Timing Security Assessment and Solutions

Glen Chason, EPRI

October 26, 2016

Agenda

Overview

Status

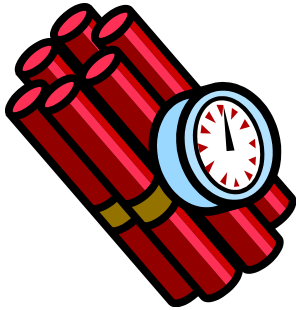
Timeline

Next Steps

Emerging Technologies Create New Promise and Peril

More Utility Applications Rely on Precision Timing

- Substation Automation Algorithms
- Fault Location
- UAVs
- Synchrophasors
- Telecommunications networks

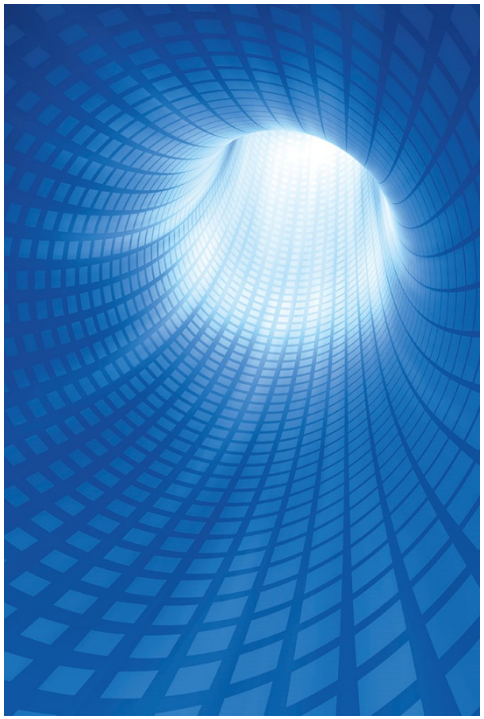


Precision Timing Vulnerabilities

- Spoofing
- Celestial Jitter
- Denial of Service
- Geomagnetic interference
- Timing Drift

Questions Utilities Should Ask

- **Vulnerability**: Is equipment deployed - or being considered for deployment - to provide timing synchronization vulnerable to attacks that could impact synchronized operations?
- **Criticality**: For equipment vulnerabilities identified; to what extent can those vulnerabilities be exploited to negatively impact power delivery?
- **Solutions**: Can mitigations be found to reduce the potential risks associated with the exploitation of vulnerabilities in power systems that rely on highly synchronized operations? If mitigations can be found, what is required to implement those mitigations?

