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

Cyber-Attack Detection and Accommodation for the Energy Delivery System

GE Global Research

Matthew Nielsen

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Cyber ADA for Energy Delivery System

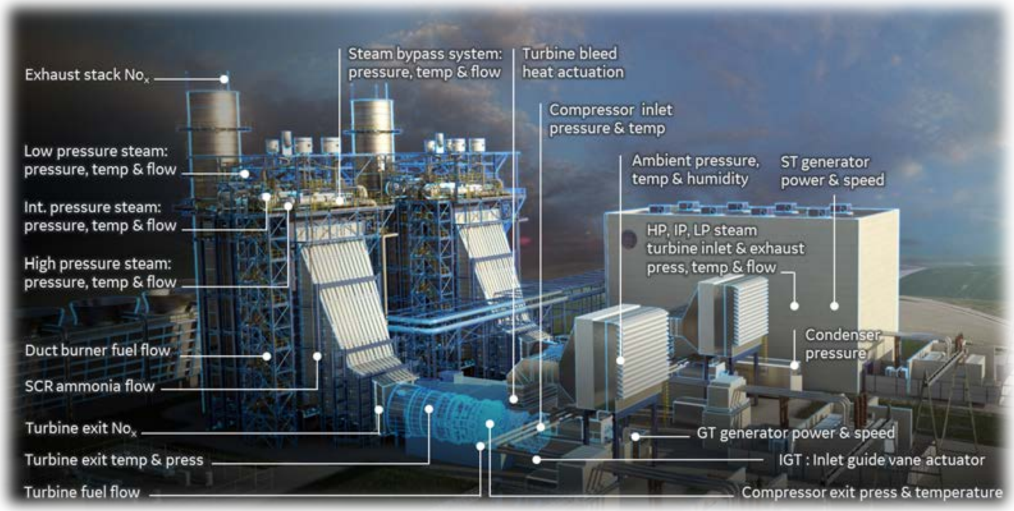
Objective

- Problem: cyber-attacker has made it past IT/OT security
- Proposed Technology:
  - **Detect** asset abnormal behavior
  - **Locate** attack focal points (nodes)
  - **Forecast** trending to abnormal behavior
  - **Neutralize** attacked nodes

Schedule

- Project dates: 10/1/16 – 9/30/19
- Key milestones & deliverables
  - Threats & Attack Simulations: 8/31/18
  - Feature Discovery: 5/16/18
  - ADA Algorithms: 8/31/18
  - Early Warning Algorithms: 8/31/18
  - Requirements & Concept Def: 12/30/18
- GE developing commercial plan & go to market strategy now.

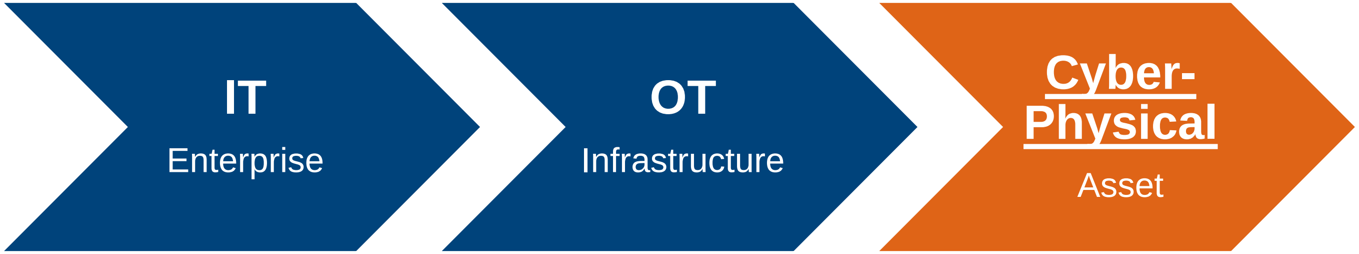
Detect **Locate** **Neutralize**


Exhaust stack No_x
Steam bypass system: pressure, temp & flow
Turbine bleed heat actuation
Compressor inlet pressure & temp
Low pressure steam: pressure, temp & flow
Ambient pressure, temp & humidity
ST generator power & speed
Int. pressure steam: pressure, temp & flow
HP, IP, LP steam turbine inlet & exhaust press, temp & flow
High pressure steam: pressure, temp & flow
Condenser pressure
Duct burner fuel flow
SCR ammonia flow
Turbine exit No_x
GT generator power & speed
Turbine exit temp & press
IGT : Inlet guide vane actuator
Turbine fuel flow
Compressor exit press & temperature

