



ASHE Lunch and Learn Asset Connectivity and Cybersecurity

October 2, 2018

Eric Ditman

Sr. Digital Program Manager

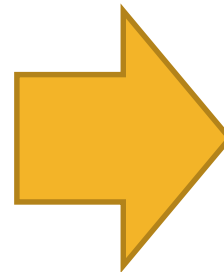
Caterpillar

Agenda

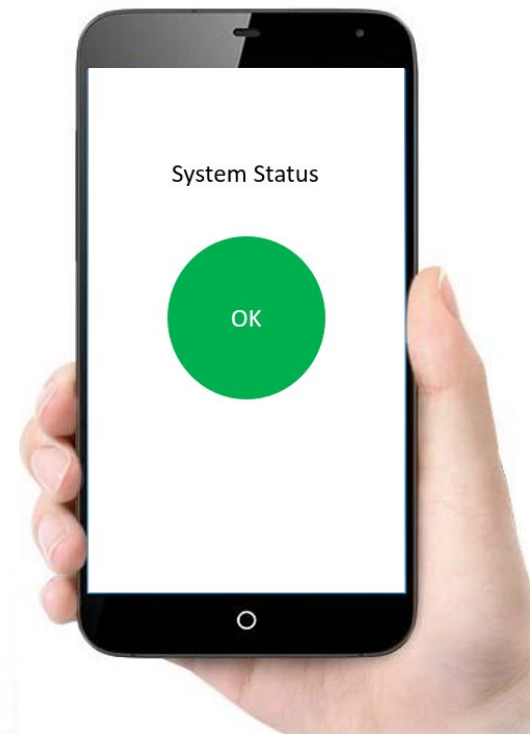
- + Connectivity
- + Cybersecurity

Know the Customer

PROBLEM



SOLUTION



Customer Value

Peace of mind

- + Ready to Start
- + Job security / Risk Management



Simplicity

- + Trusted partners
- + Value added support / tools

System availability / reliability

- + Max. uptime / min. downtime
- + System efficiency

Reputation

- + Data security
- + Brand recognition
- + Safety / Compliance



Profitability

- + Cost control

Productivity

- + Maximum uptime
- + Minimum downtime
- + Asset utilization
- + Value added support / tools