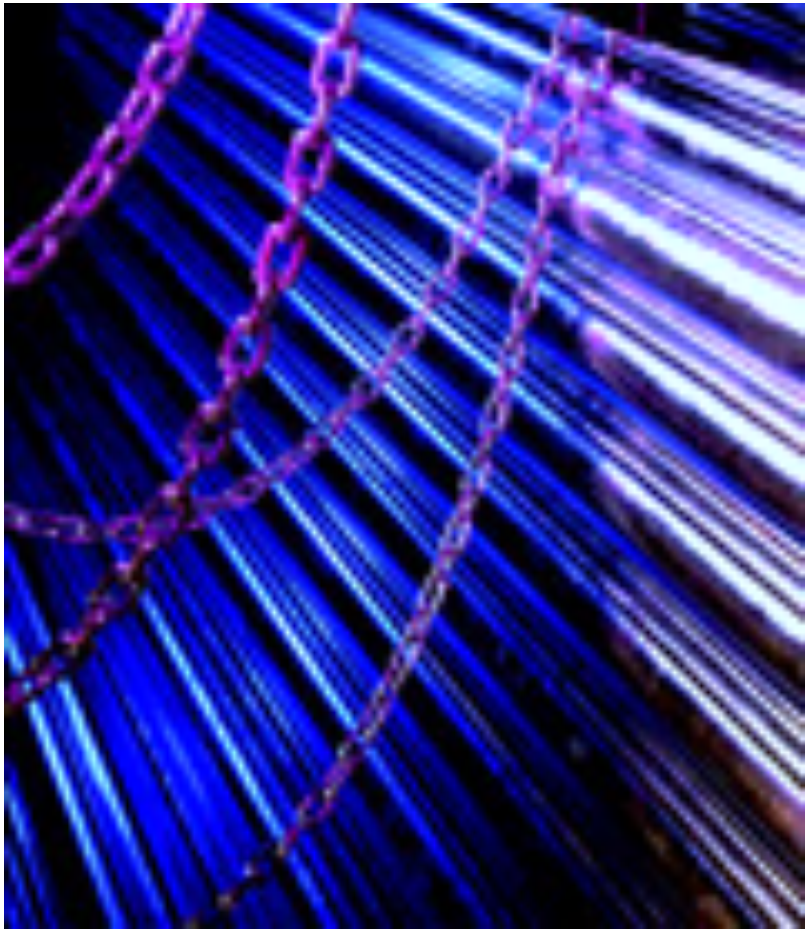


How Vulnerable Are We?

- Determine the extent to which equipment deployed in electric sector reliant on precision timing may be vulnerable to malicious intrusion and alteration.
- Identification of the vulnerabilities that exist, their pervasiveness in deployed equipment, and techniques for identifying the vulnerabilities will be documented.
