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

Tempus Project

Schweitzer Engineering Laboratories, Inc.

Ken Fodero

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Tempus Project

Objective

- To develop a secure, modular, and customizable time synchronization platform that provides layers of protection from GPS spoofing attacks and vulnerabilities.

Schedule 2016 - 2019

- Publish industry benefits whitepaper - Done
- Final commercial release – June 2019
- Publish best practice guide – June 2019
- Industry testing and validation results – Nov 2019

Total Value of Award:	**$ 3,595,343.00**
Funds Expended to Date:	**% 30.59**
Performer:	**SEL**
Partners:	**Bonneville Power Administration, Dominion Energy℠**

Advancing the State of the Art (SOA)

- **Describe current "state of the art"**
  - Current satellite clocks trust GPS signals and have only minimal algorithms to prevent or detect signal manipulation

Advancing the State of the Art (SOA)

- **Describe why your approach is better than the SOA**
  - The end user will benefit from Tempus's ability to monitor multiple time sources and identify errant time sources
  - Produce time with high confidence in its integrity
- **Describe how the end user of your approach will benefit**
  - The end user will benefit from Tempus's ability to monitor multiple time sources and identify errant time sources.

Advancing the State of the Art (SOA)

- **Describe how your approach will advance the cybersecurity of energy delivery systems**
- Through monitoring multiple sources and detecting manipulation of individual sources the Tempus clock will have the resiliency to provide qualified time to downstream devices during external source interference or outage.

Challenges to Success

What time source do we trust – all sources are vulnerable

- A time source integrity algorithm determines confidence in each source based off source type and continuous monitoring. With several independent, high integrity sources in agreement, time can be confidently output to end devices.

Detecting signal attacks and vulnerabilities

- Characterize attack signatures and monitor against independent sources

Industry education

- Industry benefits whitepaper
- Application notes
- Best practice guide

Progress to Date

Major Accomplishments

- System specification complete
- GNSS front-end development
- GNSS receiver analysis and testing
- PTP component
- Completed industry benefits whitepaper
- Platform design underway

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

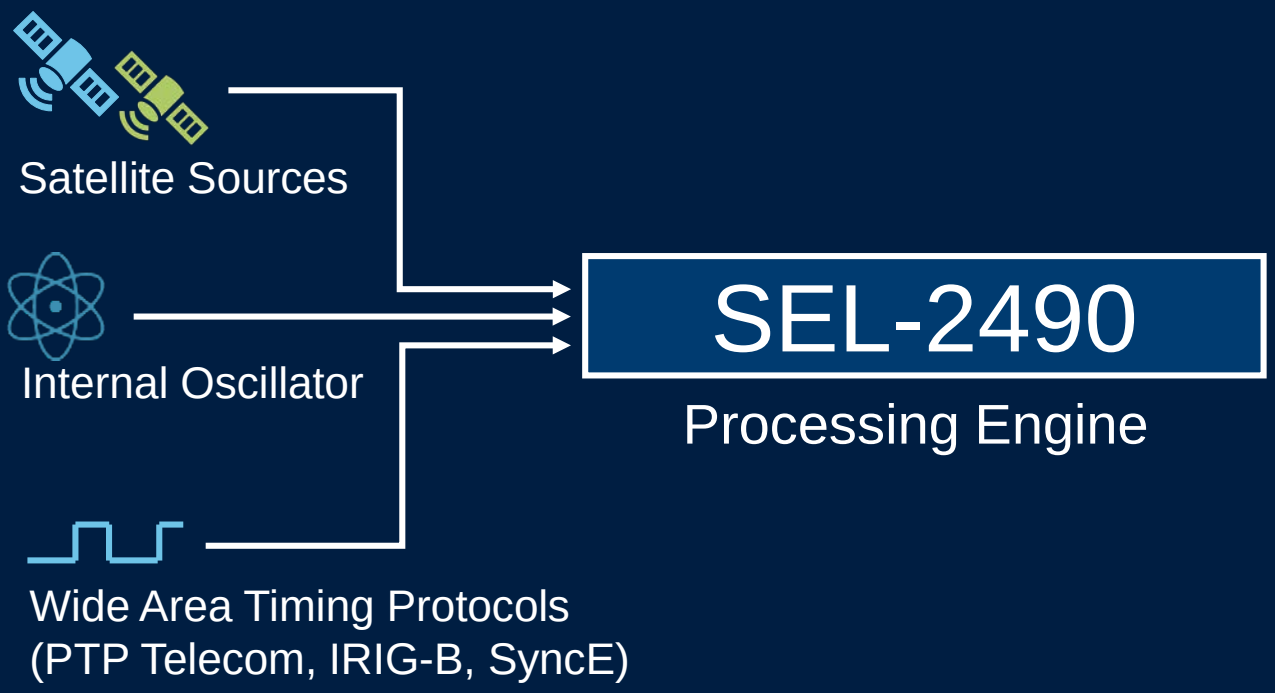
- What category is the targeted end user for the technology or knowledge? (e.g., Asset Owner, Vendor, OEM)
  - The targeted end user is Asset Owner
- What are your plans to gain industry acceptance?
  - Describe testing and demonstrations planned
  - Field testing by our partners; BPA and Dominion Energy
  - Best practice guide
  - Industry webinars and training