Total Value of Award:	**$4.1MM**
Funds Expended to Date:	**70%**
Performer:	**GE Global Research**
Partners:	**GE Power**

Advancing the State of the Art (SOA)

- **Today…**
  - Many current commercial products focus on keeping out attacker.
  - Industry, R&D & commercial efforts underway looking at learning models to understand OT network behavior and finding anomalies.
- **GE's ADA is a new layer of defense and uses the <u>physics</u> of the power generation asset for protection**



- **Feasibility demonstrated with plant/asset/grid dynamic simulations**
- **GE ADA should provide end users:**
  - High detection accuracies and (better observability)
  - Low false positive rates (less alarm fatigue)

Challenges to Success

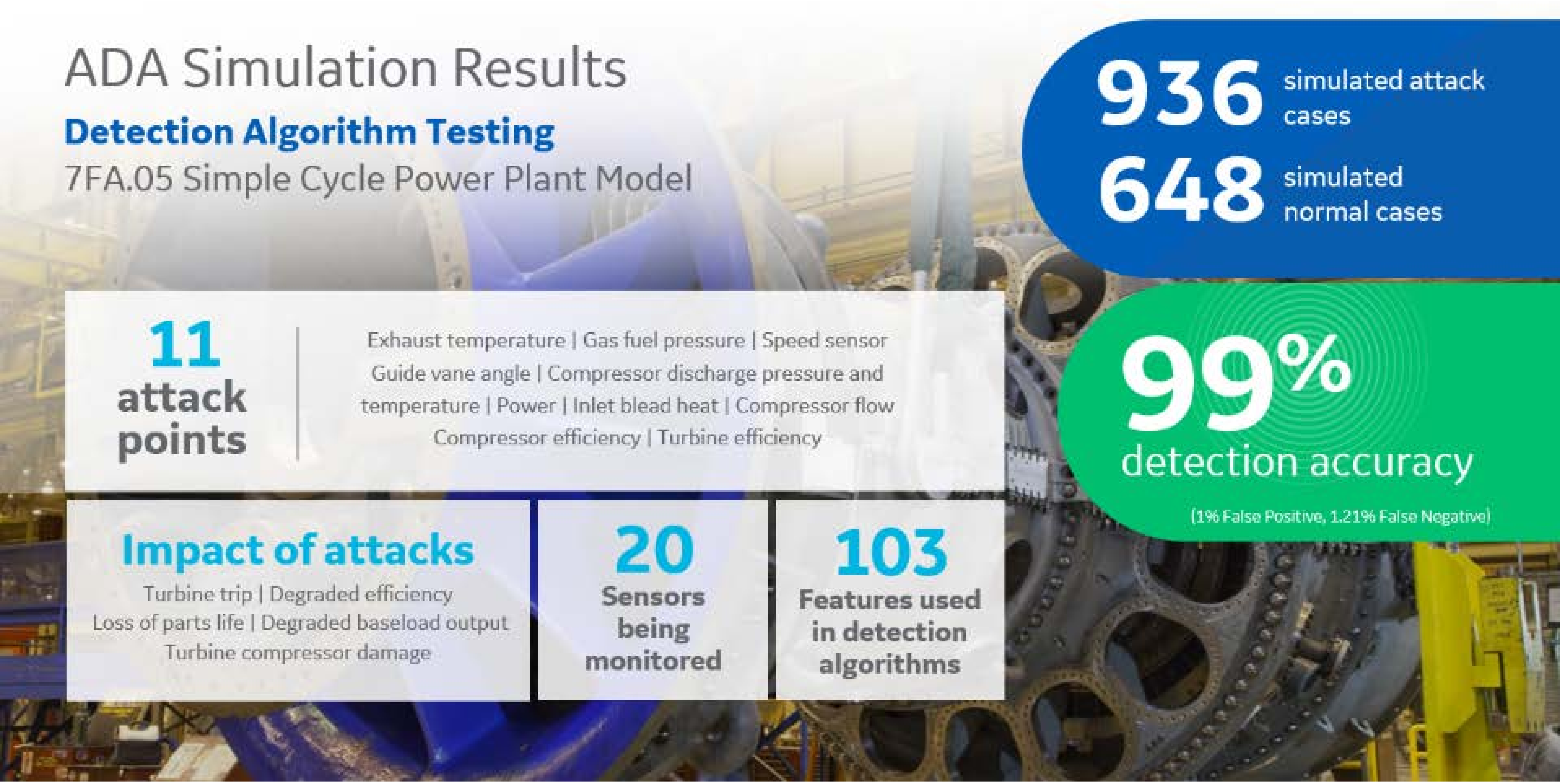
Challenge 1 – Focal Plant for Phase 2 Demonstration

