Security Prognostics

Scott Evans, Ph.D. (evans@ge.com)
Machine Learning Lab – GE Research

Outline

Context And Sources

Why Security Prognostics?

What are “Security Prognostics?”

What is the Current State?

- Digital Twin

Wind Power Use Case

- Performance and Validation
- Security Offerings – Wind Power Use Case

How Can We move Forward?

Main Sources

Security Prognostics: Cyber meets PHM

Scott C. Evans
GE Global Research
Niskayuna, NY, USA
evans@ge.com

Piyush Mishra
GE Global Research
Niskayuna, NY, USA
mishrapi@ge.com

Weizhong Yan
GE Global Research
Niskayuna, NY, USA
Yan@ge.com

Bouchra Bouqata
GE Global Research
Niskayuna, NY, USA
bouqata@ge.com

***Abstract*— In this paper we cast a vision for Security Prognostics (SP) for critical systems, promoting the view that security related protections would be well served to integrate fully with Monitoring and Diagnostics (M&D) systems that assess the health of complex assets and systems. To detect complex Cyber threats we propose combining system parameters already in use by M&D systems for Prognostics and Health Monitoring (PHM) with security parameters. Combining system parameters used by M&D to detect non-malicious faults with the system parameters used by security schemes to detect complex Cyber threats will improve: (a) accuracy of PHM (b) security of M&D, and (c) availability and safety of critical systems. We also introduce the notion of Remaining Secure Life (RSL), assessed based on the propagation of "security damage," to create the prospect for Security Prognostics. RSL will assist in the selection of appropriate response(s), based on breach or compromise to security component's and potential impact on system operation. An example of M&D data is provided which is normally associated with non-malicious faults providing input to detect Malware execution through time series monitoring.**

Keywords-component: Cyber-Security; Remote Monitoring and Diagnostics; Prognostics and Health Monitoring; Zero Day Attack

I. INTRODUCTION

Cyber threats are difficult to address for tactical platforms and critical infrastructure precisely because of the mission critical and time sensitive nature of these platforms. Compromise and/or loss of use of these resources provide disproportionate harm, and any action taken in response to attack or compromise must be carefully selected. These actions need to consider the platforms at risk, their role in the overall mission, and the state of mission conditions at the time. Today there is no effective way to navigate these issues and provide Security Prognostics (SP) for a critical system.

Part of the cause of this situation is that, in our view, cyber security has suffered from being treated as a separate/independent task in the monitoring of information systems rather than an integral part of Monitoring and Diagnostics M&D or Prognostics and Health Management (PHM). M&D systems, for example, can detect imminent air craft engine failure through anomaly detection and various classification and diagnostic techniques/machine learning algorithms, but if these types of algorithms are applied to the problem of cyber security it is generally as part of a separate system that is "bolted on" after the fact rather than developed within systems that monitor and maintain system health. Certainly PHM and M&D systems must be made secure. But more – these systems must be able to distinguish between a material failure of a component and, for example StuxNet. Today systems lack complete situational awareness to detect and respond to complex Cyber threats which are gradual and subtle processes often taking course over time periods ranging from days to years as shown in Figure 1. Detection against innovative, zero day, attacks requires even more care.

We propose a vision for Security Prognostics (SP) by integrating PHM, information security, and Machine Learning diagnostics technologies. In this paradigm we consider cyber-health as an integrated aspect of system PHM and consider malicious attack as a subset of faults that systems incur. Just as prognostics systems seek to detect impending non-malicious failures and assessing remaining useful life based on the damage sustained, so will SP assess the cyber-health of a system and its Remaining Secure Life – a measure of the urgency with which security issues must be addressed. It is important to note that due to increased frequency and intensity of cyber threats, tight coupling of PHM, M&D, and information security is also essential to support the emerging paradigm of remote and/or cloud-based M&D. Likewise, this integration will not be without risk, as more capable systems if compromised are susceptible to deeper damage.

In this paper we outline the current state of our research on SP paradigm and its main components: (a) M&D of traditional physical parameters currently used to assess material health status of a system and how it can provide new methods for detecting malicious breach, (b) innovative M&D of cyber parameters to monitor and analyze the operating state of cyber systems controlling physical systems, and (c) information security schemes used to secure flow of information among physical and digital systems. shows a simplified view of the integrated approach using power plant setup as an example. Our view is that goals of both system health and Cyber-health speak to a converged system of PHM/SP.

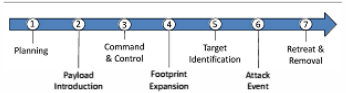
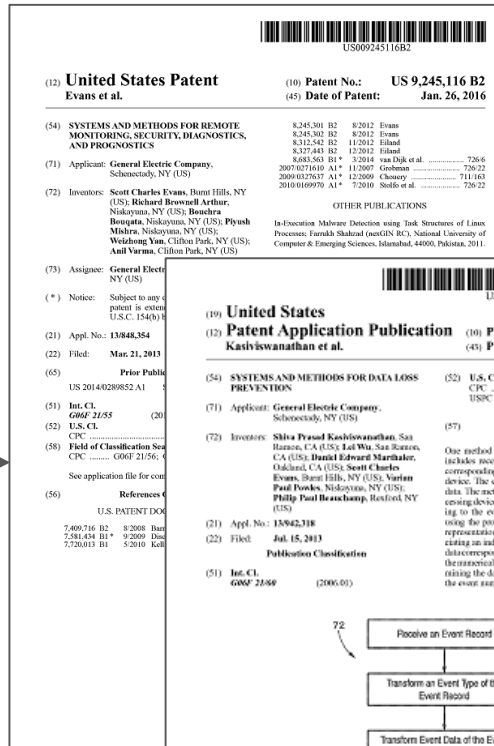


Figure 1: Seven steps of cyber-attack

Prognostics and Health Management (PHM), 2013 IEEE

US Patent Issued January 2016

US Patents Application Published Jan 15



US009245116B2

(12) **United States Patent**
Evans et al.

(10) **Patent No.: US 9,245,116 B2**
(45) **Date of Patent: Jan. 26, 2016**

(54) **SYSTEMS AND METHODS FOR REMOTE MONITORING, SECURITY, DIAGNOSTICS, AND PROGNOSTICS**

(71) Applicant: **General Electric Company**, Schenectady, NY (US)

(72) Inventors: **Scott Charles Evans**, Burnt Hills, NY (US); **Richard Brownell Arthur**, Niskayuna, NY (US); **Bouchra Bouqata**, Niskayuna, NY (US); **Piyush Mishra**, Niskayuna, NY (US); **Weizhong Yan**, Clifton Park, NY (US); **Anil Varma**, Clifton Park, NY (US)

(73) Assignee: **General Electr** NY (US)

(*) Notice: Subject to any o patent is exten U.S.C. 154(b) b

(21) Appl. No.: **13/848,354**

(22) Filed: **Mar. 21, 2013**

(65) **Prior Publi**
US 2014/0289852 A1

(51) **Int. Cl.**
G06F 21/55 (20

(52) **U.S. Cl.**
CPC .....

(58) **Field of Classification Sea**
CPC G06F 21/56;
See application file for com

(56) **References C**

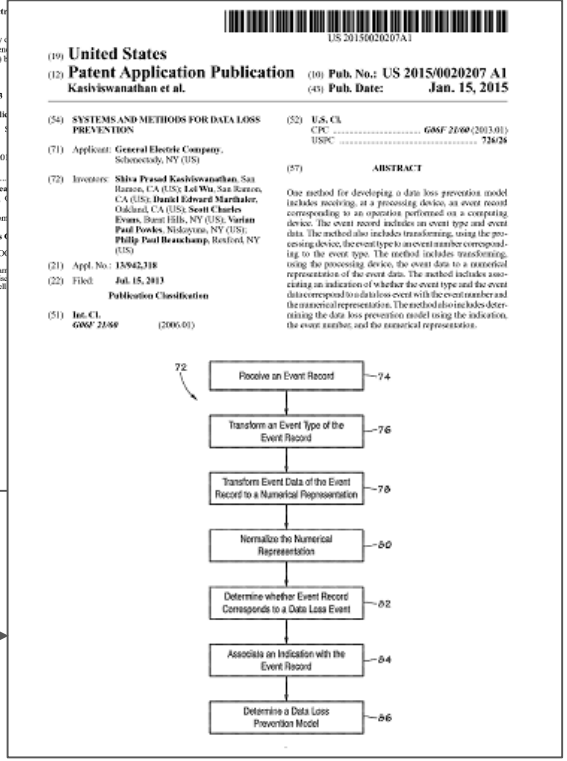
U.S. PATENT DO

7,409,716 B2 8/2008 Ban
7,581,434 B1 * 9/2009 Dia
7,720,013 B1 5/2010 Kell

8,245,301 B2 8/2012 Evans
8,245,302 B2 8/2012 Evans
8,312,542 B2 11/2012 Eiland
8,327,443 B2 12/2012 Eiland
8,683,563 B1 * 3/2014 van Dijk et al. 726/6
2007/0271610 A1 * 11/2007 Grobman 726/22
2009/0327637 A1 * 12/2009 Chouery 711/163
2010/0169970 A1 * 7/2010 Stolfo et al. 726/22

OTHER PUBLICATIONS

In-Execution Malware Detection using Task Structures of Linux Processes; Farrukh Shahzad (nexGIN RC), National University of Computer & Emerging Sciences, Islamabad, 44000, Pakistan, 2011.



US 20150020207A1

(19) **United States**
(12) **Patent Application Publication**
Kasiviswanathan et al.

(10) **Pub. No.: US 2015/0020207 A1**
(45) **Pub. Date: Jan. 15, 2015**

(54) **SYSTEMS AND METHODS FOR DATA LOSS PREVENTION**

(71) Applicant: **General Electric Company**, Schenectady, NY (US)

(72) Inventors: **Shiva Prasad Kasiviswanathan**, San Ramon, CA (US); **Lei Wu**, San Ramon, CA (US); **Daniel Edward Marthaler**, Oakland, CA (US); **Scott Charles Evans**, Burnt Hills, NY (US); **Varun Paul Powles**, Niskayuna, NY (US); **Philip Paul Beauchamp**, Renford, NY (US)

(21) Appl. No.: **13/942,318**

(22) Filed: **Jul. 15, 2013**

Publication Classification

(51) **Int. Cl.**
G06F 21/60 (2006.01)

(52) **U.S. Cl.**
CPC *G06F 21/60* (2013.01)
USPC **726/26**

(57) **ABSTRACT**

One method for developing a data loss prevention model includes receiving, at a processing device, an event record corresponding to an operation performed on a computing device. The event record includes an event type and event data. The method also includes transforming, using the processing device, the event type to an event number corresponding to the event type. The method includes transforming, using the processing device, the event data to a numerical representation of the event data. The method includes associating an indication of whether the event type and the event data correspond to a data loss event with the event number and the numerical representation. The method also includes determining the data loss prevention model using the indication, the event number, and the numerical representation.

#IndustrialInternet

Why Security Prognostics?