Next Steps for this Project

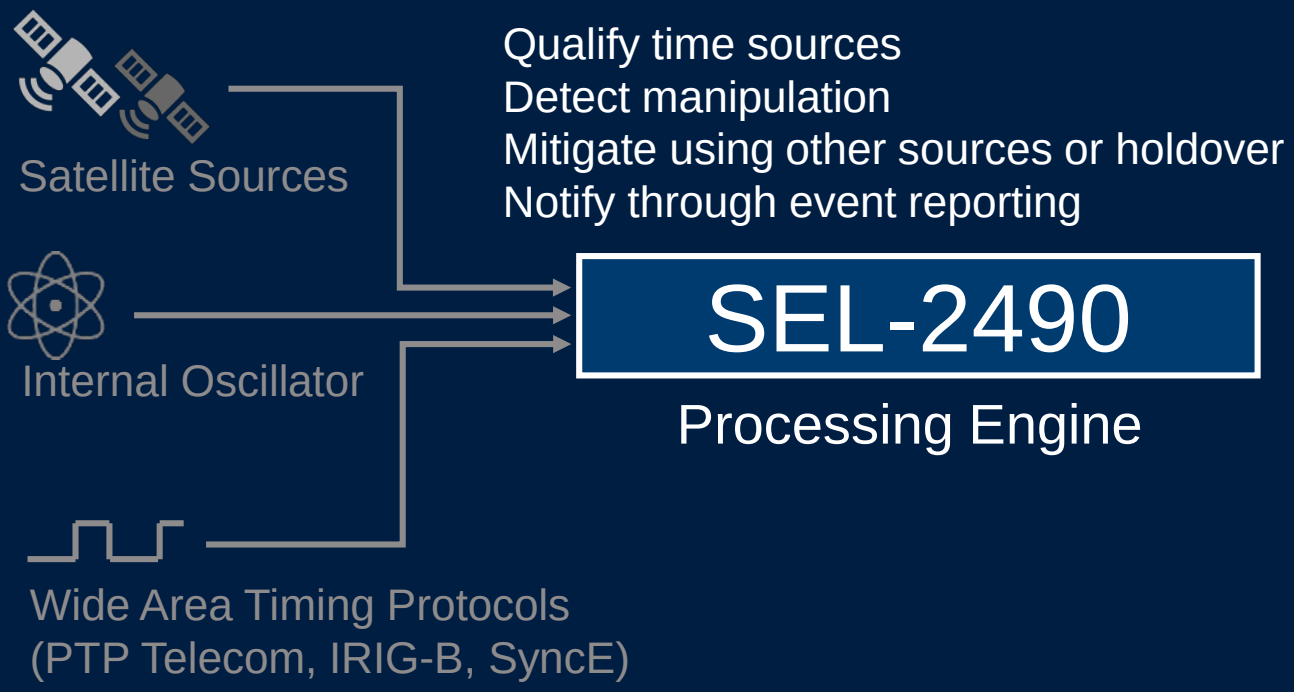
Approach for the next year or to the end of project