- The results of this research on vulnerabilities include guidance on testing for the vulnerabilities in existing equipment.

How Serious are these Vulnerabilities?

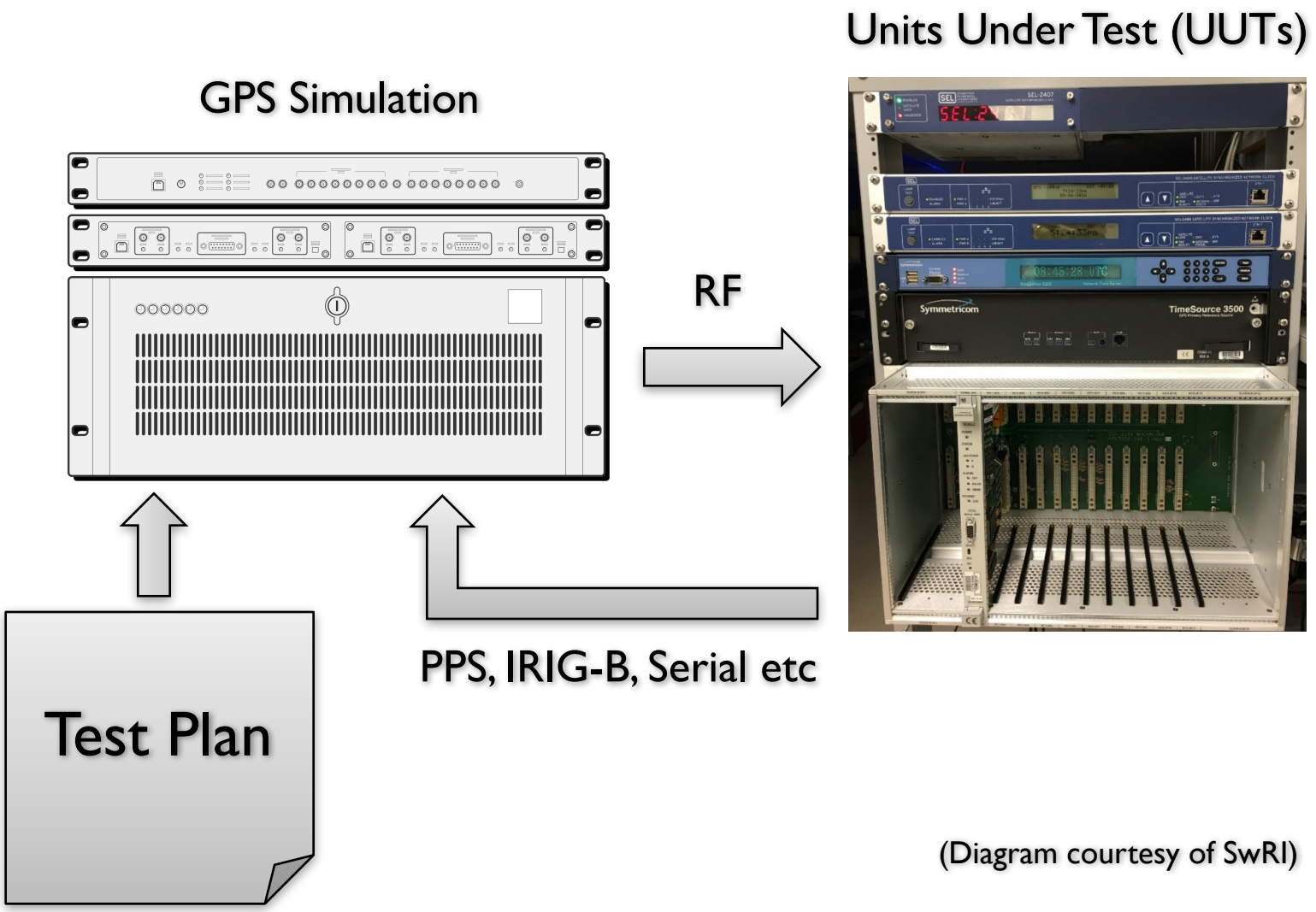
- Analyze the potential impacts to operations if identified vulnerabilities are exploited.
- Potential impacts to power delivery and power restoration.
- Results of this project will include guidance to assist utilities in prioritizing and performing similar analysis on their respective systems



