U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Timing Intrusion Management Ensuring Resiliency (TIMER)

Texas A&M Engineering Experiment Station

Mladen Kezunovic

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

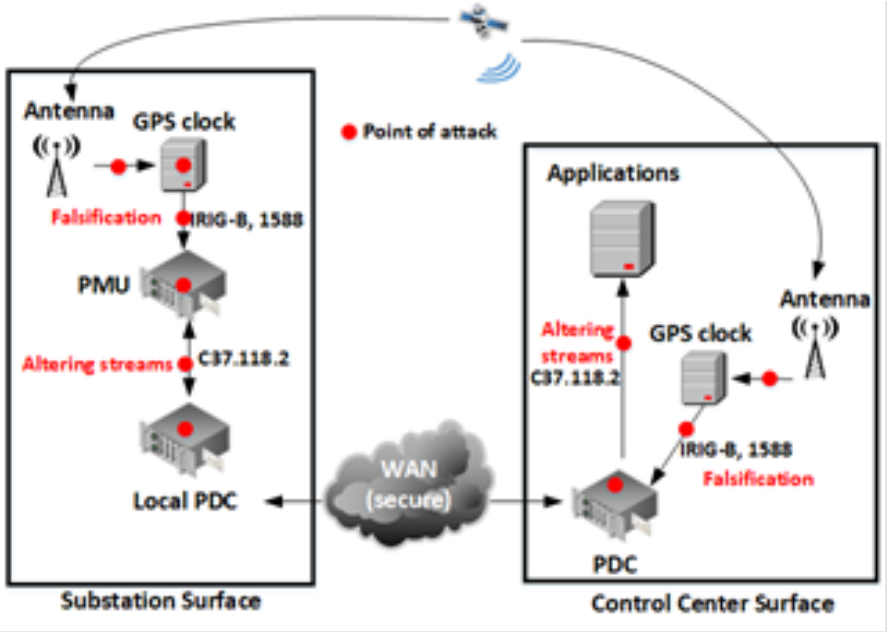
Summary: Timing Intrusion Management Ensuring Resiliency (TIMER)

Objective

- Make end-to-end Synchrophasor systems and applications more resilient under timing attacks
- Goal: to develop detection methods & tools to manage timing signal intrusions.

Schedule

- 10/1/2016-9/30/2019
- Key deliverables: 1) Software & hardware solutions to detect timing intrusions; 2) Advanced testbed & field evaluations; 3) Risk-based evaluation methodology & metrics;
- Transition to the energy sector: Field demonstration at IPC; Promotional meetings with end-users.



Total Value of Award:	**$4,429,451**
Funds Expended to Date:	**38.93%**
Performer:	**Texas A&M Engineering Experiment Station**
Partners:	**PNNL, Idaho Power, EPG**

Focus: Tools and methodologies

Tools (references)

- Uncompromised GPS clock
- Accurate “Gold” PMU
- Flexible portable Field test set
- Communication tester (1588 and 37.118.2 packets)
- Selected application (FL)

Methodologies

- System calibration
- Abnormality detection
- In-service troubleshooting
- Nested testing
- Type tests
- Application tests
- Assessment of application impact

Advancing the SOA: Uncompromised GPS Clock

- SOA for GNSS Timing
  - High performance GNSS receiver & clocks
  - No known timing integrity checker solution for substation/control center
- Our approach
  - Cross checking of different timing data – we have only one time reference
  - Monitor GNSS signal behavior at different layers
  - Off-the-shelf component Implementation

- Benefits over the SOA
  - Plenty signal data in commercial receivers suitable for behavior modeling
  - Hold-over clocks at user's choice
  - Timing checker circuit -- first of its kind
  - Networking capable for wide area defense
- Benefits to the end user
  - Computing resources much cheaper than specialized RF equipment
  - Practical technology easily integrated with existing equipment
- Advance the cybersecurity of energy delivery systems
  - Detect critical timing anomaly which cannot be done by regular cybersecurity tools

Challenges to Success

Challenge 1: Sites see different satellites

- Environment adaption and Two phase operation
  - o Profiling of satellites, Pattern learning, followed by monitoring