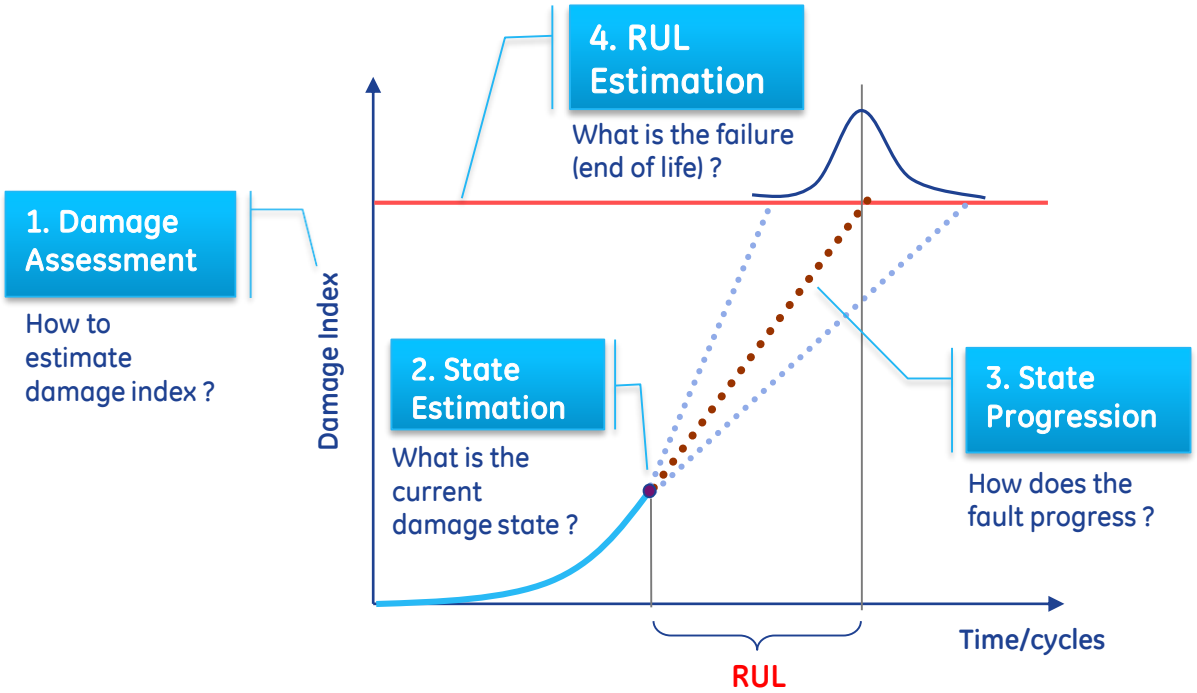
Current State: Cyber-Security has suffered from being treated as a separate/independent task in the monitoring of information systems rather than an integral part of Remote Monitoring and Diagnostics (M&D) or Prognostics and Health Management (PHM).

View: Defense against planned, coordinated malicious attacks such as the Critical Infrastructure can expect to encounter will **require *more system integration and functionality*** *than detection and correction of non-malicious faults*, ***not less***

Challenges*:* Multi-level security, Vulnerability to new attacks

Convergence provides more features to learn on, more models with which to distinguish behavior.

Prognostics



What are the Crack Equivalents for Security?

Time since Re-image

Number of Ports/Users

Number of incomplete Patches

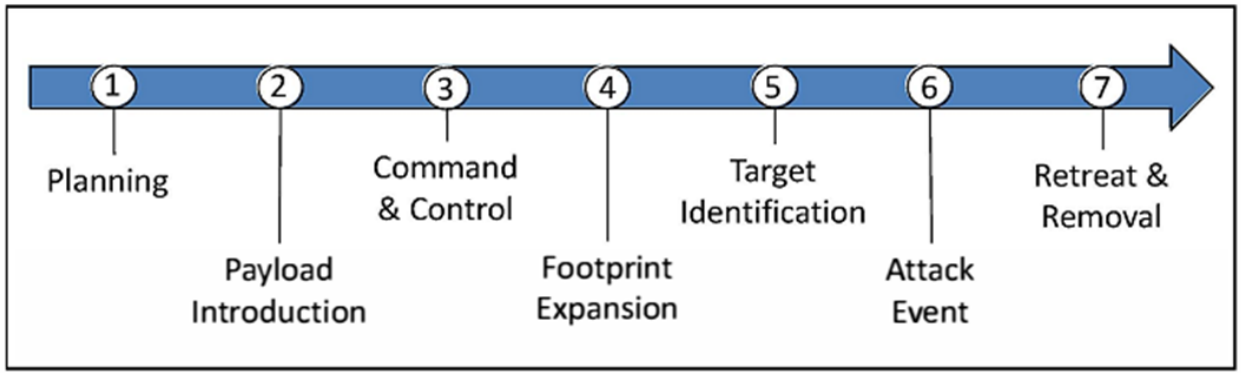
Age of Architecture

Encryption

Any Measurable Surface Area or Distance Metric

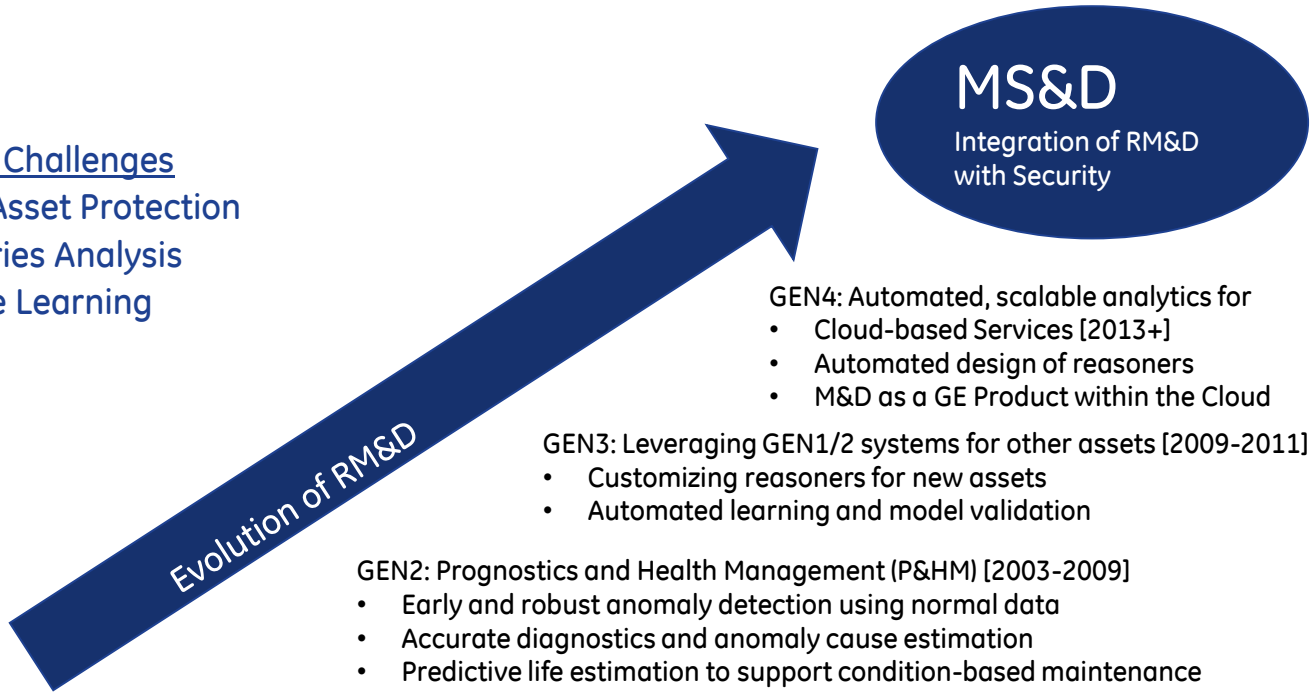
Prognostics -> Security

Prognostics and Health Domain	Cyber Security Domain
Remaining Useful Life (RUL)	Remaining Secure Life (RSL)
Damage	Breach/Compromise
Anomaly Detection	Anomaly Detection



7 Steps of Cyber Attack

Evolution of service analytics and Security



Time Series Diagnostic Process

Illustrative Example: Benign vs. Malicious processes

1	'pBytes'
2	'pCount'
3	'reads[name]'
4	'writes[name]'
5	ftypes (minor)'
6	ftypes (major)'
7	'run_time[target()]'
8	'io_wait_time[target()]'
9	'sleep_time[target()]'
10	'queued_time[target()]'
11	uscaled'
12	kscaled'
13	'syscalls[target()]'
14	'allticks'
15	'gettimeofday_ns()'
16	'stack_used()'
17	'stack_size()'
18	'task_stime()'
19	'uaddr()'
20	'proc_mem_size()'
21	'proc_mem_rss()'
22	'proc_mem_shr()'
23	'proc_mem_txt()'
24	'proc_mem_data()'
25	'mem_page_size()'

(a)

1	'pBytes'
2	'pCount'
3	'reads[name]'
4	'writes[name]'
5	ftypes (minor)'
6	'run_time[target()]'
7	'sleep_time[target()]'
8	'queued_time[target()]'
9	uscaled'
10	kscaled'
11	'syscalls[target()]'
12	'allticks'
13	'gettimeofday_ns()'
14	'stack_used()'
15	'task_stime()'
16	'uaddr()'
17	'proc_mem_size()'
18	'proc_mem_rss()'
19	'proc_mem_shr()'
20	'proc_mem_txt()'
21	'mem_page_size()'

(b)

Figure 1: Feature set of interest

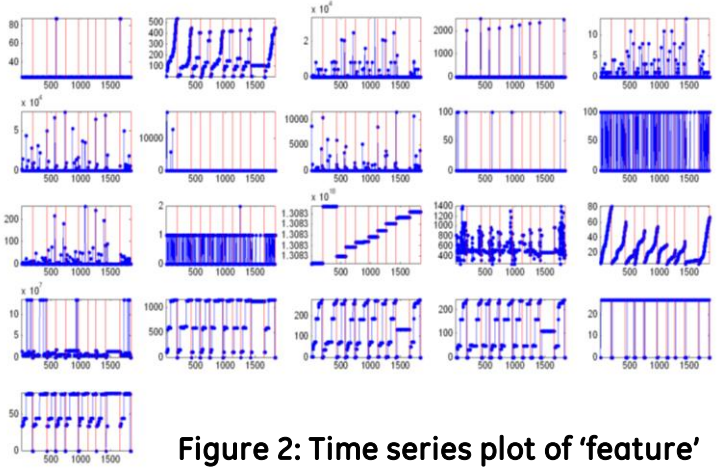


Figure 2: Time series plot of 'feature'

Results and Analysis

Table I: Extracted Feature

#	Features
1	mean of 'proc_mem_size'
2	mean of 'proc_mem_shr'
3	mean of 'mem_page_size'
4	ratio of maximum 'pCount' and maximum 'task_stime'
5	variance of 'proc_mem_size'
6	variance of 'proc_mem_shr'
7	variance of 'mem_page_size'
8	median of 'stack_used'
9	correlation coefficient between 'stack_used' and 'mem_page_size'
10	correlation coefficient between 'proc_mem_shr' and proc_mem_txt'

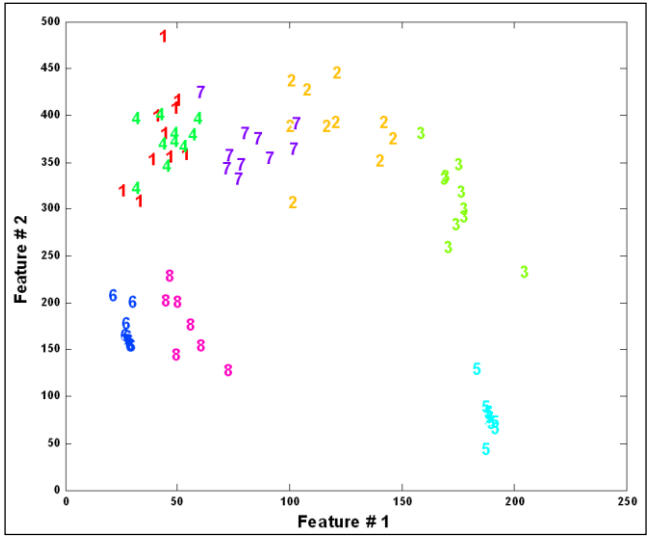
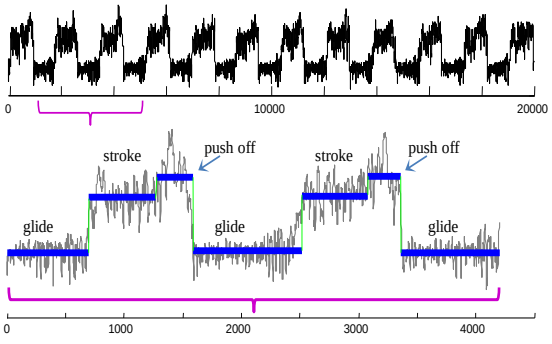