- Execute on development plan successfully
- Complete hardware development through type testing
- Develop remaining time sources and time systems
- Demonstrate prototype system against attack vectors

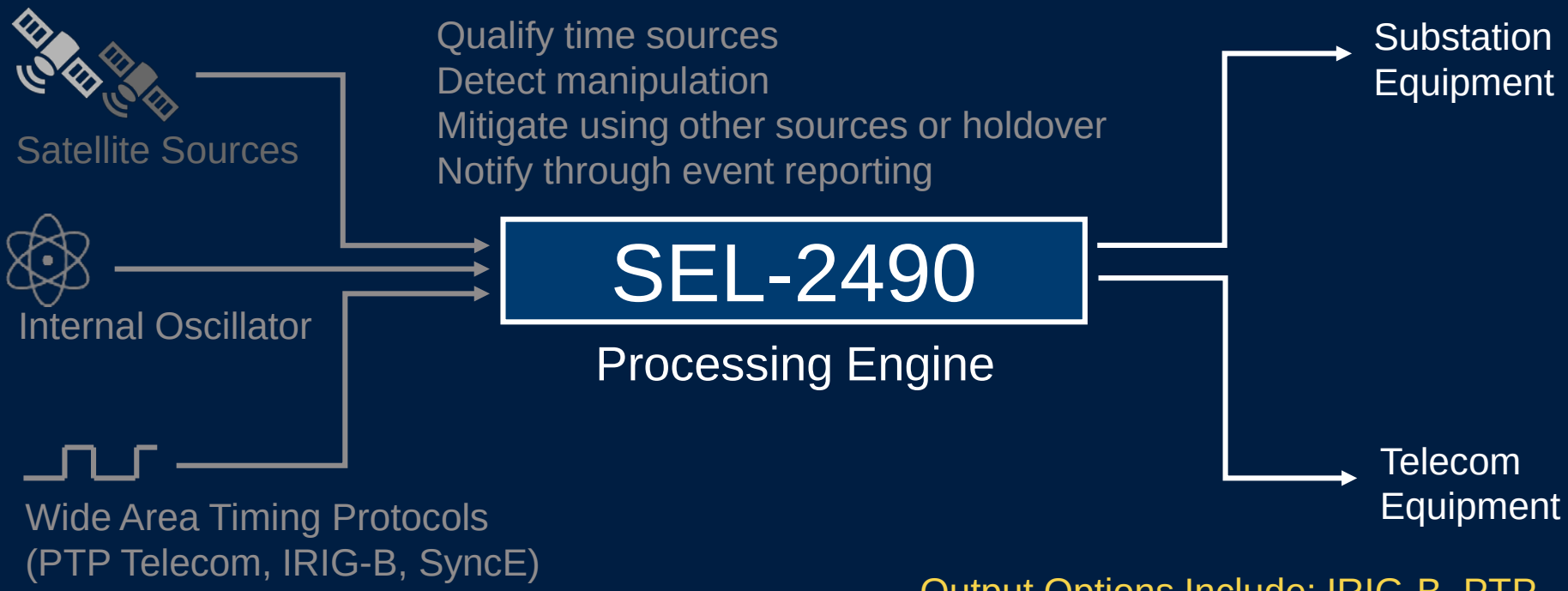
Reception of Multiple Time Sources



Ability to Evaluate and Compare Sources



Deliver High Accuracy Time Via Different Formats



Output Options Include: IRIG-B, PTP (Telecom and Power Profile), NTP, Pulse

SEL-2490 Advanced Detection