- *Strategically shifting to larger gas turbine fleet*
- Connecting with GE O&M sites (GE run plants)
- Utilizing GE's extensive customer network
- Timeline: finalize by year end

Challenge 2 – Validating & Acceptance of Accommodation

- *Accommodation will happen during asset operation*
- Continue validation with high fidelity simulations
- Test at GE full speed, full load test stand
- Timeline: continue work in 2019+

Progress to Date: Gas Turbine Detection



ADA Simulation Results

Detection Algorithm Testing

7FA.05 Simple Cycle Power Plant Model

936 simulated attack cases

648 simulated normal cases

11 attack points

Exhaust temperature | Gas fuel pressure | Speed sensor
Guide vane angle | Compressor discharge pressure and temperature | Power | Inlet blead heat | Compressor flow
Compressor efficiency | Turbine efficiency

99% detection accuracy

(1% False Positive, 1.21% False Negative)

Impact of attacks

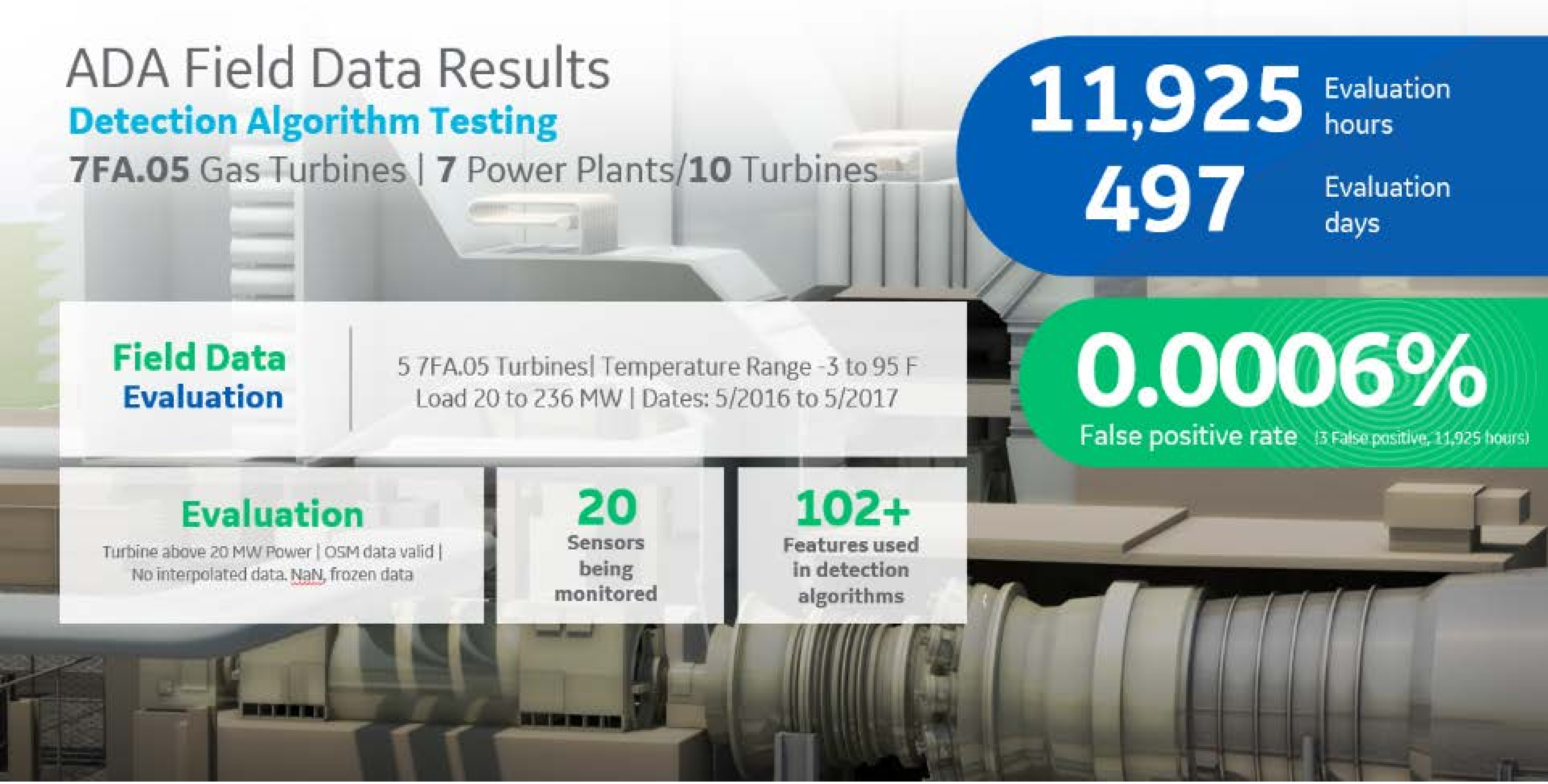
Turbine trip | Degraded efficiency
Loss of parts life | Degraded baseload output
Turbine compressor damage

