t) + \mathbf{D}u(t) + v(t)$$

Where's the Cyber?

- Not obvious where the connection between cyber action and control system dynamics occurs

In short:

- A cyber attack will modify the structure of the control system
- This will affect the performance of the control system

Measuring Cyber Impact

Security vs Resilience metrics
- Loss to system security vs loss to system ability to provide service

Cost to system security - Impact Sub Score (ISC)
- Sub-component of the Common Vulnerability Scoring System (CVSS)
- Each impact component is graded as {'None': 0, 'Low': 0.22, 'High': 0.56}

$$ISC = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$$

Cost to system performance - Systemic Impact (SI), Total Recovery Effort (TRE), Recovery Dependent Resilience (RDR) [Biringer et al, 2013]

$$SI(s_n) = \sum_{i=1}^{3} \left[\int_0^{100} ACE_i^2(t, s_n)dt - \int_0^{100} ACE_i^2(t, s_1)dt \right]$$

$$TRE(s_n) = \sum_{i=1}^{3} \left[\int_0^{100} u_i^2(t, s_n)dt - \int_0^{100} u_i^2(t, s_1)dt \right]$$

$$RDR(s_n) = SI(s_n) + TRE(s_n)$$

Scenarios

Scenario	Scenario Type	Definition	Simulation Modification
1	Baseline	No Degradation	None
2	Loss of Availability, Low	Denial of Service to Communications Network, Communication Latency / Time Delay	Time Delay = 8 Seconds
3	Loss of Availability, High	Denial of Service to Communications Network, Communication Latency / Time Delay	Time Delay = 24 Seconds
4	Loss of Integrity, Low	Jamming of Signals, Addition of zero-mean, Gaussian white noise	$P_n = 0.25$
5	Loss of Integrity, High	Jamming of signal, Addition of zero-mean, Gaussian white noise	$P_n = 0.75$
6	Loss of Confidentiality + Availability, Low	Loss of Generation capability, tripping of relays / disabling generators	CA 2 Loses 1 Generator
7	Loss of Confidentiality + Availability, High	Loss of Generation capability, tripping of relays / disabling generators	CA 2 Loses 2 Generators
8	Loss of Confidentiality + Integrity, Low	Measurement signals manipulated for secondary control loop (LFC)	Zero out ACE measurement in CA 2
9	Loss of Confidentiality + Integrity, High	Measurement signals manipulated for secondary control loop (LFC)	Flip sign of ACE measurement in CA 2

Scenario Results

A few points to look at:

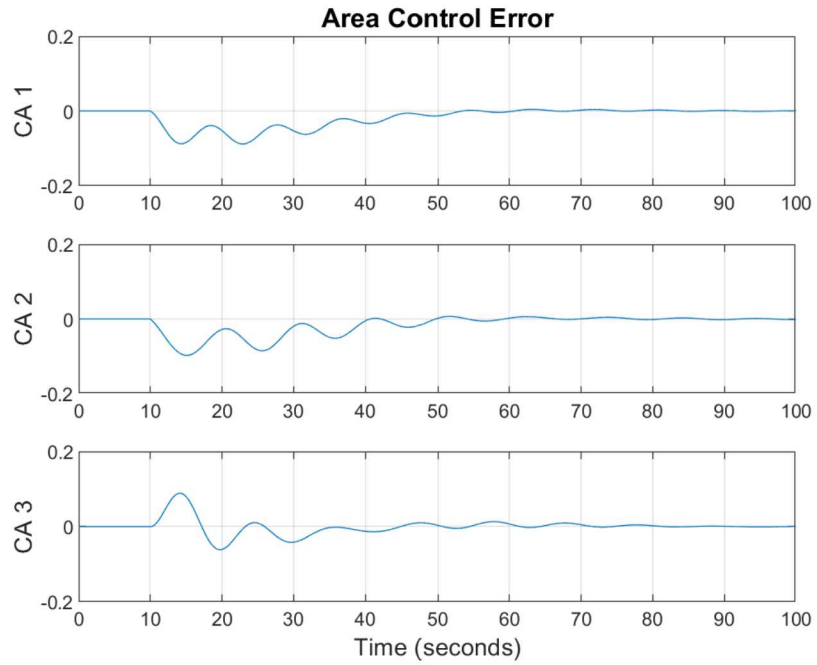
- RDR vs. ISC
- Scenario 7 vs. Scenario 9
  - Loss of generation vs. flipped signal
- Scenario 4 vs. Scenario 5
  - Noisy signals
- SI and TRE give insight on type of impact
  - Scenario 4 and Scenario 5

