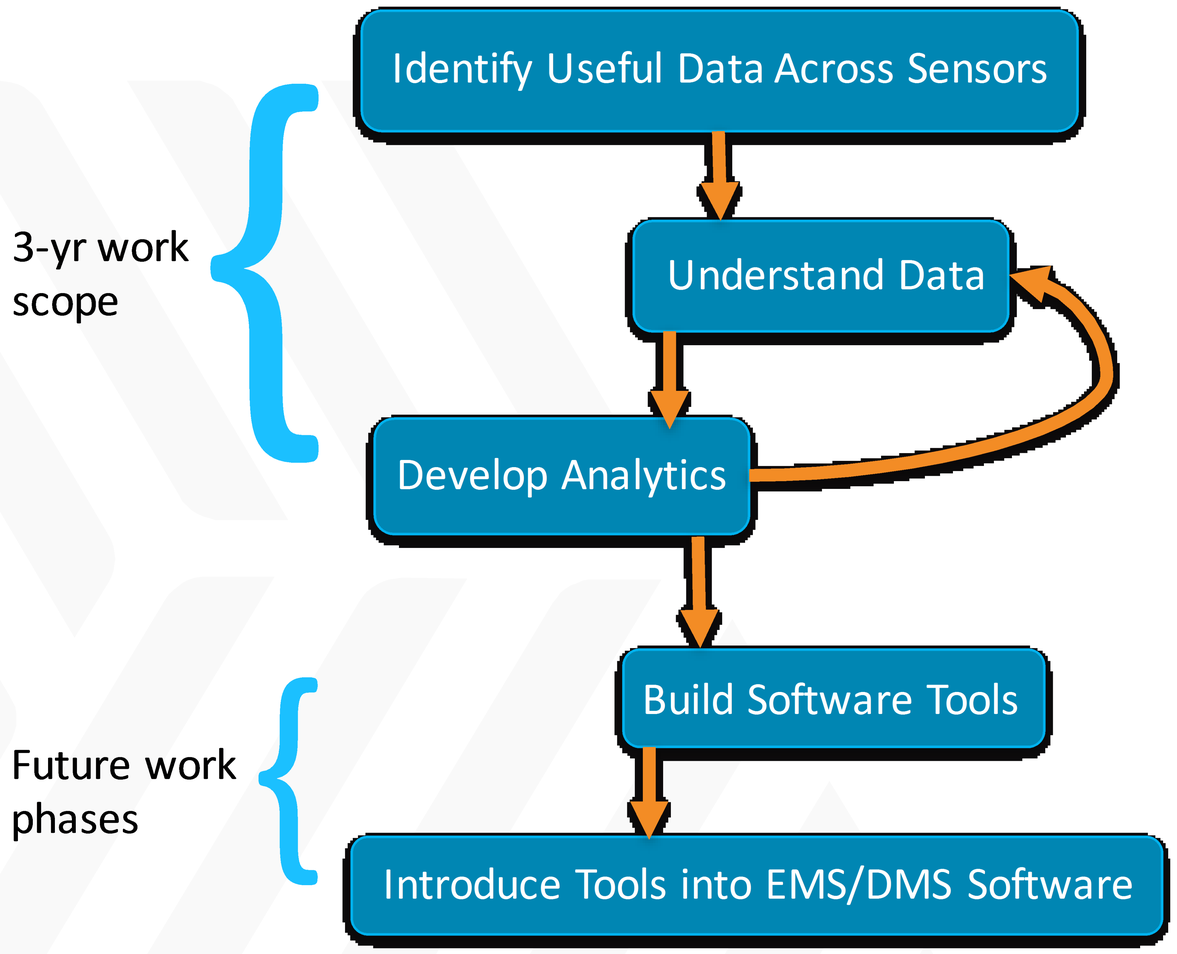
Threat Detection and Response with Data Analytics

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Project Description

- Develop advanced analytics on operational technology (OT) cyber data in order to detect complex cyber threats. Differentiate between cyber and non-cyber-caused incidents using available cyber data.



Expected Outcomes

- Analytics being developed will assist asset owners in triaging grid incidents
- Identifying incidents in a timely manner reduces outages and associated costs

Significant Milestones	Date
Establish MOU with industry collaborator (EPB) and identify sample data sets (related to NESCOR, EPB Smart Grid operations, etc.) for analysis. (ORNL)	10/1/16
Establish use case for evaluation of case studies. (INL)	4/1/17
Integrate SEL-3620 into selected NESCOR scenario. Identify physical and cyber events (features) in SEL-3620 available for monitoring. (SNL)	4/1/17
Organize subset of public outage data for specific distribution outages and transmission circuits for analysis. (ORNL)	4/1/17
Identify simulator requirements to perform attack-defense-mitigation study on PNNL testbed. (PNNL)	4/1/17

Progress to Date

- Preparing submittal to Resilience Week 2017
- Presented project to DARPA, EPSA, DHS, WAPA and CAISO
- Seeking further industry partners for data sharing, demonstration, and commercialization