Losing Faith in the Modern World

A BELIEF THAT ICS IS AT OR BEYOND LIMITS OF DEFENSIBILITY

ENTIRELY TOO MUCH FAITH IN ABILITY TO DEFEND COMPLEX SYSTEMS

THE THING THAT WILL NOT FAIL YOU IS PHYSICS

Tim Roxey

1 November 2019

Losing Faith (for good reason)

Initial Assumptions

- Societies dependence on Automata is at or beyond limits of defensibility
- Too much faith in ability to defend complex systems
  - Info sharing, Best Practice, Standards
  - All necessary yet inadequate for defense
- Technology is soooooo complex (high-levels of abstraction)

Initial Condition of Grid protections

- Holes in coverage (next slide)
  - AURORA's asynchronous attack example
  - Typically, protection implemented in complex, computer-based architecture

Possible New Class of ICS Protection

- Goes back to simple representation of physics
- Re-implements in logic yet differently

The Two Paths We Travel

Our current path: Incrementalism

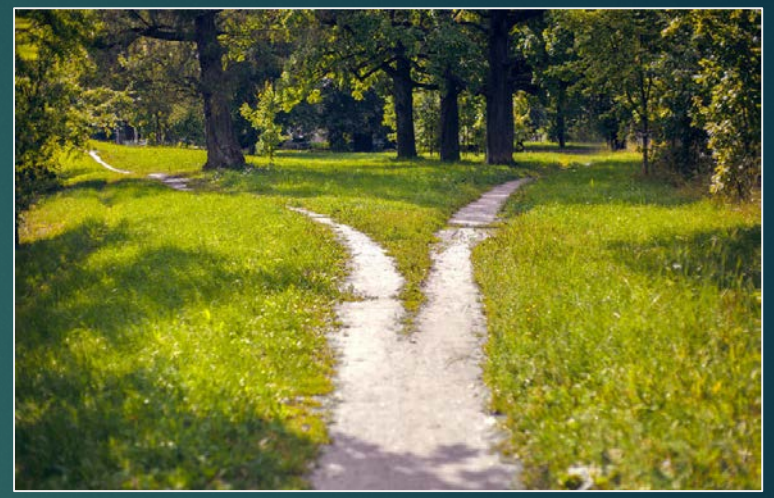
- Simple expansion of functions yield new markets. (Driver)
- Building on existing code base far simpler that generating entirely new code base (although not the safest approach)
- Legacy components almost impossible to QA
- Every implementation is susceptible to computer intrusion!

A needed path: Transformational

- Back to basic physics and re-implemented without a computer OS and Comms
- New manner of achieving a solution
- Quantum? (gratuitous Buzzword)

Both approaches based on the same Physics for the ultimate endpoints

- But how a given function is achieved is quite different



Some new terms

- Crumple zones
- Limits of testability, Software Quality Assurance and its limits
- Controlling equations, re-baselining

Prospective Paths to Hope

1) Some words for consideration:

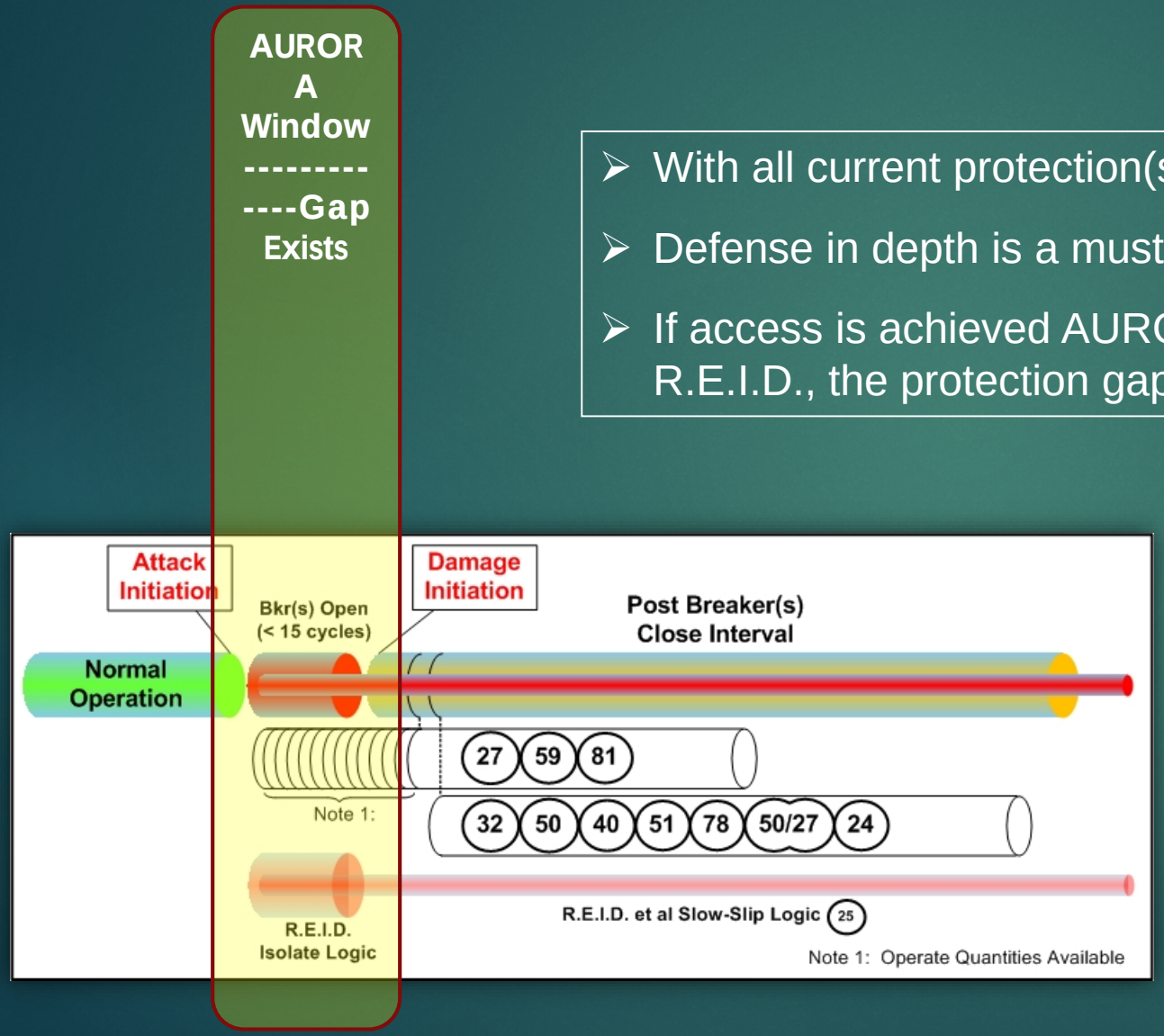
*"Those systems, structures, or components deemed necessary to protect the " health and safety" of the public (for nuclear) or deemed highly critical via appropriate regulations for non-nuclear CIKR **SHALL** be protected by systems that can be shown effective via Deterministic Methods." **

2) INL's new methodology for countering cyber sabotage:

Consequence-Driven Cyber-Informed Engineering (CCE)

* This means formal methods for SQA and other appropriate testing for physical systems such as structures or components.