Scenarios	SI	TRE	RDR	ISC
1	0.000	0.000	0.000	0.00
2	0.096	0.102	0.198	0.22
3	0.617	0.673	1.290	0.56
4	0.003	0.100	0.103	0.22
5	0.011	0.297	0.308	0.56
6	0.281	1.489	1.770	0.3916
7	2.213	5.729	7.942	0.8064
8	2.103	1.573	3.677	0.3916
9	269.378	187.315	456.693	0.8064

Scenario 1: Baseline

Some cost from regulation of system under normal conditions

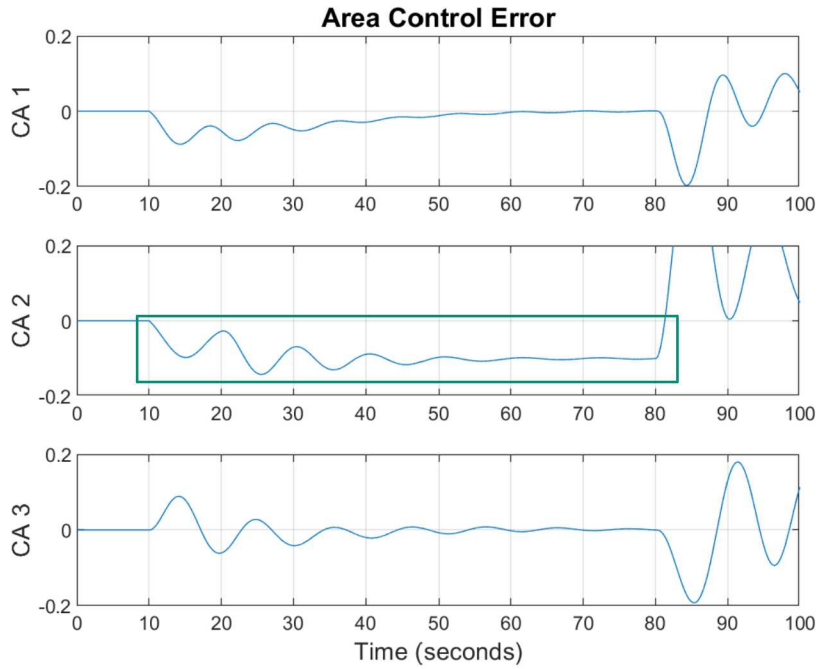
- Step load change at t = 10 seconds
- No degradation from a cyber attack



Scenario 7: Lose Generation, High

Control Area 2 loses generator 1 & 3

CA 2 unable to recover until the attack ends (Loss of Controllability)