Challenge 2: Inherent noise in GNSS signals

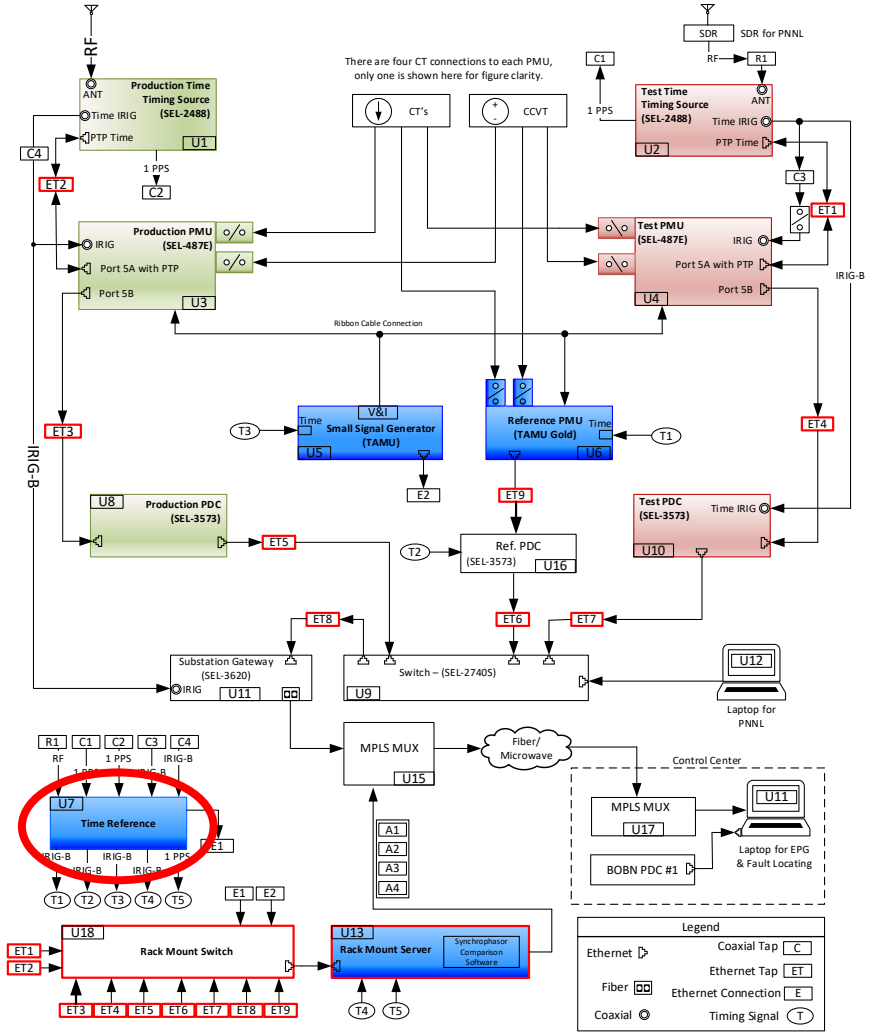
- Qualification of satellite signals during different times
- Estimate the acceptable behavior range
- Experiments showed highly consistent patterns

Challenge *3:* High cost of high performance RF equipment

- A defense-in-depth strategy to use algorithm based, multiple behavior criteria to detect anomaly

Progress to Date

- **A custom made prototype system**
  - Ublox receiver
  - GNSS SDR
  - GPSDO holder-over clock
  - FPGA based 4-channels of IRIG-B, 1pps integrity checker,
  - Multiple hold-over IRIG-B and 1pps outputs
- **Monitoring software system**
  - Management controller
  - GNSS signal behavior statistic and update
    - Database
    - Graphic user interface



Advancing the (SOA): Waveform generation and accurate measurement

- Current “state of the art”:
  - Field test set do not posses automate type and application test tailored to TI impact evaluation on applications
  - Highly accurate PMU with adaptive algorithm selection is not available
- The feasibility of our approach
  - We developed prototype to test feasibility
- Why our approach is better than the SOA
  - It is tailored to the specific TI detection and impact evaluation methodology
- How the end user of our approach will benefit
  - Synchrophasor system resiliency to TI attacks will be enhanced
- How our approach will advance the cybersecurity of energy delivery systems
  - By making sure operators are made aware of the attacks timely

Challenges to Success

Challenge 1: Feasibility

- Develop porotypes and demonstrate the use
- Instrument end-to-end systems with porotypes
- Steps taken to overcome challenge of implementing the methodology

Challenge 2: Effectiveness

- Set the metrics to evaluate performance
- Engage a Red team to preform independent evaluation