20 Sensors being monitored

103 Features used in detection algorithms

1 Gas Turbine Produces Enough Power for ~250,000 Homes

Progress to Date: Field Test



ADA Field Data Results

Detection Algorithm Testing

7FA.05 Gas Turbines | **7** Power Plants/**10** Turbines

11,925 Evaluation hours

497 Evaluation days

0.0006%

False positive rate (3 False positive, 11,925 hours)

Field Data Evaluation

5 7FA.05 Turbines| Temperature Range -3 to 95 F
Load 20 to 236 MW | Dates: 5/2016 to 5/2017

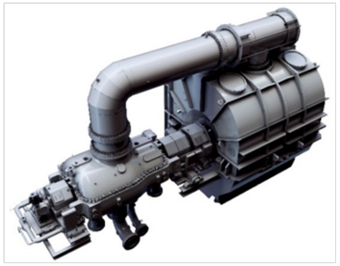
Evaluation

Turbine above 20 MW Power | OSM data valid |
No interpolated data. NaN, frozen data

20
Sensors being monitored

102+
Features used in detection algorithms

Progress to Date: Power Gen Assets

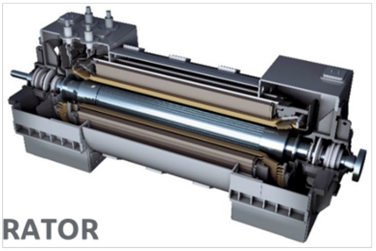


STEAM TURBINE

DETECTION		PREDICTED	
		NORMAL	ATTACK
TRUE	NORMAL	99.87	0.13
	ATTACK	1.75	98.25

LOCALIZATION		PREDICTED	
		NORMAL	ATTACK
TRUE	NORMAL	99.98	0.012
	ATTACK	2.40	97.6

Normal Cases = 480; Attack Cases = 480; Nodes = 12 (for Localization)

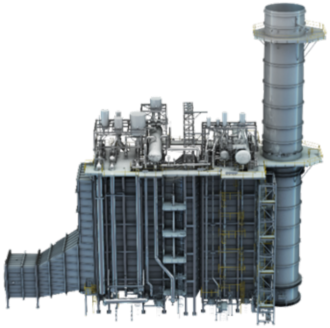


GENERATOR

DETECTION		PREDICTED	
		NORMAL	ATTACK
TRUE	NORMAL	99.00	1.00
	ATTACK	0.54	99.46

LOCALIZATION		PREDICTED	
		NORMAL	ATTACK
TRUE	NORMAL	100.00	0.00
	ATTACK	0.57	99.43

Normal Cases = 33; Attack Cases = 21; Nodes = 3 (for Localization)