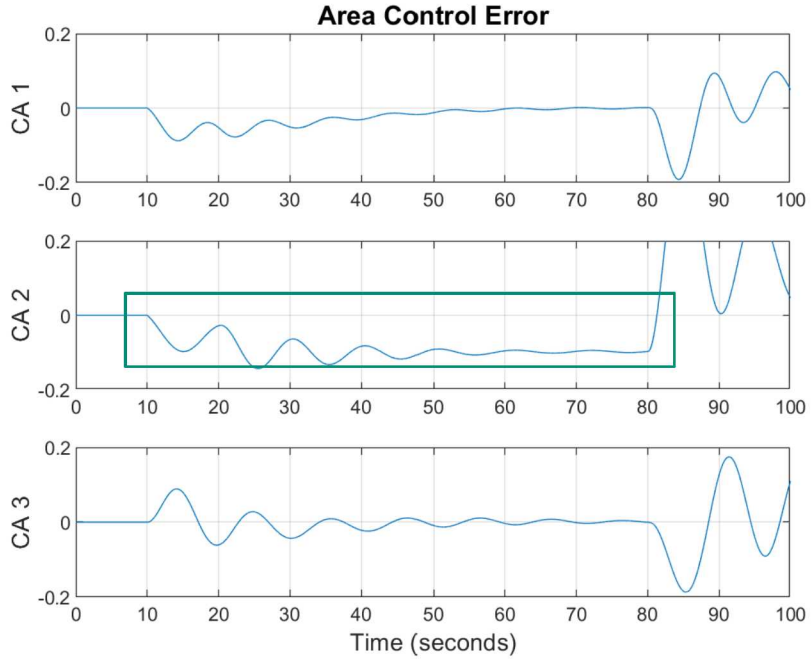


SI	TRE	RDR	ISC
2.213	5.729	7.942	0.8064

Scenario 8: Signal Manipulation, Low

Adversary has managed to zero out ACE signal to LFC

CA 2 is again unable to recover until end of attack (Loss of Observability)

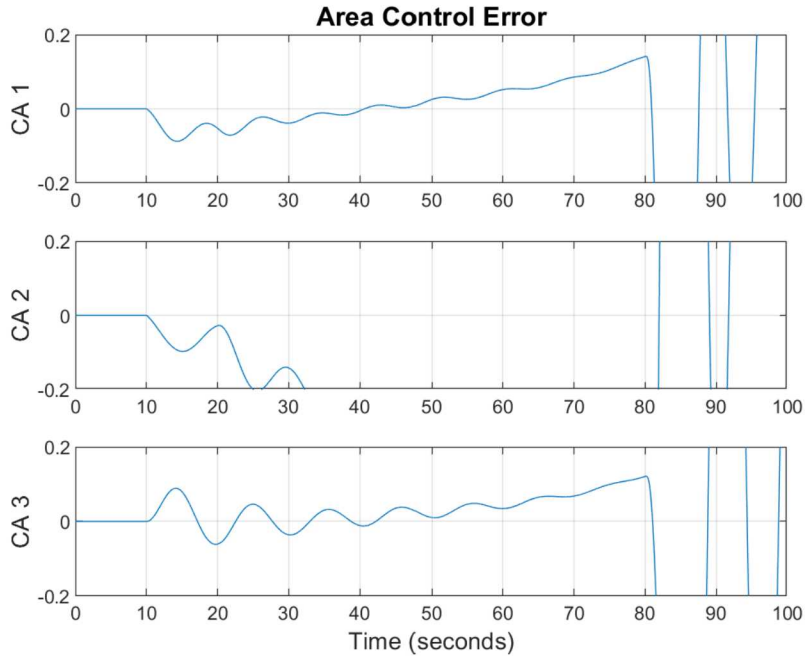


SI	TRE	RDR	ISC
2.103	1.573	3.677	0.3916

Scenario 9: Signal Manipulation, High

The measurements fed into the LFC for CA 2 have their sign flipped

CA 2 drives **away** from desired operating condition



SI	TRE	RDR	ISC
269.378	187.315	456.693	0.8064

Conclusion

In this work, we've shown an approach to quantifying cyber resilience in a controls system

- How to represent a cyber event within a set of dynamic equations
- How to measure impact to the control system performance
- Differences between measuring impact to security and resilience