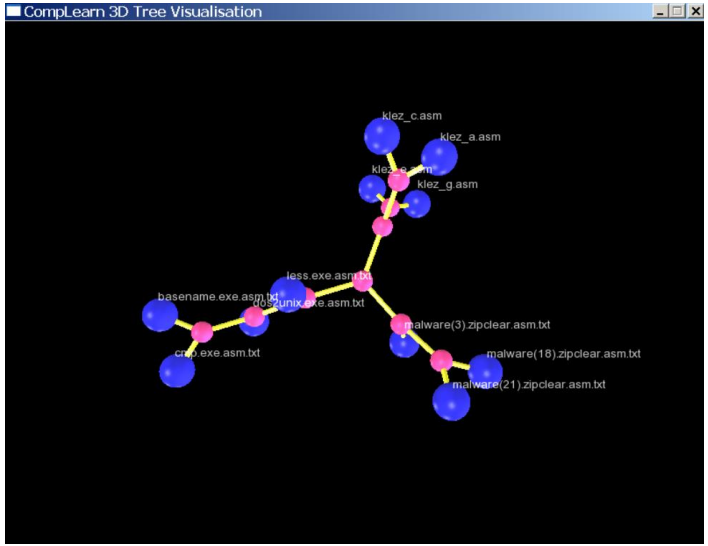
Figure 3: Scatter plot of features

		predicted						
		cat	ls	ps	pwd	top	which	who
TRUE	cat	9	0	0	1	0	0	0
	ls	0	10	0	0	0	0	0
	ps	0	0	10	0	0	0	0
	pwd	0	0	0	10	0	0	0
	top	0	0	0	0	10	0	0
	which	0	0	0	0	0	10	0
	who	0	0	0	0	0	0	10

Table I: Confusion matrix of the seven benign processes

Opportunities for Next Steps





References:

•Bing Hu, Thanawin Rakthanmanon, Yuan Hao, Scott Evans, Stefano Lonardi, and Eamonn Keogh (2011). Discovering the Intrinsic Cardinality and Dimensionality
of Time Series using MDL. ICDM 2011

•Thanawin Rakthanmanon, Eamonn Keogh, Stefano Lonardi, and Scott Evans (2011). Time Series Epenthesis: Clustering Time Series Streams Requires Ignoring Some Data, ICDM 2011

•http://www.cs.ucr.edu/~eamonn/selected_publications.htm

Outline

Context And Sources

Why Security Prognostics?

What are “Security Prognostics?”

What is the Current State?

- Digital Twin

Wind Power Use Case

- Performance and Validation
- Security Offerings – Wind Power Use Case

How Can We move Forward?

GE's Customers want Outcomes (not Technology)

Asset Performance Mgmt.

Single Asset

Reduce unplanned down time
Maintenance optimization

Analytics Based Maintenance

Life Models: Per Asset, Per Part and Per Failure Mode

Heterogeneous & Big Data

Operations Optimization

Group of Assets

Reduce operating cost
Increase output

Plant Level Optimization

Accurate Performance Models

Complex Interactions

Business Optimization

Complex Operations

Increased revenue
Cost reduction

Trip Optimizer, Movement Planner

Market Conditions

Interactions at scale

#IndustrialInternet

powered by GE

#IndustrialInternet

powered by

#IndustrialInternet

powered by

Design & Test

Operation

Inspection & Maintenance

Market

Engine #906260

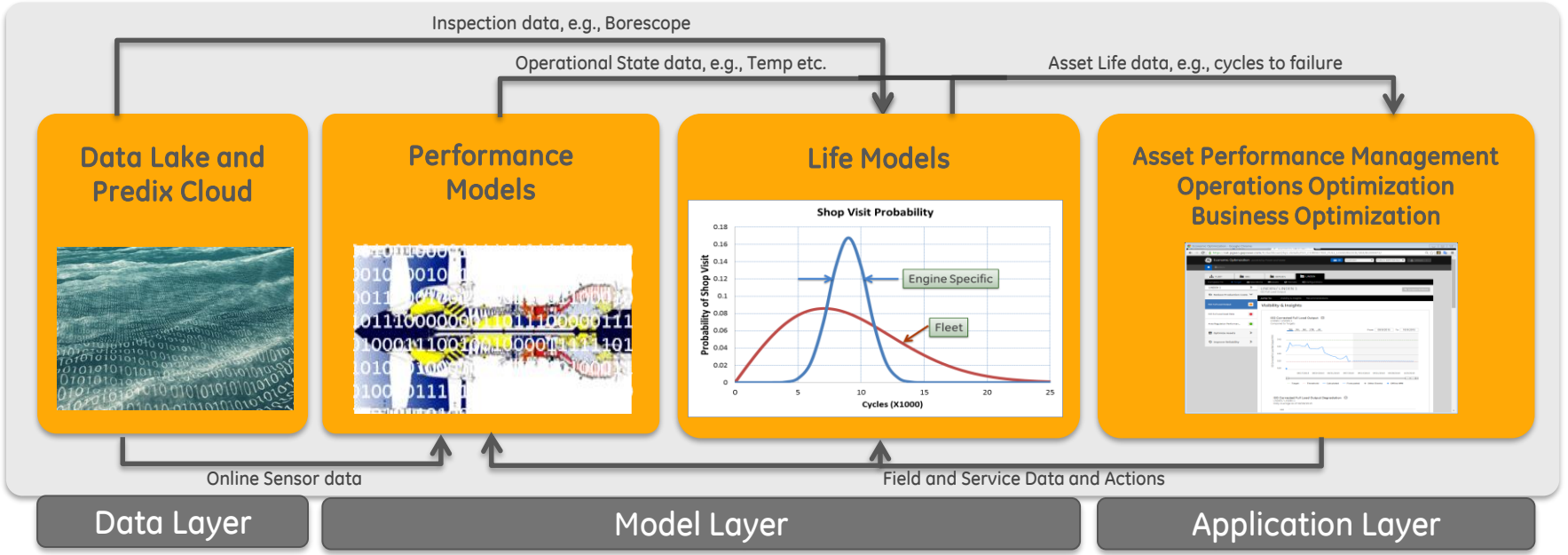
≈

Model #906260

Digital Twin Attributes

1. The model is applied per-asset
2. The model must be used to create demonstrable business value
3. The model must be adaptable
4. The model must be used in a continuous-update capacity
5. The model must be scalable

We make & connect various Digital Twin pieces



#IndustrialInternet

powered by

Key Enabling Technologies for Digital Twin

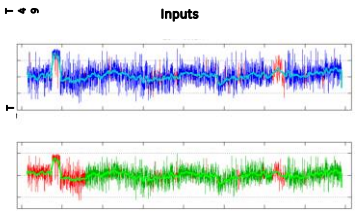
Innovation, Speed, and Scale

1 Domain Data

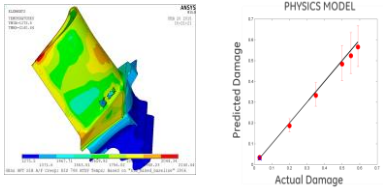
2 Physical + Digital Engineering Models

3 Industrial Analytics

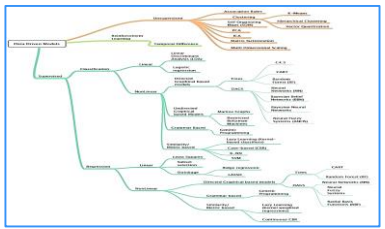
Automated Data Pre-processing



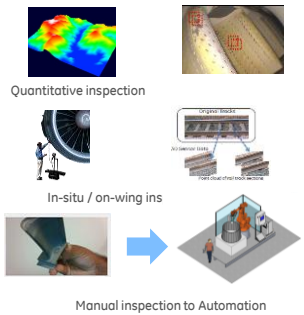
Cumulative Damage



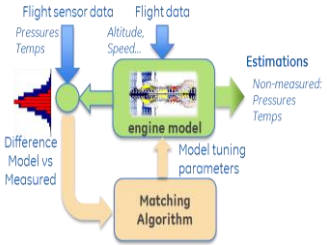
Model Generation & Automation



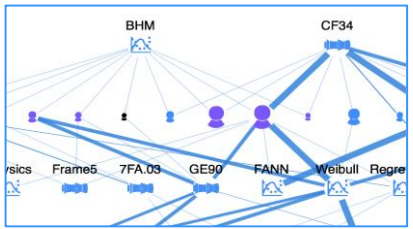
Inspection Capabilities



Dynamic Performance Estimation



Knowledge Extraction



4 PREDIX PLATFORM

Powered by GE

Outline

Context And Sources

Why Security Prognostics?

What are “Security Prognostics?”

What is the Current State?

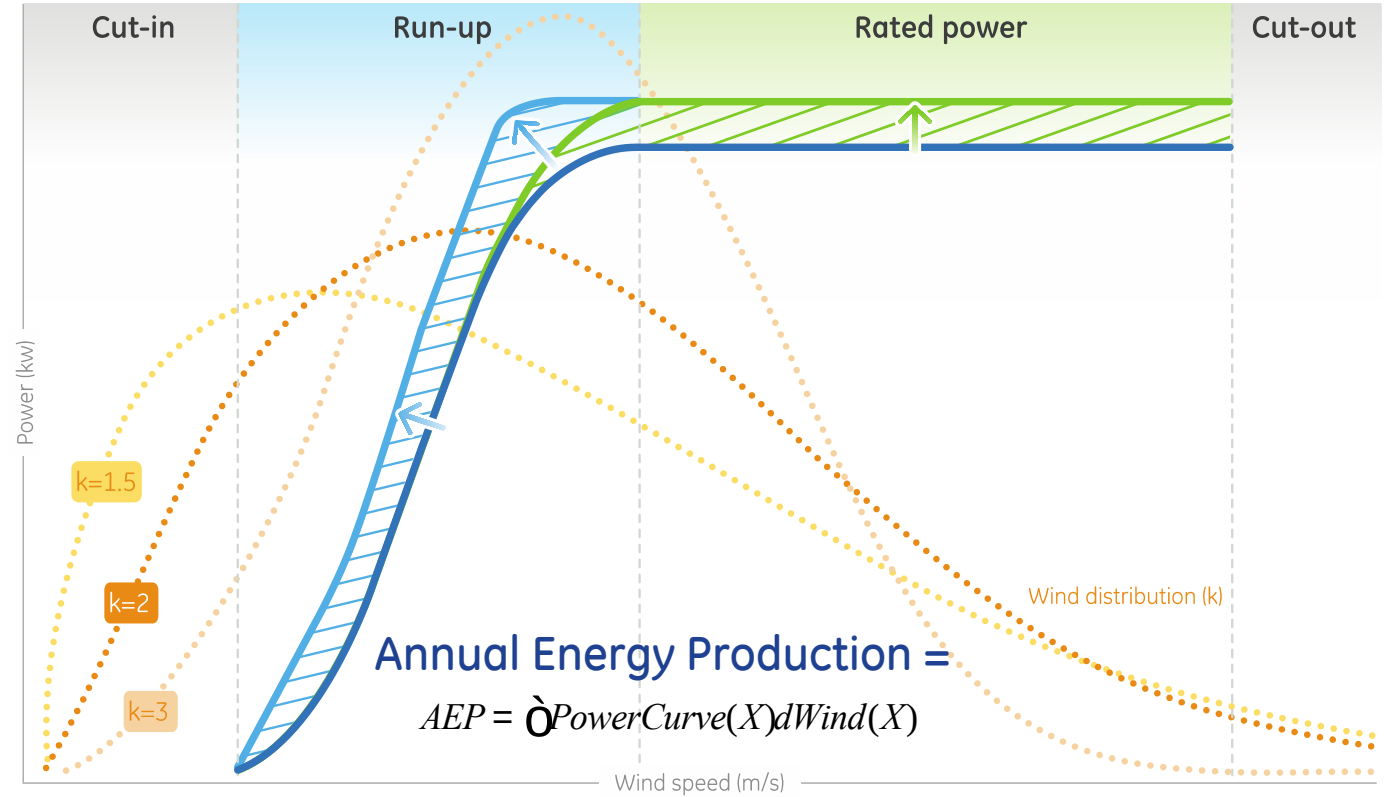
- Digital Twin

Wind Power Use Case

- Performance and Validation
- Security Offerings – Wind Power Use Case

How Can We move Forward?