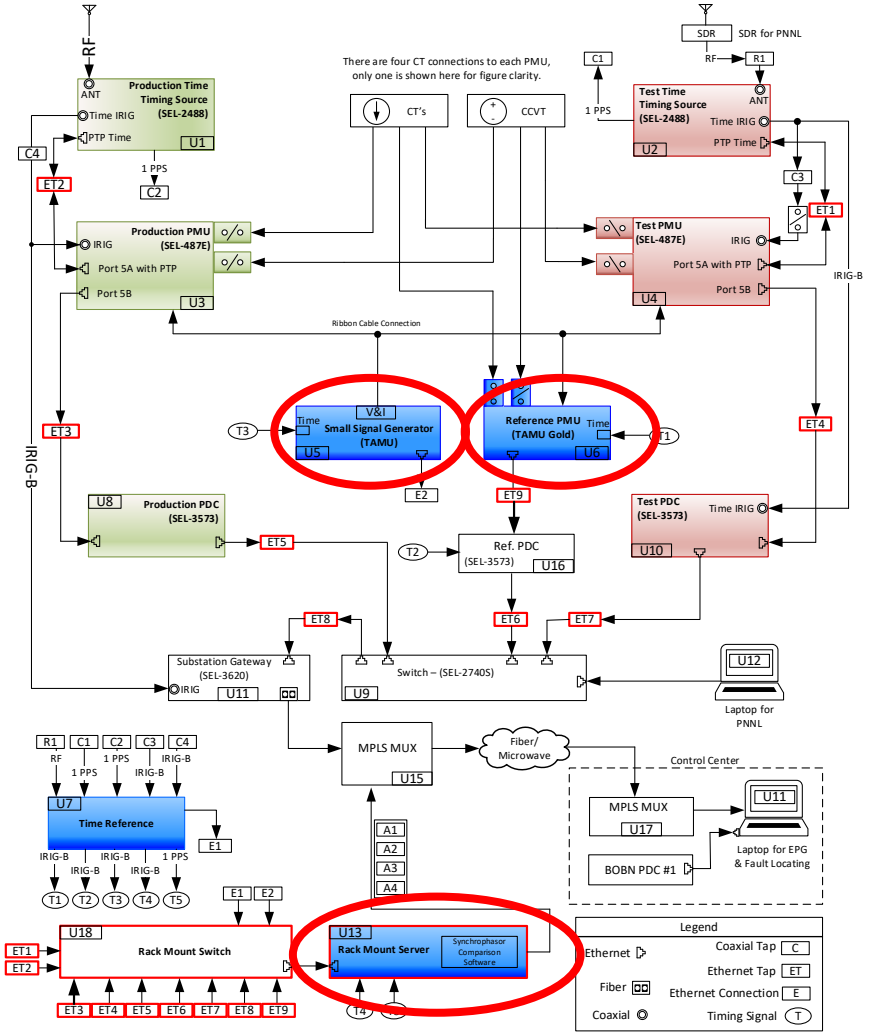
Challenge 3: Acceptance

- Allow long term demonstrations in test bed and field
- Create a community of interested users

Progress to Date

Major Accomplishments

- The tools are conceived, designed and implemented
- The methodology for the use of tools is well defined and partially tested
- The designs for testbed and field installation are accomplished
- Initial implementation of the test bed production system evaluation is under way
- Use cases for test bed and field demonstration and evaluation are already specified



Advancing the SOA: Communication Tester

- **SOA for Network Integrity**
  - IEEE 1588 and C37.118.2 packets
  - No known modeling or integrity check for malformed packets, attacks on IEEE 1588 Time Distribution Protocol, or attacks on C37.118.2 Synchrophasor protocol.
- **Our approach**
  - Alert on detection of malformed packets (IEE 1588 and C37.118.2)
  - Monitor and model normal operation of IEEE 1588 Time Distribution Protocol and C37.118.2 Synchrophasor protocol and alert on deviation from the modeled norm.
  - Use of reference (gold) PMU and PDC to establish norm.
- **Benefits over the SOA**
  - Alerts on possible communication path timing attack which is not currently done.
- **Benefits to the end user**
  - Implemented with minimal hardware infrastructure (TAPs, switch, and server)
- **Advance the cybersecurity of energy delivery systems**
  - Detect possible timing intrusion attacks which is not currently implemented .

Challenges to Success

Challenge 1: Determine normal deviations in packets

- Monitor test network and determine statistical variations over time.

Challenge 2: Lost packets / Missing data

- Use model to fill in gaps between lost data packets.
- Determine if reference PMU/PDC agree with received traffic and update variations accordingly.