Next steps

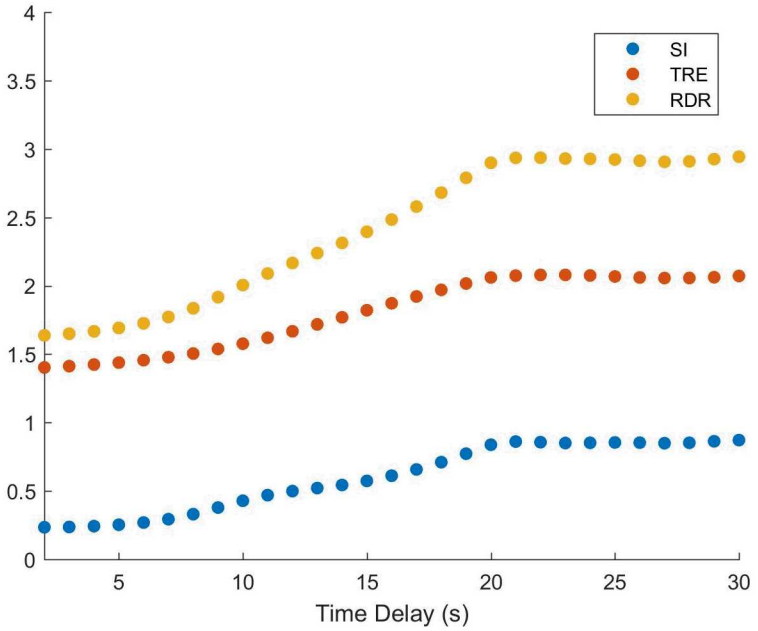
- Formally characterizing cyber event classes as discrete transitions to the state space (such as in Hybrid Systems)
- Demonstrate and apply to various control systems with real-world examples

Thank You!

Backup

Loss of Availability

Communication delays (such as from DDOS)

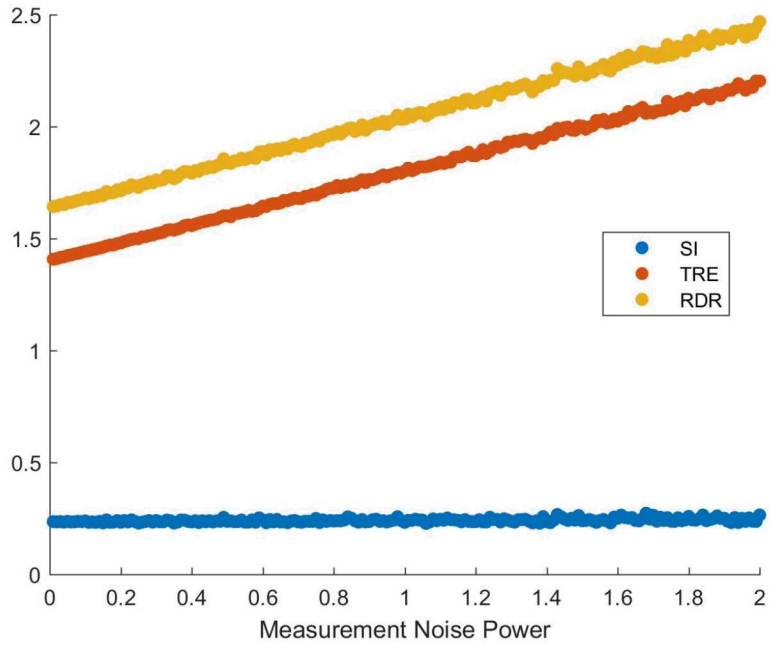


Notice nonlinear behavior

- After a certain point increases in latency start to affect the performance more and more (excessive phase lag)
- Even further, resilience costs from latency starts to plateau

Loss of Integrity

This case injects zero mean, white noise (Gaussian) into the measured signals used by the LFC, with varying levels of signal power