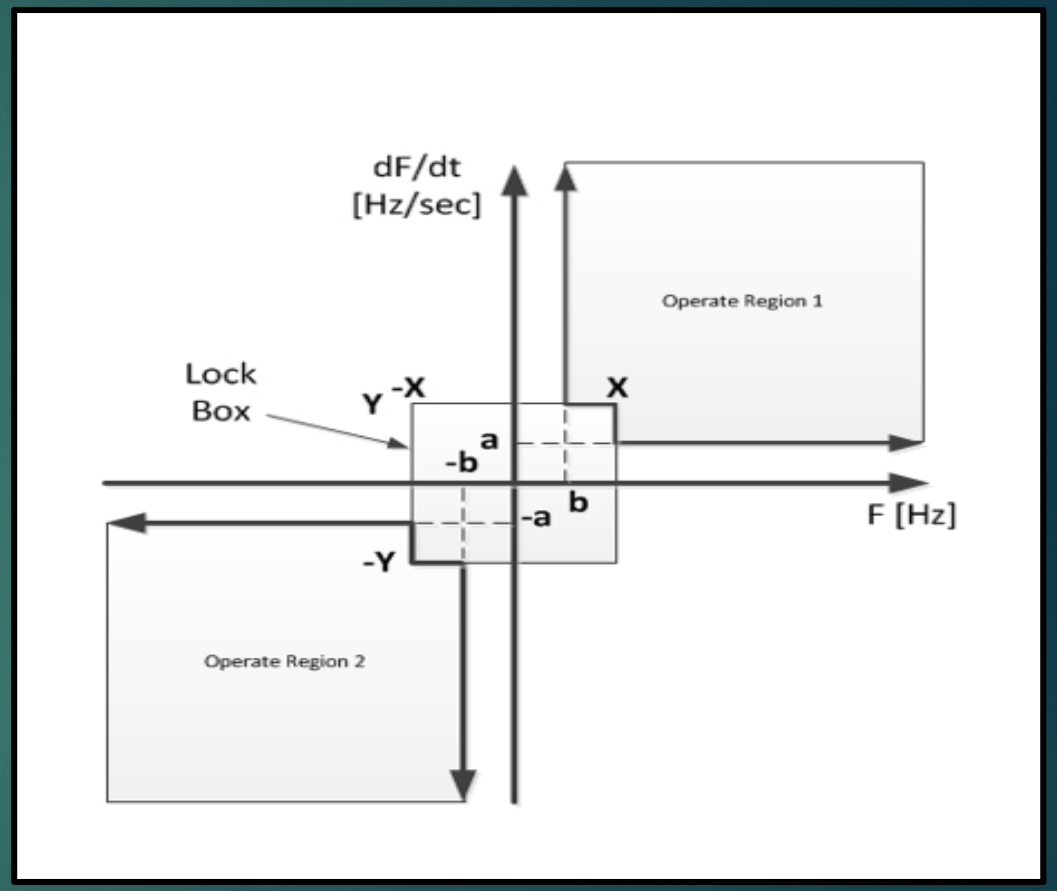
The Pesky Asynch Gap



- With all current protection(s) in place AURORA cannot be prevented
- Defense in depth is a must requiring good cyber and physical security
- If access is achieved AURORA may still happen because without a R.E.I.D., the protection gap exists

Attack Example – An Asynchronous Exploit

- Aurora attacks impact motors and generators
- Attack involves momentarily disconnecting a motor or generator from the grid
- The motor or generator quickly falls out-of-synch with the grid
- When motor or generator is maliciously reconnected catastrophic damage occurs
- Reclosing in Region 1 or Region 2 is always dangerous



The Device

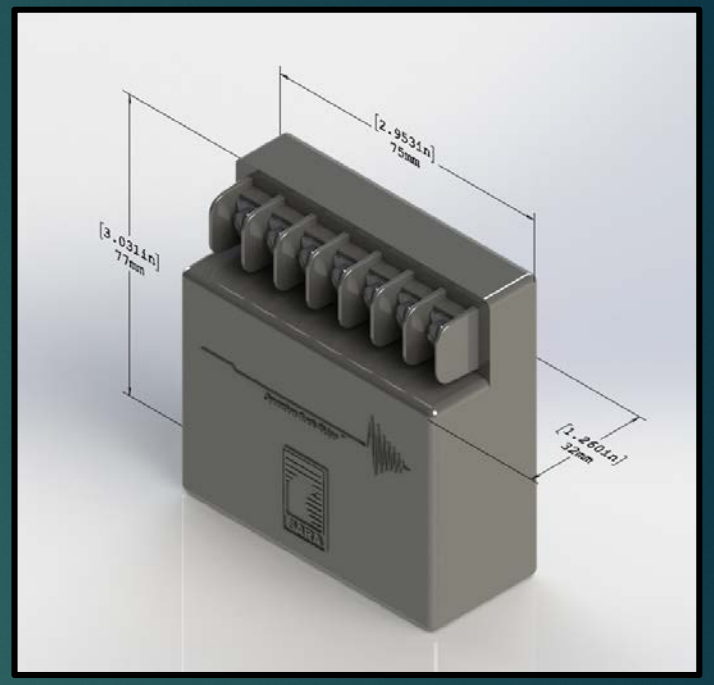
- No computer program
- No operating system
- No network layer
- No application Stack
- No ability for adversary to "discover" its presence or absence in a larger ICS system
- Just pure circuits. . .

STATUS

- Field testing is complete at major US electric utility; widescale deployment about to begin

1) 67 Volt Power Tap
2) 115 Volt Power Tap
3) Neutral

Tabs



4) Output Circuit in
5) Output Circuit out
6) Alarm out
7) Alarm out

Thank You

- scubanuke@gmail.com