Return on Investment

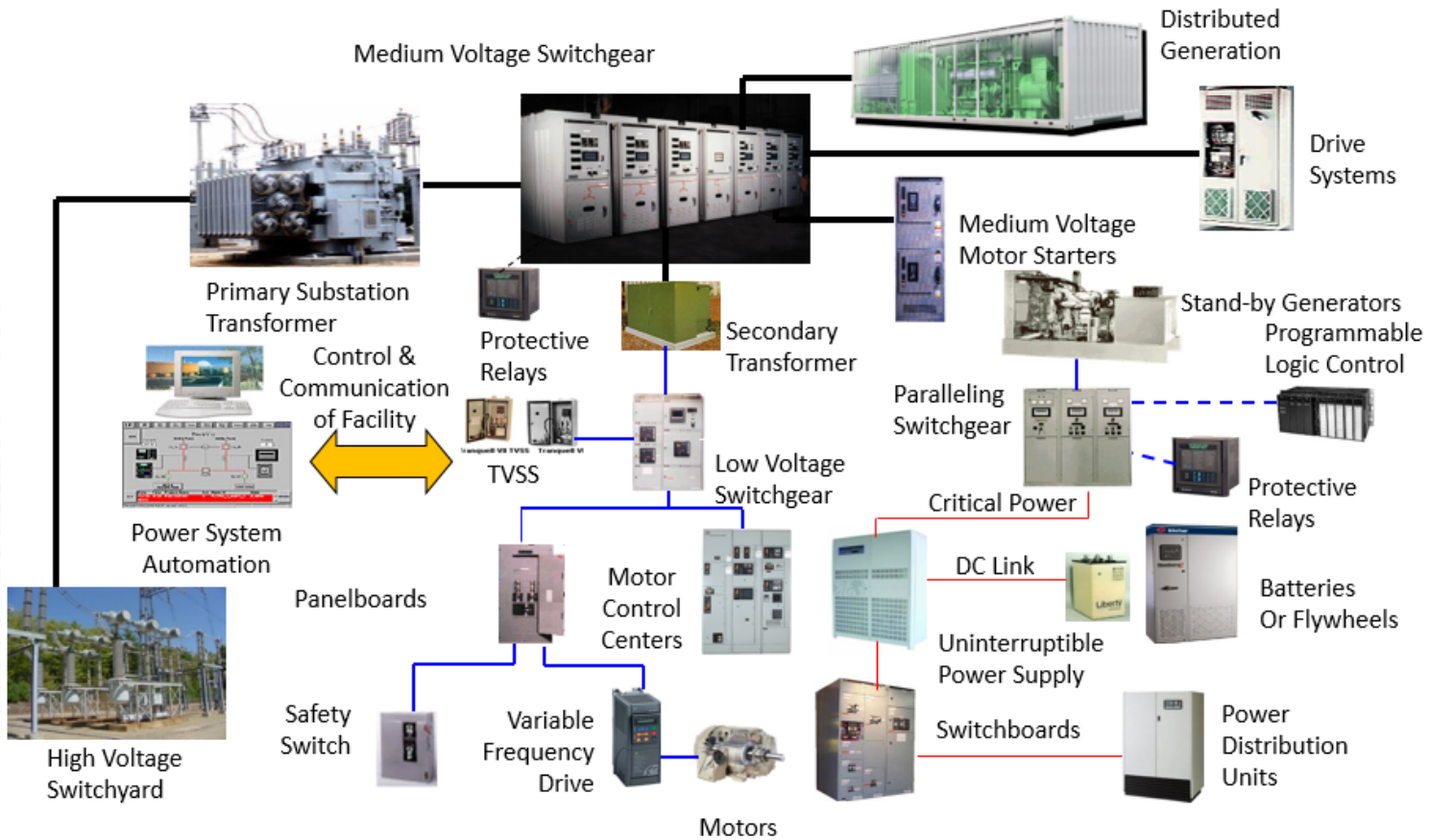
- + Cost Control
- + Fuel management
- + Reliability / durability

Risk Management

- + Trusted partners
- + Job security
- + Safety / Compliance
- + Theft prevention



Data Overload



Transform Data into Value

Connectivity Value

Identify Issues Before Failure

- + Automated analysis
- + Data science
- + Human analysis
- + Deep domain experts

Operational Performance

- + Asset Readiness/Status
- + Operating Cost
- + Efficiency
- + Regulatory Requirements
 - + Industry Specific
 - + Emissions/Environmental Impact

Preventive Maintenance

- + Understand the current condition of the equipment
- + Schedule and Prepare
 - + Optimize the work the plan
 - + Ensure resource and material availability
 - + Optimal time for the customer
- + Spot and fix small problems before they become major problems
- + Extend component Life

Respond Appropriately

- + Quickly determine the problem
- + Dispatch resources

Technology and Services create Value



TECHNOLOGY

- Data Collection Methods
- Data Transmission Options
- Data Storage

SERVICES

- Data Visibility/Usability
- Product Expertise
- Data Aggregation
- Security
- Analysis
- Recommendations
- Customized Information
- Support/Service
- Asset Management
- Risk Sharing
- Stability

VALUE ADDER

Real Time Information



- Visualize anywhere and anytime
 - Web Application
 - Mobile Application
- Operating status
- Availability
- Performance indicators
- Location
- **Example: Customer monitors the fuel level at multiple locations to determine refill priority**

Notifications

- Provided via Email or Text
- Alarms on the asset
- Location change
- Specific parameters
- Asset Availability
- Asset Operating Status
- Customizable by each user
- **Example: Customer able to relocate their staff from generator room to other critical location**



Reporting

- Asset Level
- Application Overview
- Industry Specific
- Insurance
- Regulatory
- Customizable
- Example: Customer saved \$20K by replacing emissions inspection with operating history report



Industrial Control Systems (ICS) Under Attack

Notable Breaches: Power Industry

- Davis-Besse nuclear power plant (Ohio – USA) - 2003
- Brown Ferry nuclear power plant (Alabama-USA) – 2006
- Stuxnet: Destruction of Iranian Nuclear Centrifuges (2011)
- Aurora Generator Destruction (2010)
- Ukraine power outage – 2015

➤ Attacks are increasing in number as well as sophistication
➤ Companies in the Energy and Transportation sector are now clearly targeted

The Washington Post

National Security

Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say



Cyberattacks Surge on Energy Companies, Electric Grid

Companies and utilities reported a raft of 'successful' attacks – and worry worse is yet to come.