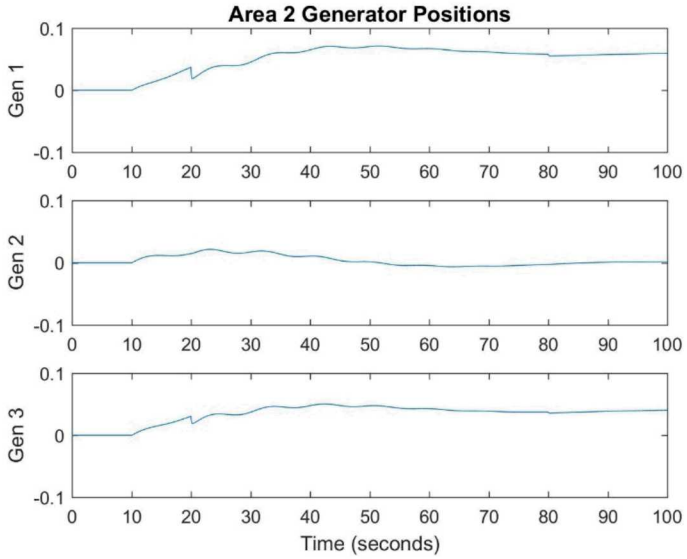


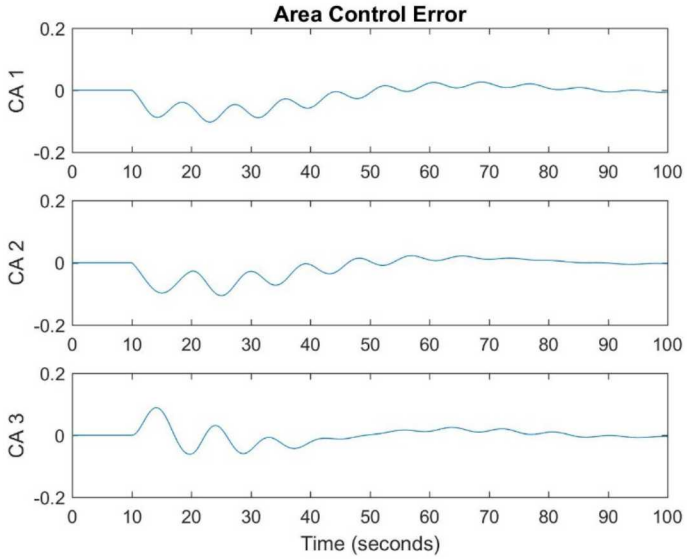
While SI increases very, very slowly, the controller must work a lot harder to accomplish its goal (TRE much larger than SI)

- Controller is *robust* to this attack, but this comes at a cost of greatly increased control effort