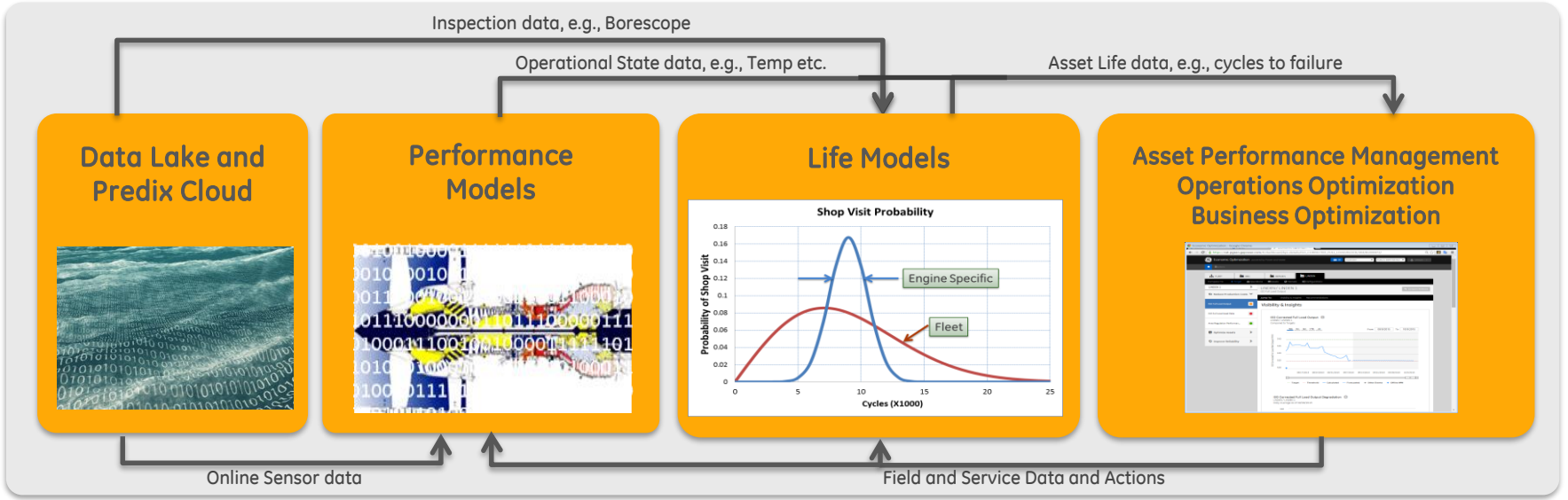
Power Up



Goal: Make Better Uses of Wind Resource Through Upgrades
https://renewables.gepower.com/wind-energy/turbine-services/platform-upgrades.html

imagination at work

We make & connect various Digital Twin pieces



Imputation Technologies

Data Driven And Physics Based

Traditional PHM

Plan of the Day Optimization

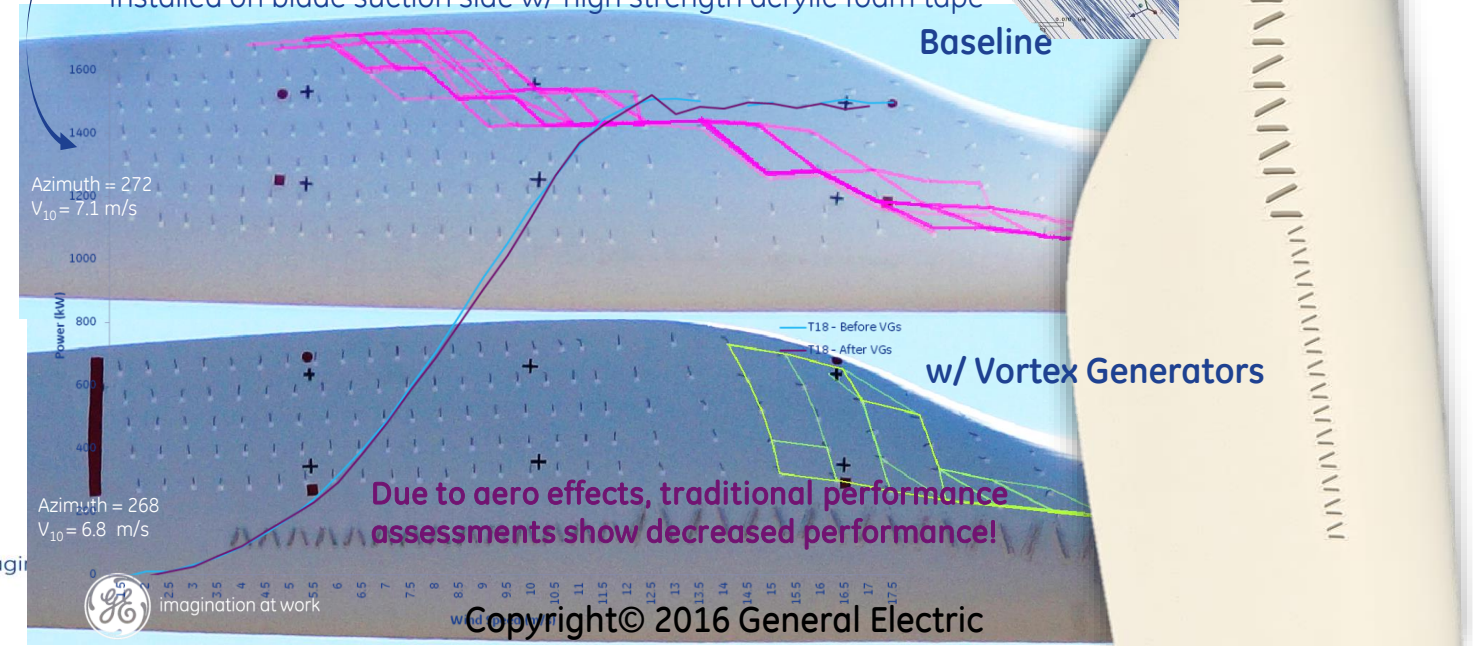
#IndustrialInternet

powered by

The Challenge

Validating Vortex Generator CM&U
Improving efficiency … 1-2% AEP

- VGs energize boundary layer & help re-attach flow
- Optimally designed through CFD & wind tunnel testing
- Field validated via wool tuft testing & production analysis
- Installed on blade suction side w/ high strength acrylic foam tape



imagination at work

Wind Empirical Models Motivation and Performance

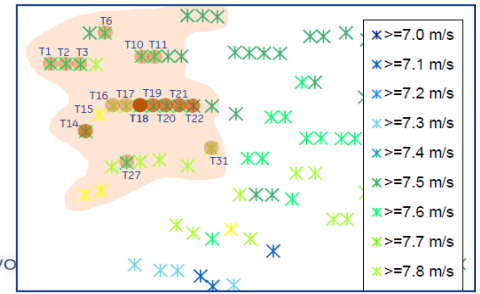
Motivation

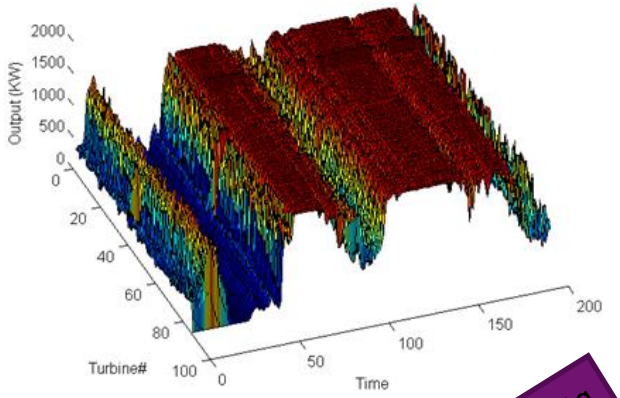
GE Wind sells many CM&Us providing small AEP gains (1-2%)

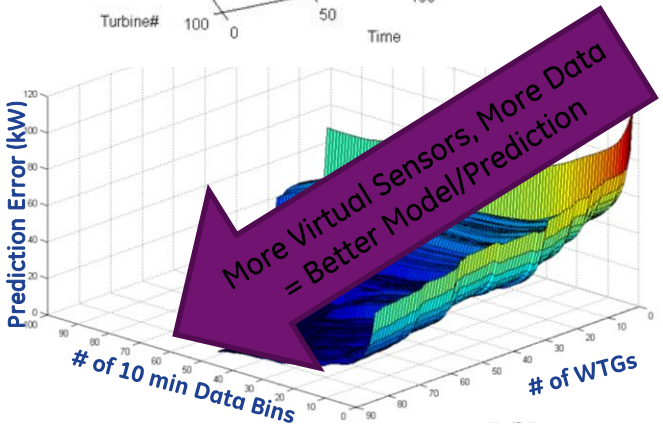
- These CM&Us are difficult to sell unless performance verified

Current AEP Performance Methods

1. Baseline using upstream Metmast
   - Limited Availability (Uncertainty ~0.5-2%)
   - $150K cost per metmast, technical restrictions
2. Use Onboard Anemometer
   - Valid if no major bias (Uncertainty ~0 .5-2%)
   - Not Valid if Aero affected – VG, Blade changes, etc.
3. GE Global Research Performance Analytics Tool
   - Uses neighboring turbines to build correlation model
   - Removes anemometer bias
   - Reduces AEP uncertainty <0.5%



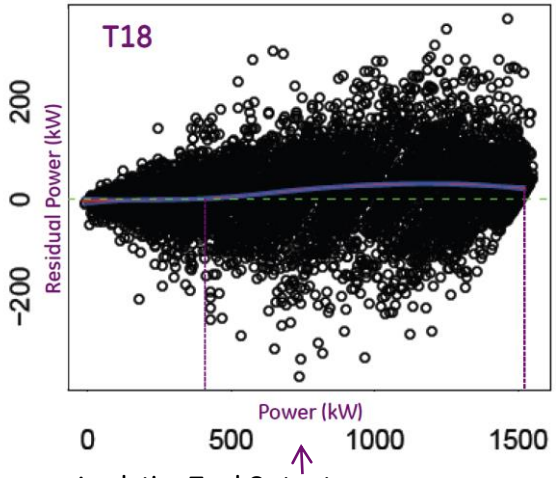




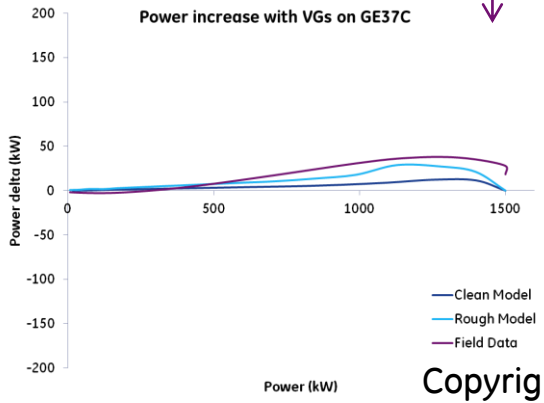
Simplified example of statistical solution:
WTG18 kW= a + b*WTG19 kW + c*WTG20 kW + …
Goal: develop a method to statistically determine coefficients a, b, c, d, …

Vortex Generator Pilot Performance Results

1.1% - 1.6% AEP Improvement



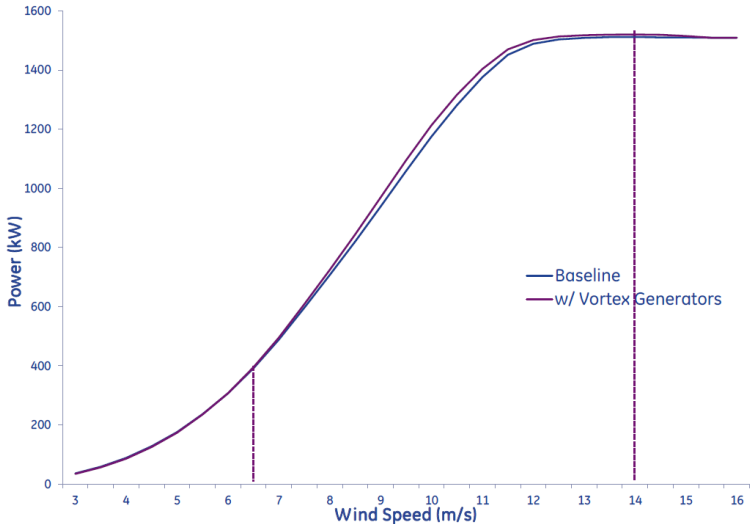
Analytics Tool Output
Matches Physics Model Simulation