HRSG

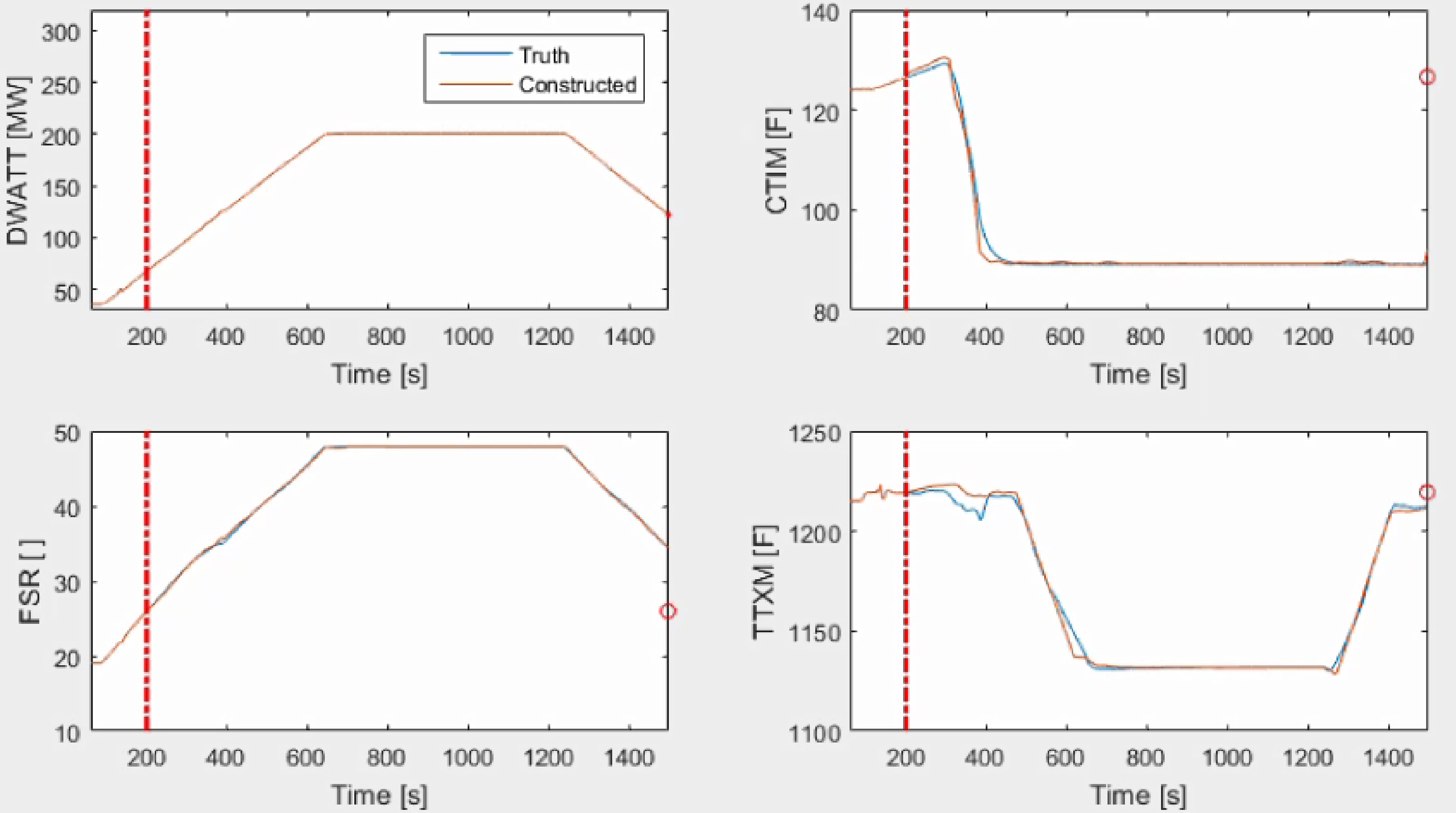
DETECTION		PREDICTED	
		NORMAL	ATTACK
TRUE	NORMAL	99.00	1.00
	ATTACK	0.34	99.66

LOCALIZATION		PREDICTED	
		NORMAL	ATTACK
TRUE	NORMAL	97.19	2.81
	ATTACK	0.00	100.00

Normal Cases = 49; Attack Cases = 7; Nodes = 7 (for Localization)