Scenario 2: Latency, Low

Time delay = 8 seconds



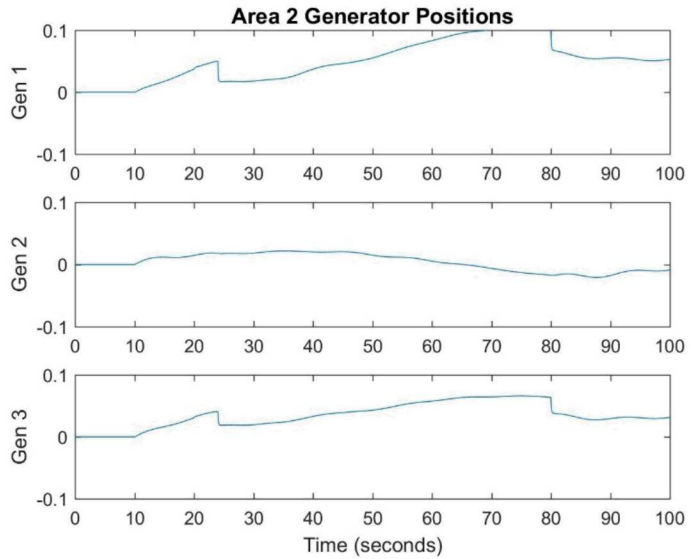


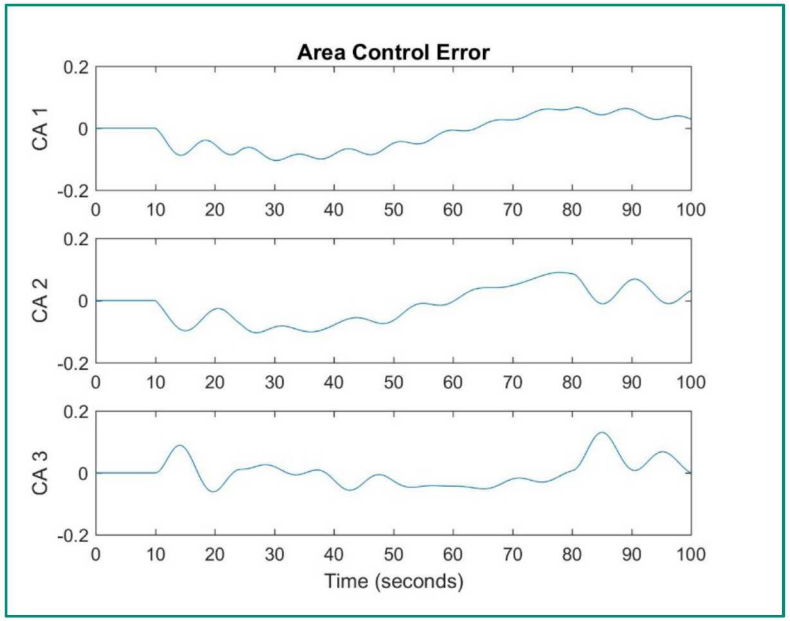
SI	TRE	RDR	ISC
0.096	0.102	0.198	0.22

Scenario 3: Latency, high

Time delay = 24 seconds

Notice the added low frequency oscillation in the output (representative of phase lag)



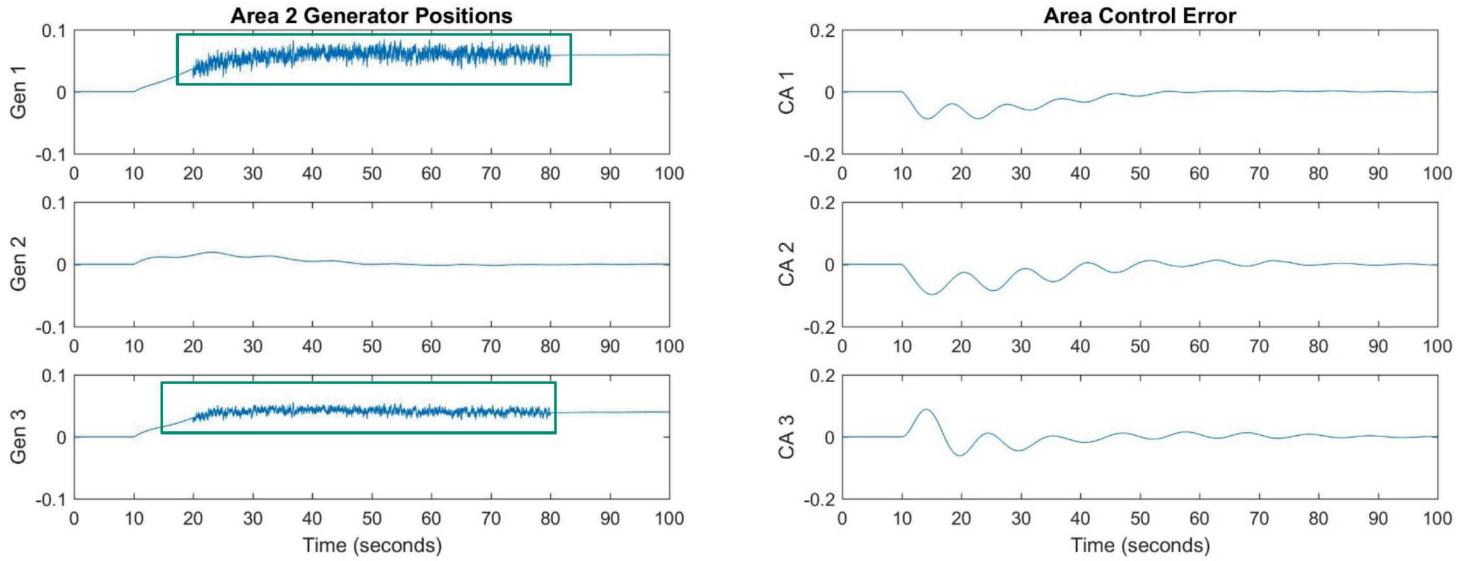


SI	TRE	RDR	ISC
0.617	0.673	1.290	0.56

Scenario 4: Noise, low

This case uses measurement noise power = 0.25

Note that the noise does not appear directly in the area control error. This is because this is *measurement noise*. It does however greatly affect the control output.