Compare Actual Power Produced After Upgrade

To

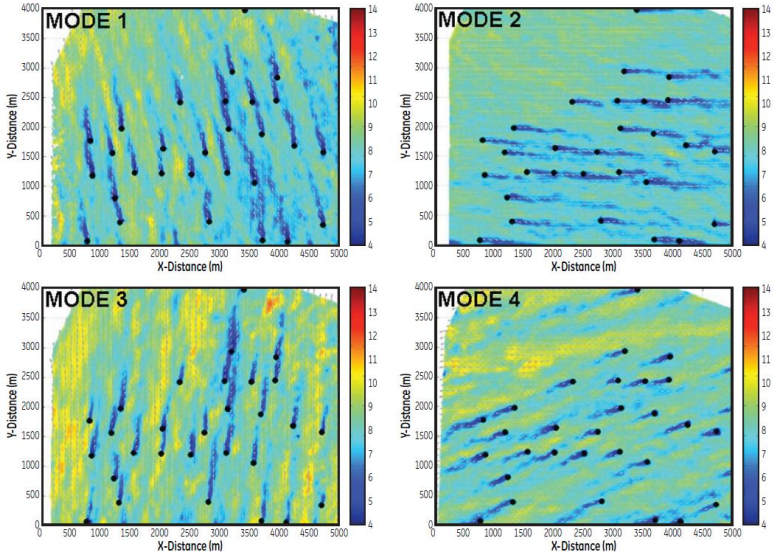
Estimated Power Expected given Other Inputs



Effective Power Curve Change

Wake Optimization Challenge

- Field Flow has huge impact
  - Flow is Complex
- Field Flow Measurement is Costly
  - Radar
  - Lidar
  - Metmast



Nacelle Mounted Lidar – $80k to $100k per sensor

Radar Wakes Measurement

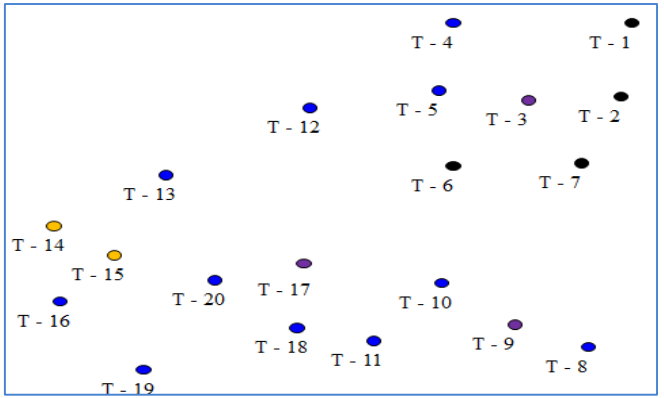
Texas Tech

Challenge: Optimize Performance and Validate Gains at Low Cost

Consider Turbines as "Virtual Metmasts

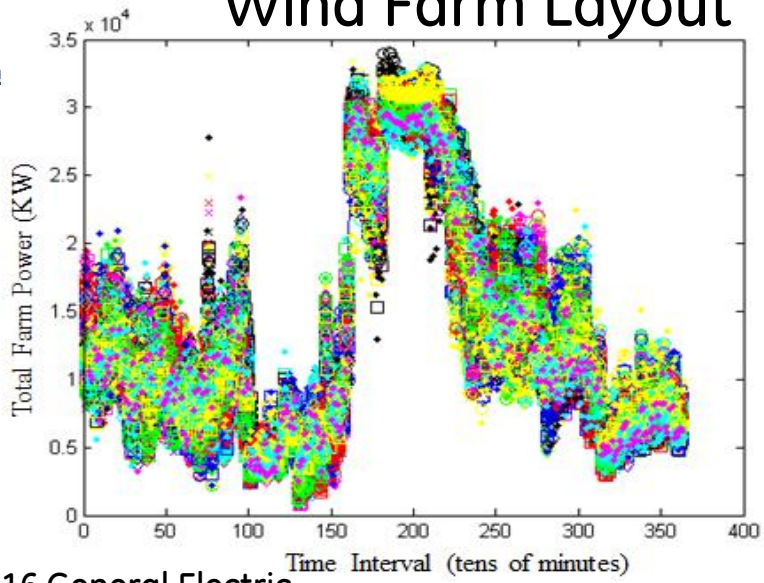
Use Machine Learning to Model Farm Power Given Reference Turbine Input

$$\hat{P}_{Farm} = c_0 + c_1 f_1 + c_2 f_2 + \ldots + c_n f_n$$

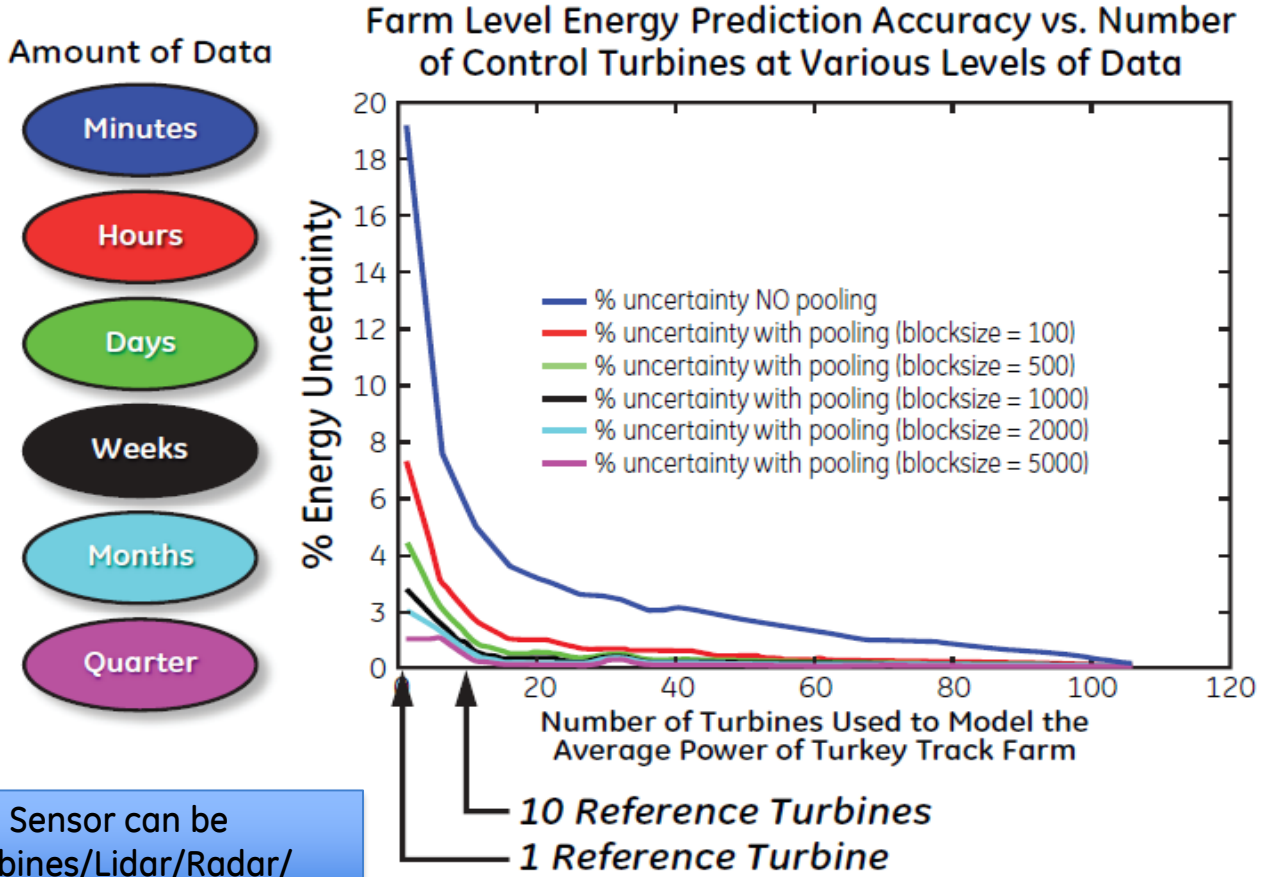


Wind Farm Layout

Prediction of Farm Power Output Given Reference



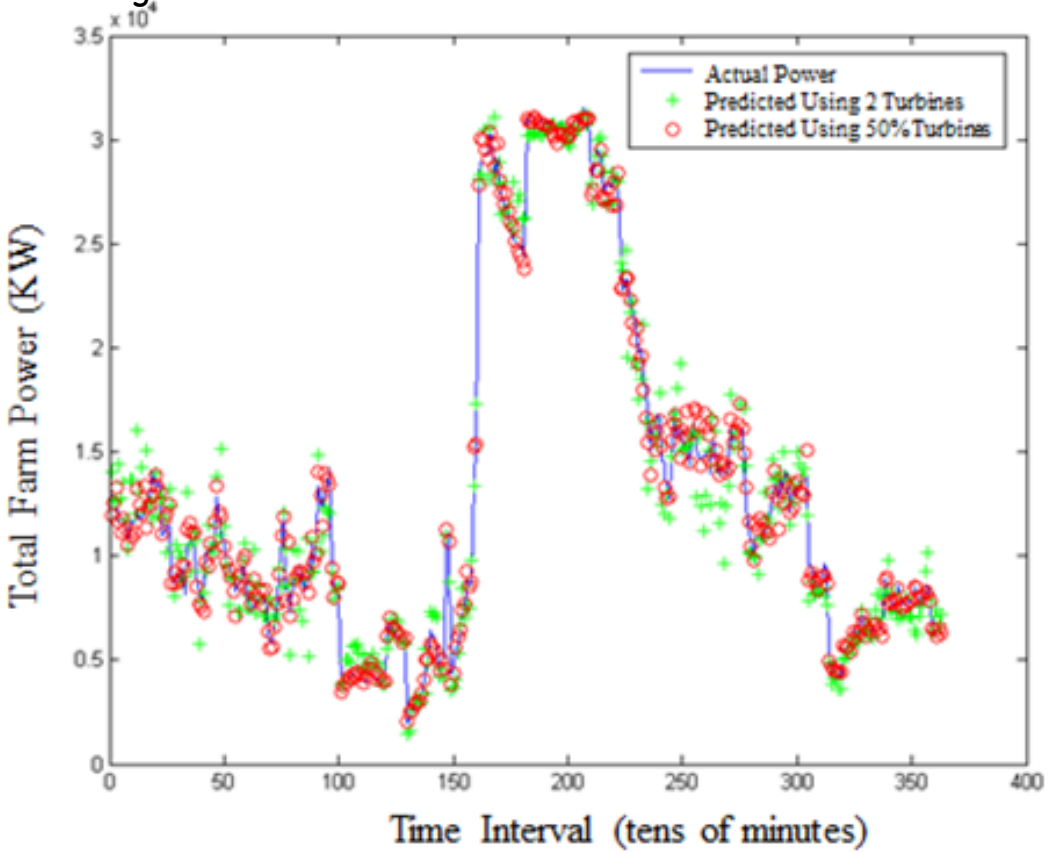
The Data Vs. Uncertainty Trade



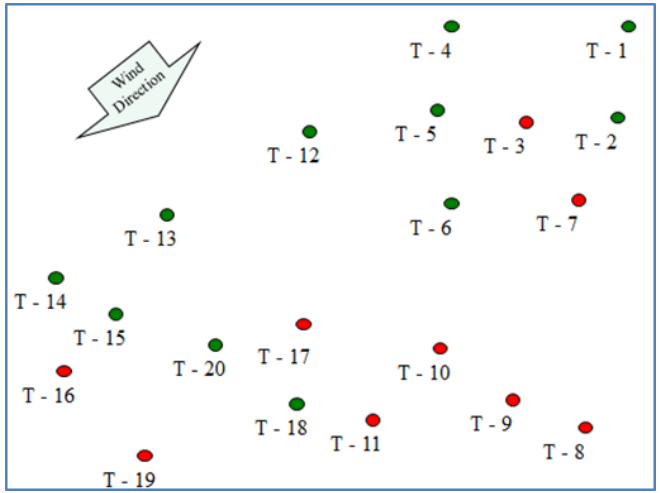
Sensor can be Turbines/Lidar/Radar/ Annemometer