How Do We Address Prioritized Vulnerabilities?

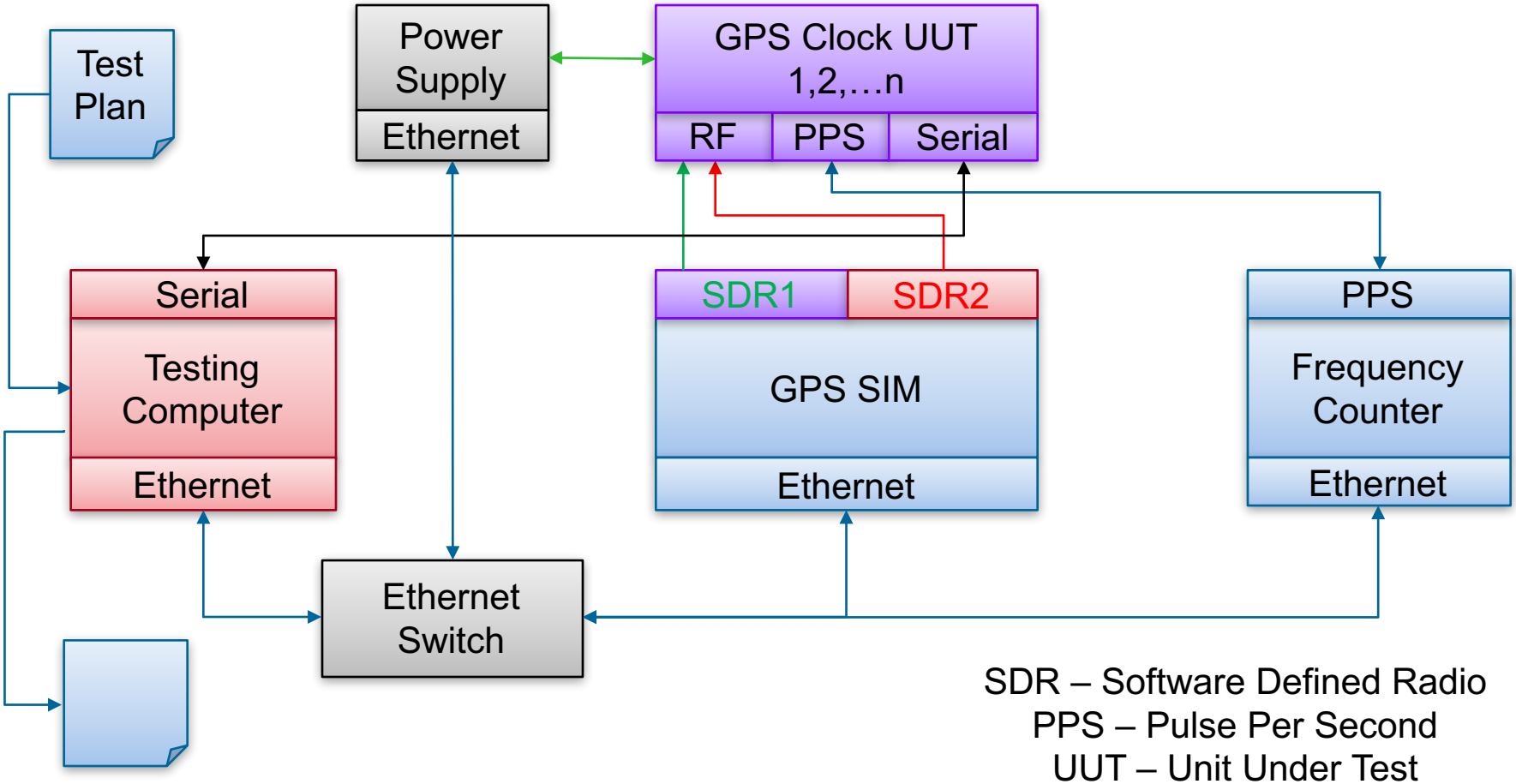
- Identify and test potential mitigations for the vulnerabilities identified.
- Test results and mechanisms for evaluating the test results will be provided to the project members.
- Guidance will assist project members to plan and deploy needed mitigations within their operations.
- Results will also include guidance to assist utilities to reduce their exposure to these vulnerabilities through their procurement processes.

Initial Testbed



(Diagram courtesy of SwRI)

High-Level Test Diagram



SDR – Software Defined Radio
PPS – Pulse Per Second
UUT – Unit Under Test
RF – Radio Frequency

(Diagram courtesy of SwRI)

Test Case Format

- **Test Case:**
  - Test Case Description
- **Vector:**
  - Access Method
- **Findings:**
  - Description from test procedure of why it is a pass or fail
- **Recommendations:**
  - This is only included if we have a failed test procedure

(Format courtesy of SwRI)

TS-3500.2 – GPS Time Spoofing

- **GPS Jamming**
  - Jam receiver and see effects on PPS output
  - TS-3500.1 (Time Source)
  - SS-S200.1 (Sync Server)
  - SSU-2000.1 (System Shelf)
- **GPS Time Spoofing:**
  - Spoof the GPS signal at a rate undetectable to the GPS receiver so that the time information is corrupted
  - TS-3500.2
  - SS-S200.2
  - SSU-2000.2

Project Timeline

- Month 1 Kickoff & identification of Level 2 systems testing
- Month 2 Vulnerability testing initiated
- Month 6 System impact testing initiated
- Month 8 Vulnerability testing completed
- Month 10 Mitigation testing initiated
- Month 10 Vulnerability testing report
- Month 12 Risk assessment and testing completed
- Month 14 Risk assessment and testing report
- Month 16 Mitigation testing completed
- Month 18 Mitigation testing report

Timing Security Assessment and Solutions

Project Membership

- Level 1
- Level 2

Project Lead

- Glen Chason gchason@epri.com, (865) 218-8161

Security is essential to ensure precision timing for utility applications

Technical Advisors

- Christine Hertzog chertzog@epri.com, (650) 387-8831

Discussion