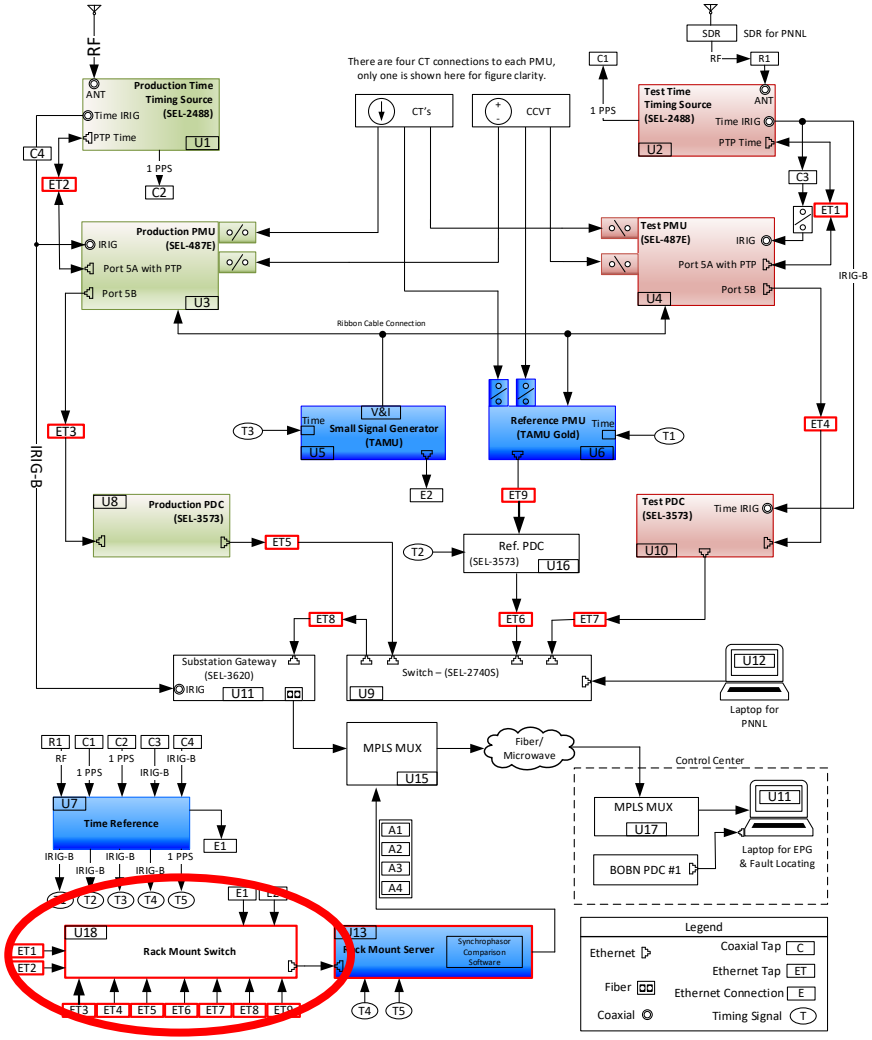
Challenge 3: Alarm Message Integration

- Working with subcontractor to verify message format and compatibility with their existing framework to integrate into their software model.

Progress to Date

Major Accomplishments

- Network architecture finalized, including ETAPs, server, IRIG-B receiver, and network switches.
- TAPs to collect IEEE 1588 (Time-Distribution Protocol) and C37.118 (Synchrophasor Protocol) traffic integrated into test system.
- Server to store packets and examine for intrusions installed.
- Script to filter aggerated TAP traffic and store in MySQL database completed.
- Test traffic data is now being collected on TAMU test system.
- Intrusion detection algorithm is now being developed.
- Alarm aggregation message and implementation methodology determined.



Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- What category is the targeted end user for the technology or knowledge? (e.g., Asset Owner, Vendor, OEM)

  - The targeted end-users are asset owners and vendors

- What are your plans to gain industry acceptance?
  - o Demonstrate the concept in production type testbed at TEES
  - o Evaluate the concept in field environment at IPC
  - o Organize visits of interested parties to the testbed and/or field installation
  - o Meet with prospective end-users and vendors in discussion sessions about the needs for timing intrusion detection, and how our tools and methodologies may meet the needs
  - o Prepare evaluation report with assessment metrics and use case test results

Next Steps for this Project

Approach for the next year or to the end of project

- Complete tool developments
- Integrate the tools in the production testbed
- Perform testbed evaluation to demonstrate the methodology and objectives
- Instrument the field environment with the solution to enable field evaluation
- Monitor in-service behavior to demonstrate effectiveness
- Develop a community of interested prospective users and engage them in tuning the specifications