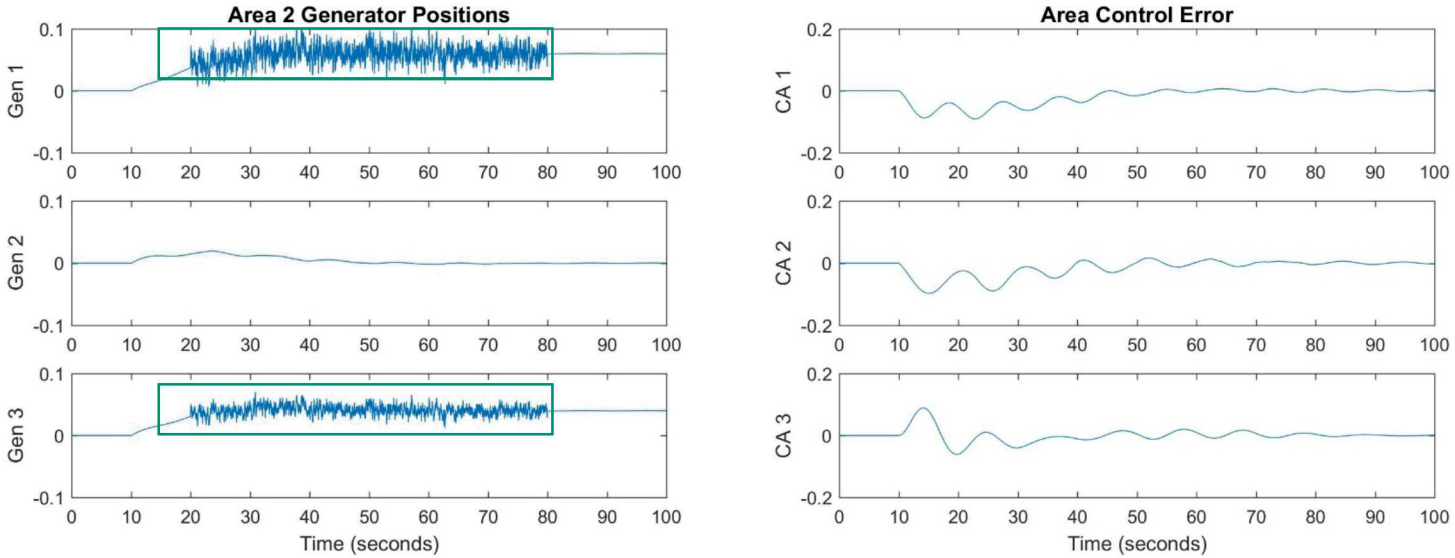


SI	TRE	RDR	ISC
0.003	0.100	0.103	0.22

Scenario 5: Noise, High

This case uses measurement noise power = 0.75

Larger power for "jamming" signal results in more variation to control output and more control effort, but the system performance is still mostly unaffected