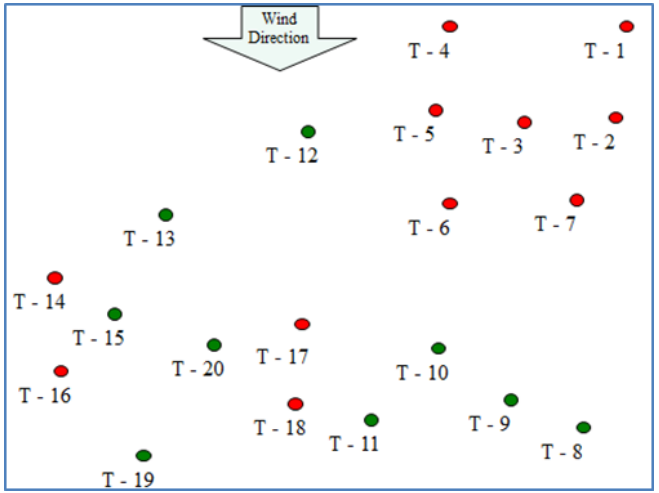
Many Options to Find Good Solutions

Stepwise Linear Regression on Turbine Power Features

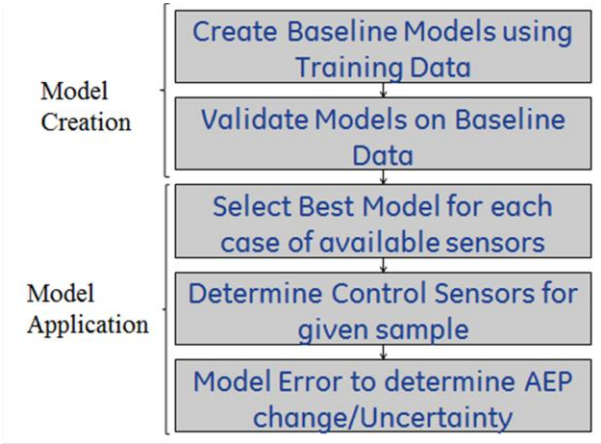


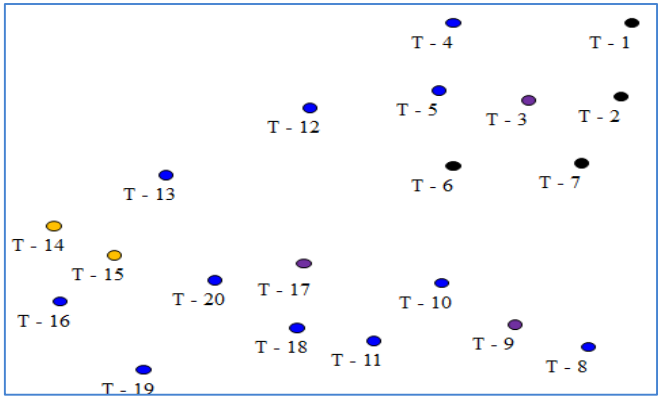
But Not All Virtual Metmasts (Turbines) are Honest Brokers!



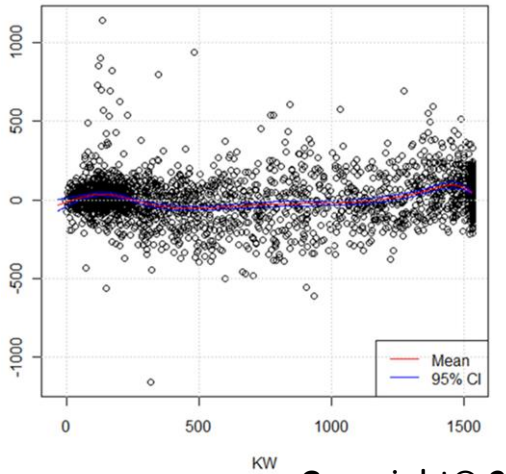


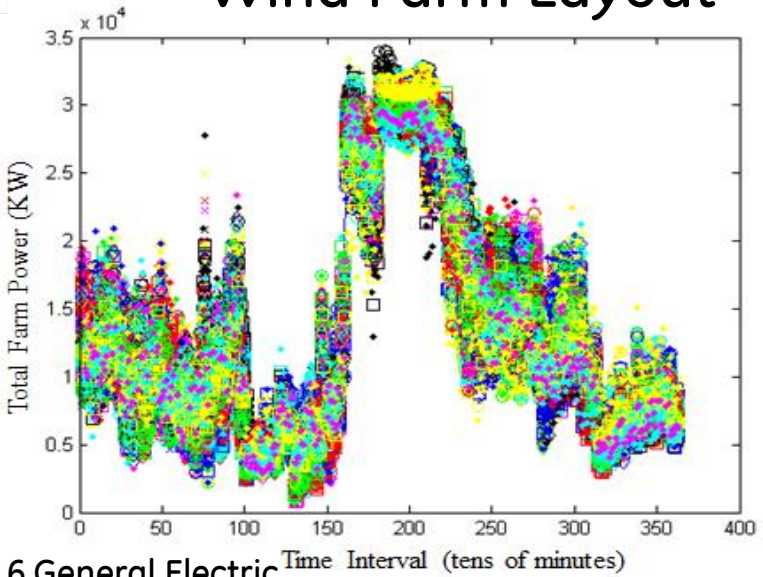
We define **Honest Brokers** to be control turbines or sensors that are considered to be valid and consistent in both the training and testing intervals





Wind Farm Layout





What about Cyber?

CONSIDERATIONS WHEN SHRINKING THE ATTACK SURFACE OF THE WIND FARM

William Noto

March 15, 2016

DEEP ROOTS IN SECURING CRITICAL ASSETS

Services → Products

Our Offerings	Build security in	Validate/certify for security	Operate processes securely
Our Customers	 Device manufacturers	 Integrators	 Operators, asset owners

2006 ----------→ 2016

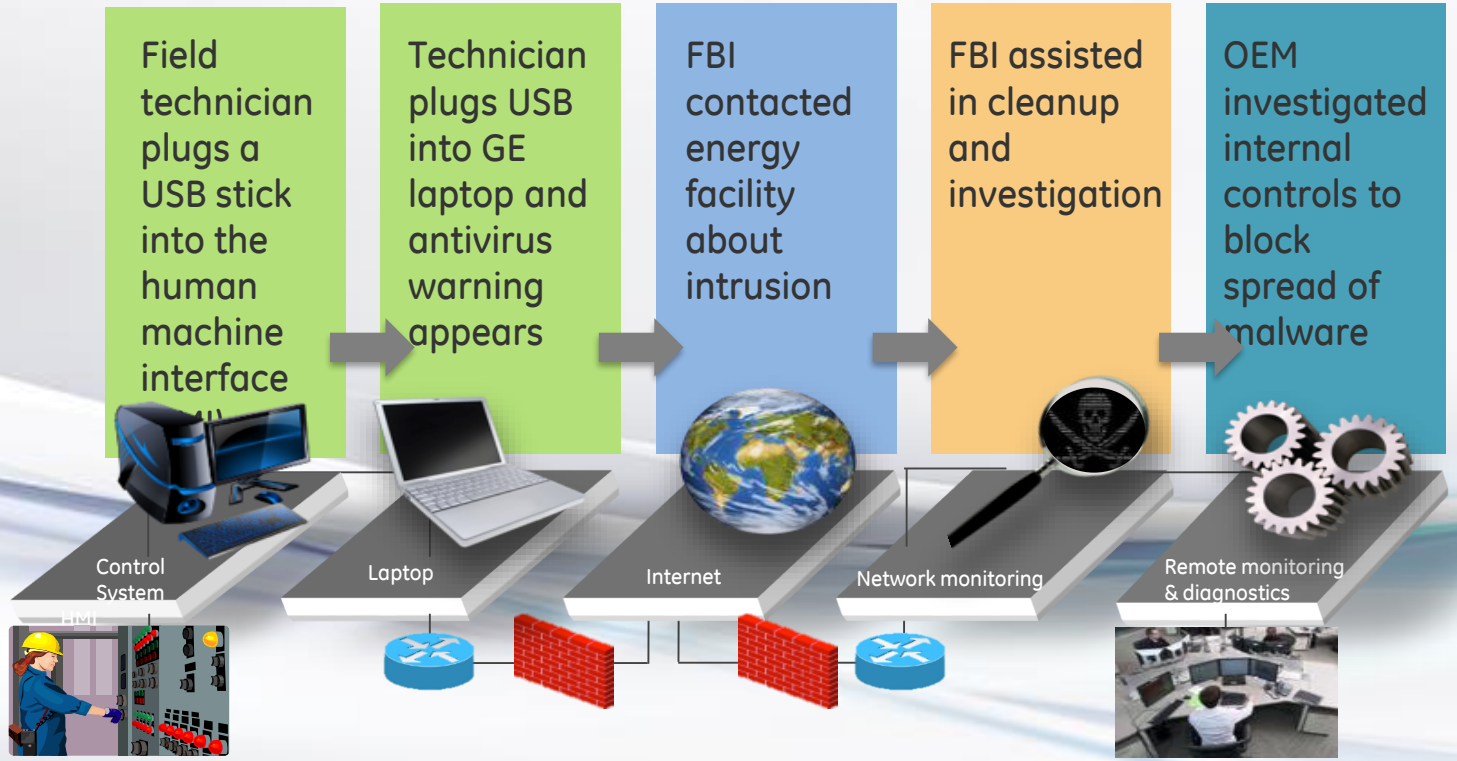
wurldtech
A GE Company

Threat overview

		How	Potential Impact
Hacktivism		Highly visible attacks targeting large corporations and government agencies	• Denial of service to customers • Public image
Advanced Persistent Threat (APT)		Organized and state funded groups methodically targeting the enterprise, country or customer	• Grid reliability • Intellectual property theft • Customer site compromise
Insider / Malicious Intent		Employee with legitimate access to PII/sensitive info publically releasing, selling or going to competitor	• Intellectual property theft • Business process damage
Cybercrime		Organized crime rings targeting individuals and corporations for financial gain	• Financial losses • Employee personal impact