METHDOLOGY SCALES ACROSS MULTIPLE ASSETS

Progress to Date: GT Accommodation



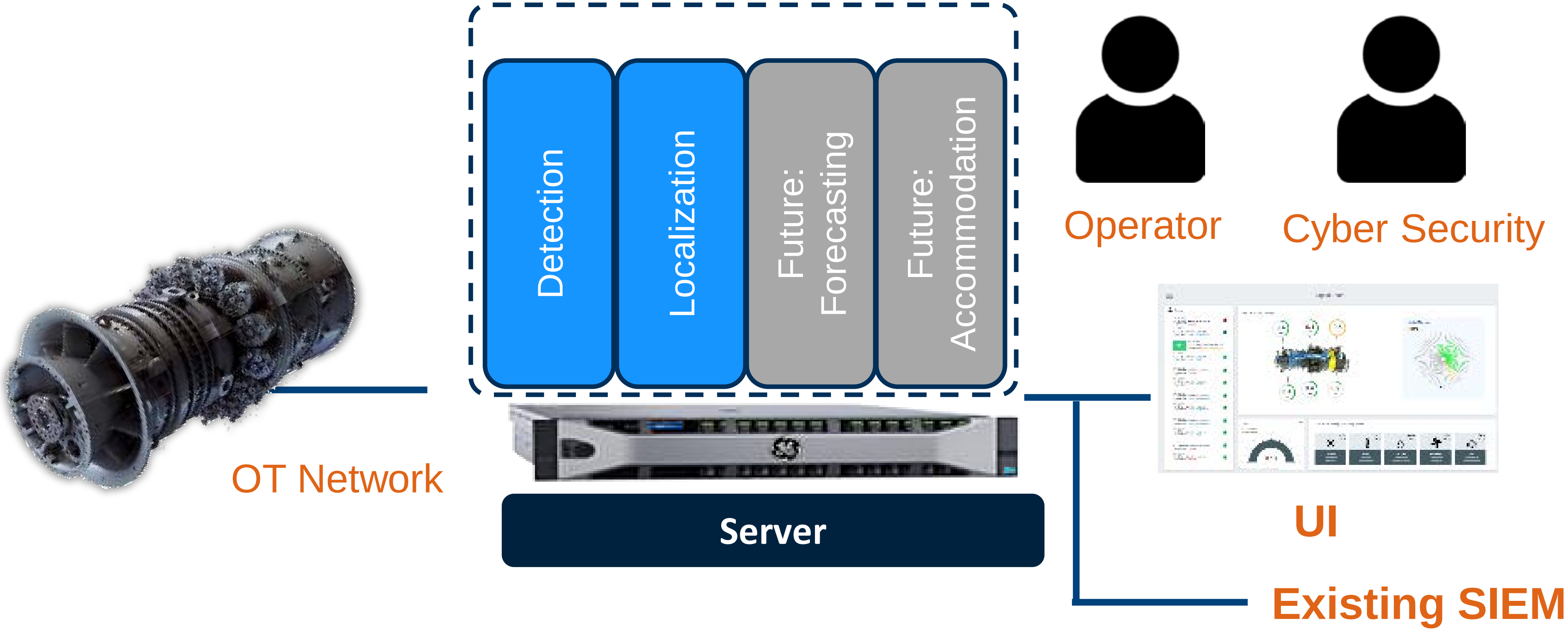
7F Gas Turbine Simple Cycle Simulation

30MW to Baseload to 30MW

6 out of 15 nodes attacked

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

Collaboration/Technology Transfer



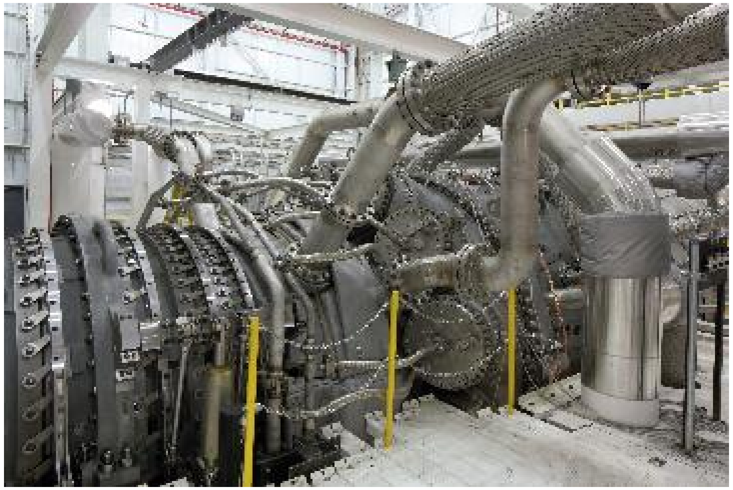
Technology Transfer

- End users: power plant operators and cyber security specialists
- Working with GE Power to define requirements for commercial product
- Future: run proof-of-concepts

Next Steps for this Project

Milestones for Phase 2

1) Commercial strategy & product requirements
2) GE test stand with 9HA.02 gas turbine full speed, full load
3) Power plant with 7FA.04 gas turbine



GE Test Stand (1)

7FA.04 GE Gas Turbine (2)

(1) https://www.ge.com/reports/point-break-where-the-worlds-largest-gas-turbines-prove-their-mettle/
(2) https://www.ge.com/power/gas/gas-turbines/7f-04