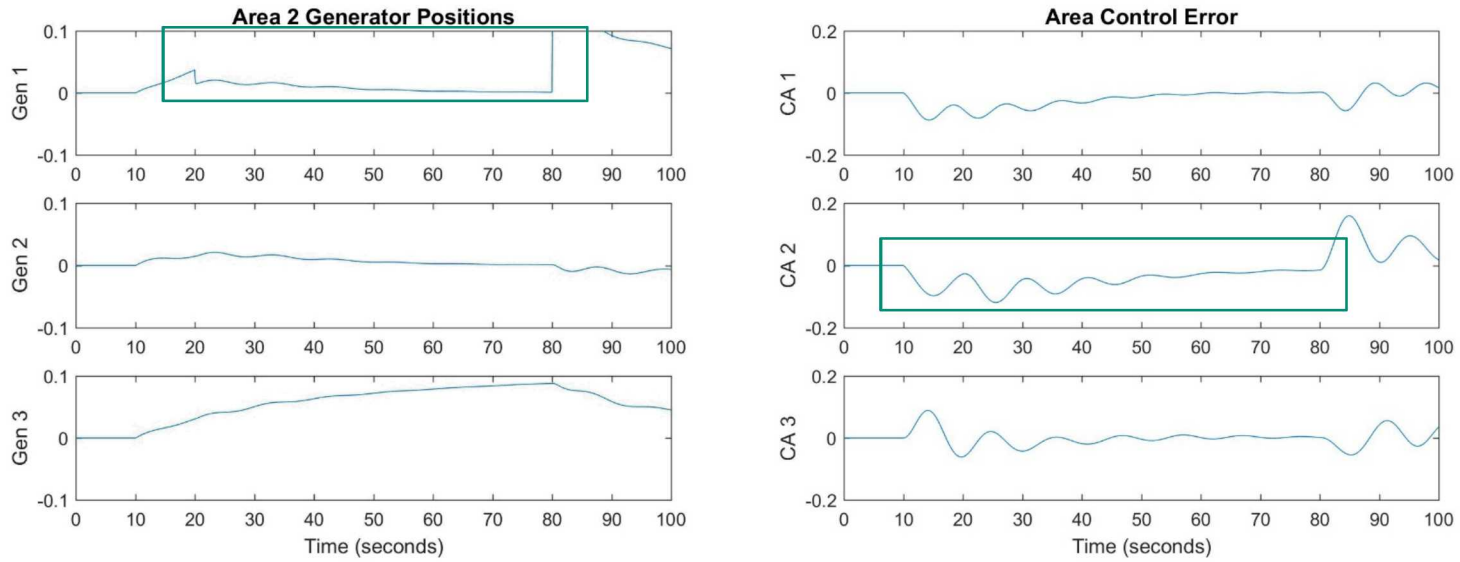


SI	TRE	RDR	ISC
0.011	0.297	0.308	0.56

Scenario 6: Lose Generation, Low

Control Area 2 loses generator 1

Notice Generator 3 struggling to cover load. Also, both CA 1 and CA 3 are supplying power to CA 2



SI	TRE	RDR	ISC
0.281	1.489	1.770	0.3916

Observability and Controllability

Observability and Controllability are control concepts regarding an ability to observe and control the system states.

Loss of sensors and actuators can thus be shown to have an effect on either of the two

- We see rank(ctrb(A,B)) and rank(obsv(A,C)) affected in scenarios 6-9

With our approach here, we are able to measure how Observability and Controllability change due to a cyber attack

- And can leverage other control theoretic constructs and tools as needed

Disabling generation (Scenarios 6 and 7)

For Control Area 2, loss of generation has following results:

Ex. CA 2:

- Rank of ctrb == 9

Drop Generator 1 (scenario 6)

- Rank of ctrb == 9

Drop Generator 1 & 3 (scenario 7):

- Rank of ctrb == 0
- Loses all ability within CA 3 to control system
- Note: Tertiary Control has Generator 2 set as backup, not used in base case. If operator enables Generator 2 then rank of ctrb would return to 9

This shows that even with some generation, we can somewhat control frequency (but perhaps not adequately, see ACE / other measures)

Signal Manipulation (Scenarios 8 and 9)

When measuring system states, we say a system is fully *observable* iff we can observe all the state variables

Ex. CA 2:

- Rank of obsv == 9

Scenario 8 (Zero out ACE measurement signal):

- Rank of obsv == 8
- Zeroing out ACE measurement modifies C, resulting in a system that is no longer fully *observable*

Scenario 9 (Flip ACE measurement signal):

- Rank of obsv == 9
- Flipping sign still modifies C but the matrix is still full rank. It does not see the change to measurement logic