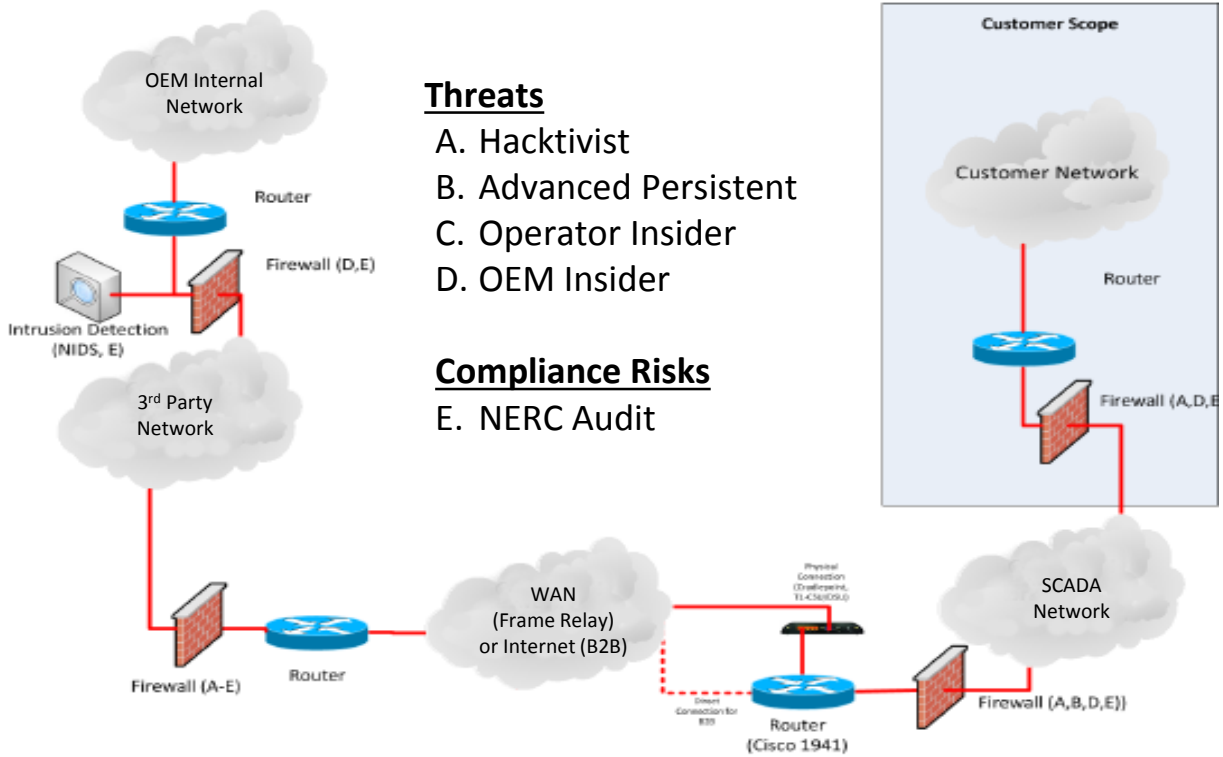
Targeted attacks against network and software vulnerabilities in the wind farm industrial control systems/SCADA increase risks to Operators and OEM's reputation

Example compromise – power plant site



wurldtech
A GE Company

Wide Area Network Attack Surface



Threats

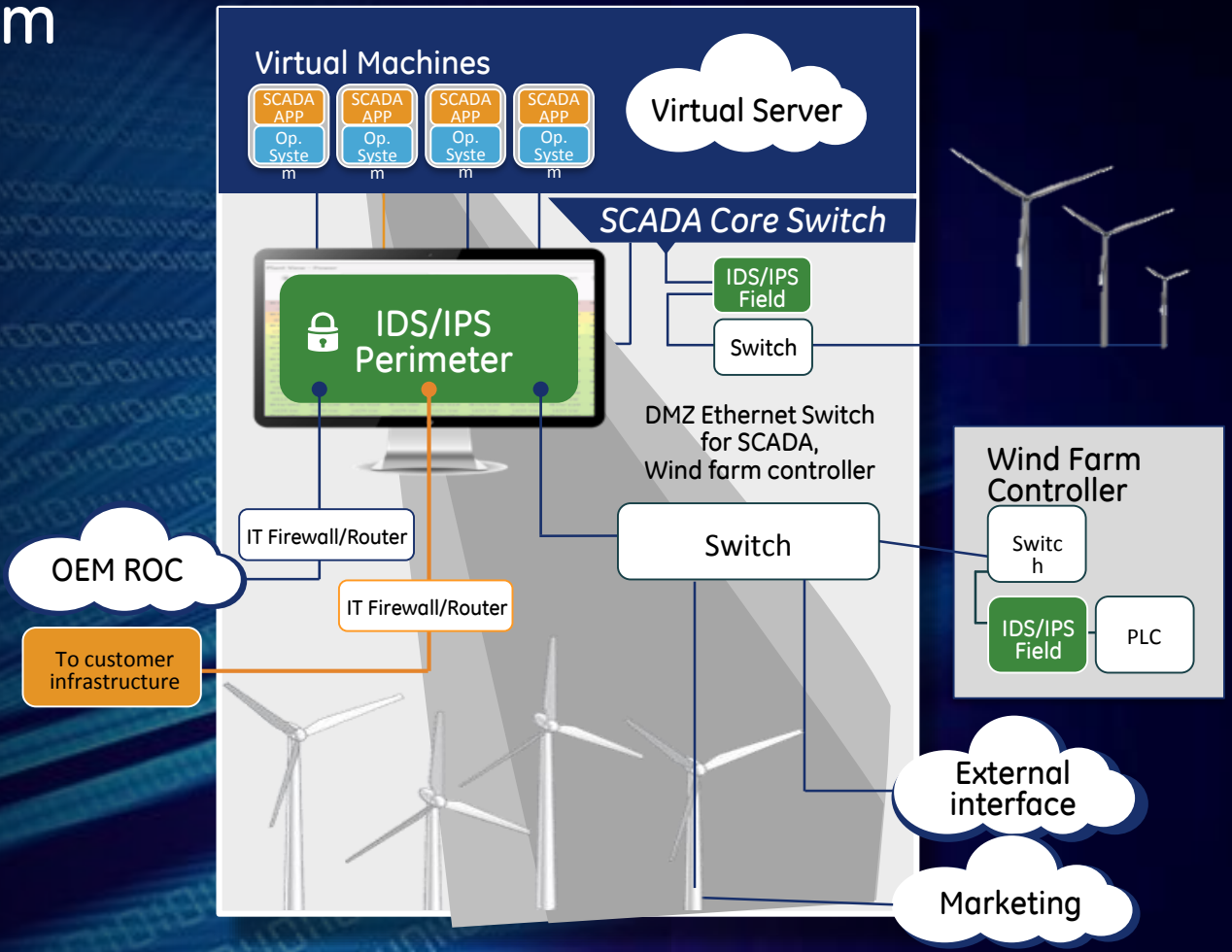
A. Hacktivist
B. Advanced Persistent
C. Operator Insider
D. OEM Insider

Compliance Risks

E. NERC Audit

wurldtech
A GE Company

Wind Farm Network Attack Surface



wurldtech
A GE Company

The SCADA system

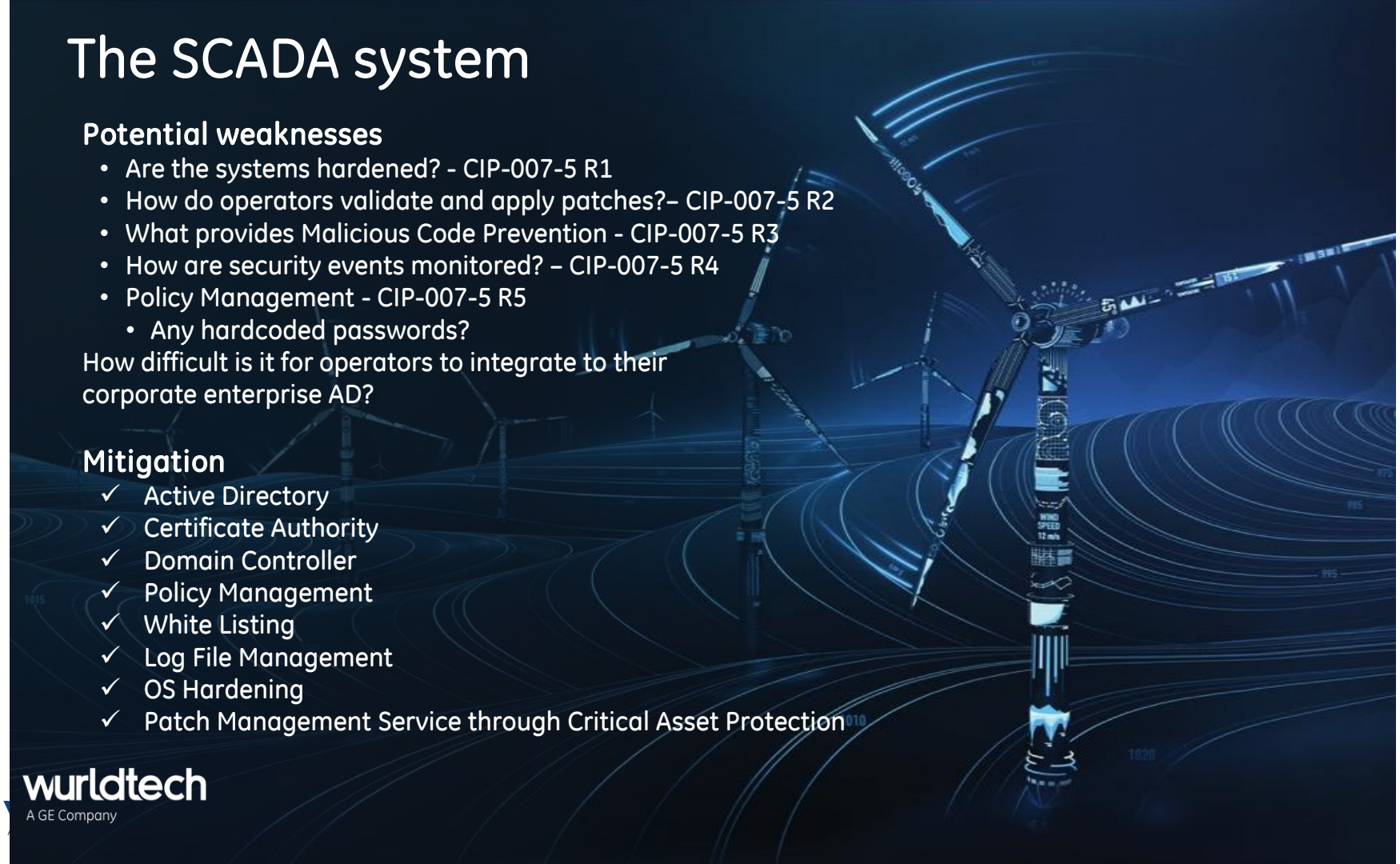
Potential weaknesses

- Are the systems hardened? - CIP-007-5 R1
- How do operators validate and apply patches?– CIP-007-5 R2
- What provides Malicious Code Prevention - CIP-007-5 R3
- How are security events monitored? – CIP-007-5 R4
- Policy Management - CIP-007-5 R5
  - Any hardcoded passwords?

How difficult is it for operators to integrate to their corporate enterprise AD?

Mitigation

- ✓ Active Directory
- ✓ Certificate Authority
- ✓ Domain Controller
- ✓ Policy Management
- ✓ White Listing
- ✓ Log File Management
- ✓ OS Hardening
- ✓ Patch Management Service through Critical Asset Protection



wurldtech
A GE Company

SCADA Network

Potential Weaknesses

- Any default passwords, any unmanaged policies - CIP-007-5 R5
- Any network access control (NAC)?, How many available open ports require authentication - CIP-003-5 R3
- Switch firmware patching - CIP-007-5 R3
- Any hardcoded passwords - CIP-007-5 R4
- Any ability to detect and prevent an intrusion?

Mitigation

- ✓ OpShield for OT NIDS/NIPS
- ✓ IT Security Services
  - Active Directory
  - Certificate Authority
  - Domain Controller
  - Radius
  - Configuration management for switches
- ✓ NAC through 802.1X & RADIUS – Packet Fence, e.g.
- ✓ MAC Based filtering for non 802.1X Supplicants

wurldtech
A GE Company

Control System – Wind Turbine Control

Potential Weaknesses

- Default simplistic passwords, and no managed policy - CIP-007-3 R5
- Open industrial protocols with no encryption, susceptible to Man-In-The Middle (MITM) attacks
- Is Firmware *signed* or *whitelisted*?

Mitigation

✓ Securing controllers may require:

- Active Directory
- Certificate Authority
- Domain Controller

✓ MAC Based filtering for non 802.1X Supplicants GE's configuration management

✓ Require technology suppliers to address firmware weaknesses
e.g., MITM, firmware signing, etc.

Wurldtech Professional Services

Site Security Services

✓**Site Security Assessment**

In-depth, comprehensive site evaluation

✓**Site Security Health Check**

Rapid facility overview

✓**NERC CIP CVA**

Comprehensive assessment for U.S. electric utilities

Device Security Services

✓**Device Security Assessment**

In-depth, comprehensive device evaluation

✓**Device Security Health Check**

Rapid, economical engagement

Professional Security Services

✓**Product Development Security Assessment**

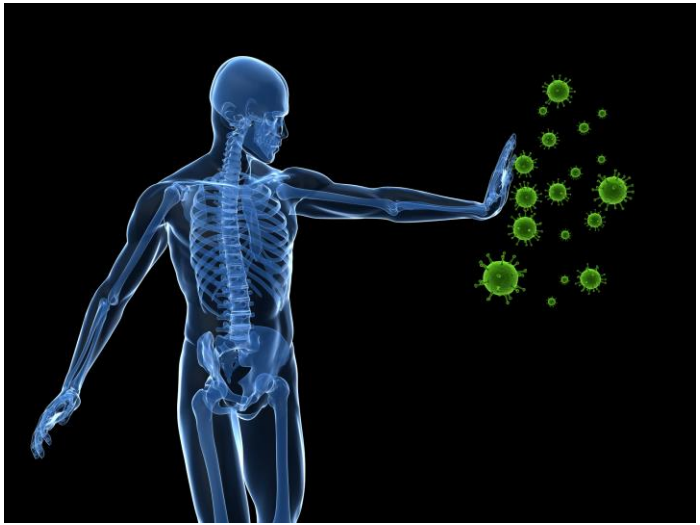
Comprehensive evaluation of security practices

✓**IEC 62443 GAP Assessment**

Comprehensive evaluation of meeting IEC requirements

Preparation for APC

DOE recently gave funding to a team of scientists at the GRC to develop and demonstrate a next-generation cybersecurity technology to help protect critical power-generation assets.



GE's project is one of 12 awards totaling $34 million of DOE investment.

"The general idea is to use our digital model of plant operations to detect anomalies that could indicate a cyber disruption or attack is underway," he said. "If one is detected, the control system we design in the plant using sensors and complex algorithms would automatically adjust its operation to reduce risk of harm to the asset and keep the system running."

More info at:
http://www.gereports.com/these-scientists-hacked-the-immune-system-to-fight-cyberattacks/

What do Security Prognostics look like?

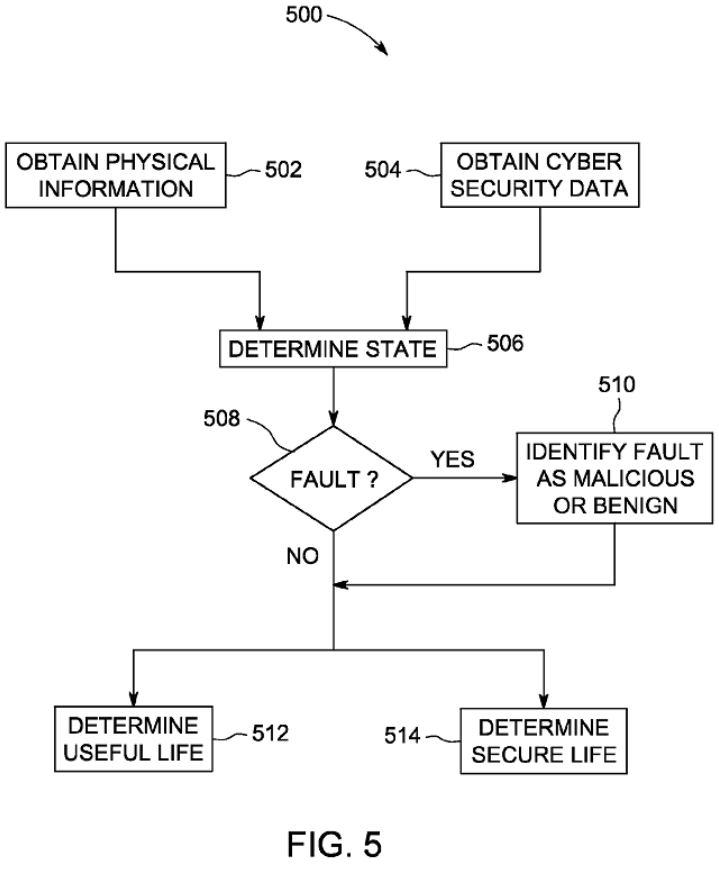


FIG. 5

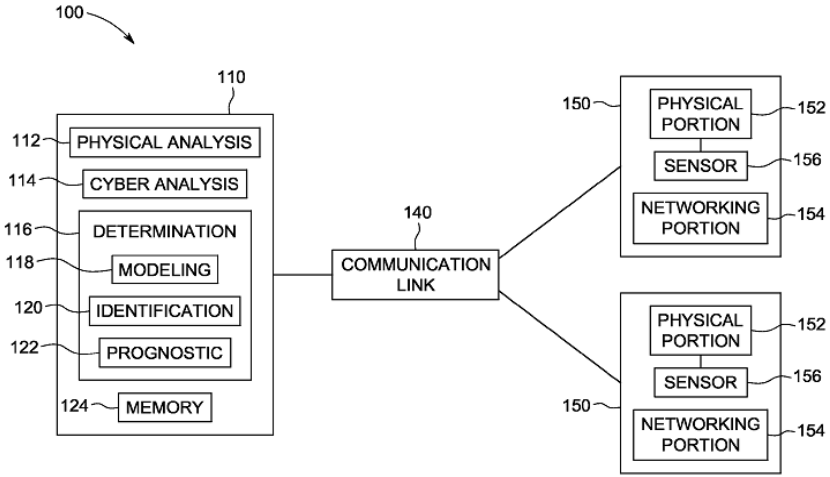


FIG. 1

Insider Threat: System and Method for Data Loss Prevention

US 20150020207A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2015/0020207 A1**

Kasiviswanathan et al. (43) **Pub. Date: Jan. 15, 2015**

(54) **SYSTEMS AND METHODS FOR DATA LOSS PREVENTION**

(71) Applicant: **General Electric Company**, Schenectady, NY (US)

(72) Inventors: **Shiva Prasad Kasiviswanathan**, San Ramon, CA (US); **Lei Wu**, San Ramon, CA (US); **Daniel Edward Marthaler**, Oakland, CA (US); **Scott Charles Evans**, Burnt Hills, NY (US); **Varian Paul Powles**, Niskayuna, NY (US); **Philip Paul Beauchamp**, Rexford, NY (US)

(21) Appl. No.: **13/942,318**

(22) Filed: **Jul. 15, 2013**

Publication Classification

(51) **Int. Cl.**
G06F 21/60 (2006.01)

(52) **U.S. Cl.**
CPC ***G06F 21/60*** (2013.01)
USPC **726/26**

(57) **ABSTRACT**

One method for developing a data loss prevention model includes receiving, at a processing device, an event record corresponding to an operation performed on a computing device. The event record includes an event type and event data. The method also includes transforming, using the processing device, the event type to an event number corresponding to the event type. The method includes transforming, using the processing device, the event data to a numerical representation of the event data. The method includes associating an indication of whether the event type and the event data correspond to a data loss event with the event number and the numerical representation. The method also includes determining the data loss prevention model using the indication, the event number, and the numerical representation.

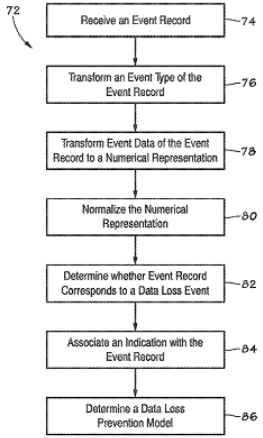
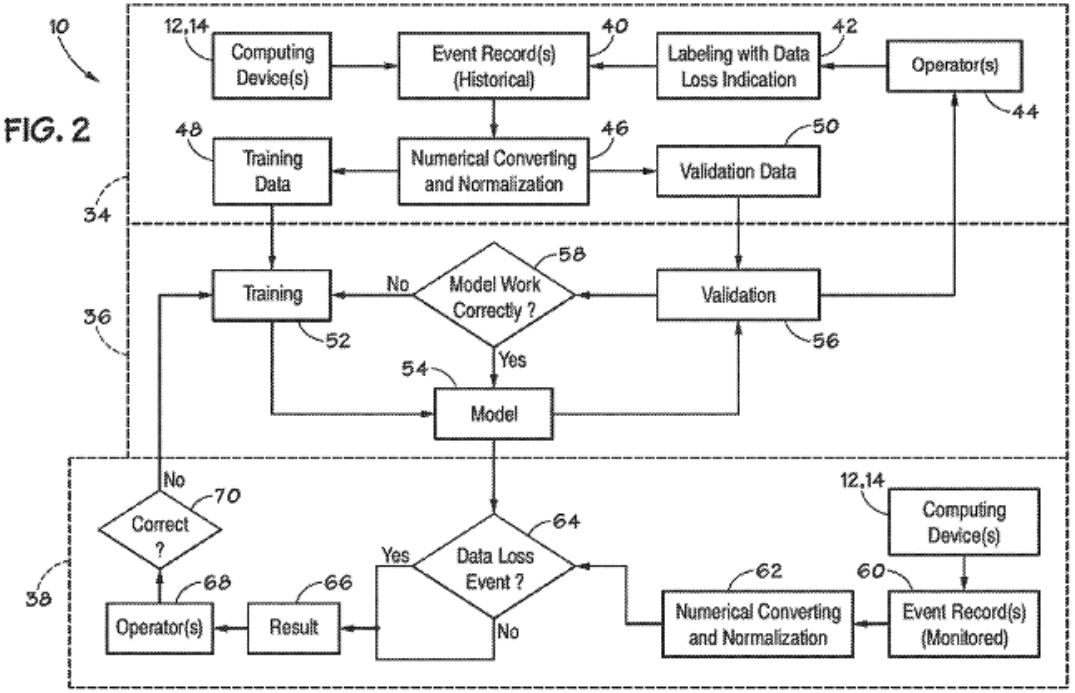


FIG. 2



We make & connect various Digital Twin pieces

Inspection data, e.g., Borescope

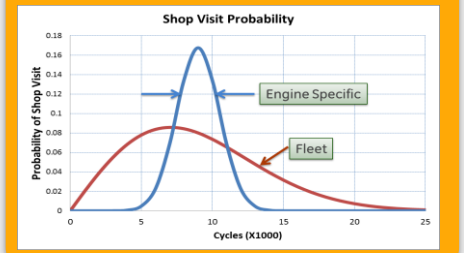
Operational State data, e.g., Temp etc.

Asset Life data, e.g., cycles to failure

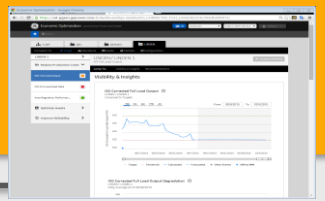
Data Lake and Predix Cloud

Performance Models

Life Models

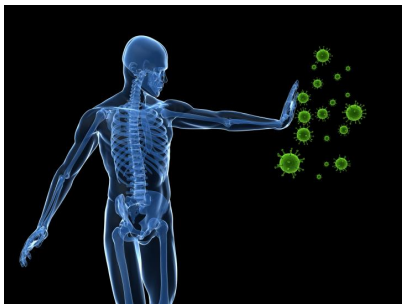


Asset Performance Management
Operations Optimization
Business Optimization



Online Sensor data

Field and Service Data and Actions



Secure Life

#IndustrialInternet

powered by GE

Conclusions

- We have put forth the position that Cyber-Security of critical infrastructure and tactical systems will require convergence of PHM Systems, Information security, and advanced diagnostics technologies into Security Prognostics – where security is right in the middle of monitoring and diagnostics – not bolted on afterward.
- Under this paradigm the best and latest tools for detecting and tracking non-malicious faults and failures can be developed further and brought to bear to the problem of cyber-security: detecting security breach and estimating remaining secure life.
- This paradigm lends itself further to creation of adaptive and resilient systems that are self-healing and situationally aware. These paradigms go against the current trend in cyber-security for security systems that are separate from M&D, but we feel the difficulty of protecting tactical systems and critical infrastructure require a re-thinking of this trend towards a unified approach, which will be the focus of our future work.

What's Next

- How Can we leverage all of PHM for Security?
- What Technologies Transfer?
- What Technologies need to be developed?
- Let's Collaborate!