By Alan Neuhauser, Staff Writer | April 8, 2016, at 4:00 p.m.

POLITICO

Vermont utility confirms system breach by Russians







By CRISTIANO LIMA and ERIC GELLER | 12/30/2016 08:45 PM EST

WIRED

ANDY GREENBERG SECURITY 07-06-17 11:38 PM

HACK BRIEF: HACKERS TARGETED A US NUCLEAR PLANT (BUT DON'T PANIC YET)

Cybersecurity Regulations/Standards

Industry	Regulation/Standard
General Industrial Control Systems	ISA/IEC 62443 (formerly ISA-99)  
	IEC 62351 Part 1-8 
	ISO 27000/27001 
Data Centers	NIST Frameworks (800-53, 800-82) and ISO 27000 series
Electric Power and Utilities	NERC-CIP (002 to 009)
Federal	Risk Management Framework (RMF), DIACAP, NIST Framework 
Health Care	Health Insurance Portability and Accountability Act (HIPAA)
	Health Information Technology Security and Privacy Rule (HITSP) 2009
Chemical	U.S. DHS CFATS
Marine	International Association of Classification Societies (IACS) 

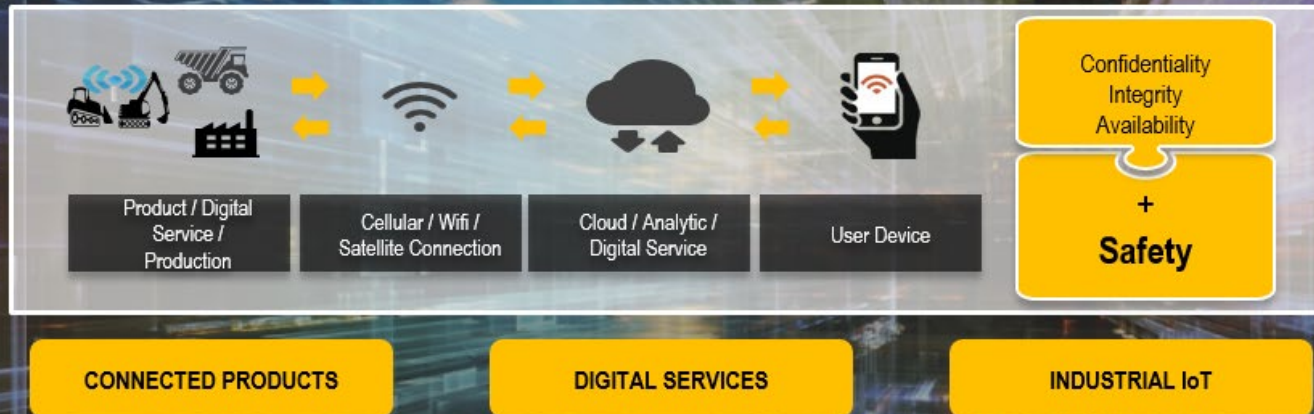
Increasing number of security and data privacy regulations and standards

- Holistic Security Program that includes – Organization, Policies, and Technology
- Defense-in-Depth: Layers of Security Controls Across the System
- Network Segmentation

Connected Asset Security

Connected Asset Security Program

A collaborative business effort managing cybersecurity risks to Caterpillar's ecosystem of connected solutions.



We provide cybersecurity governance and leadership to help Caterpillar's businesses embed secure methods into the creation and support of connected products, digital services and connected production devices.

Managing the Cybersecurity Risk of Connected Assets

Our Connected Asset Journey... the CAPABILITIES

GOVERN

- Manage cybersecurity risks
- Inventory connected solutions
- Sustain business outcomes
- Provide cybersecurity guidance

PROTECT

- Protect connected asset (CA) data
- Embed secure methods in creating CAs
- Embed secure methods in supporting CAs

DETECT

- Collaborate with customers, partners and researchers
- Log and monitor security events

RESPOND

- Respond to cybersecurity incidents

EDUCATE

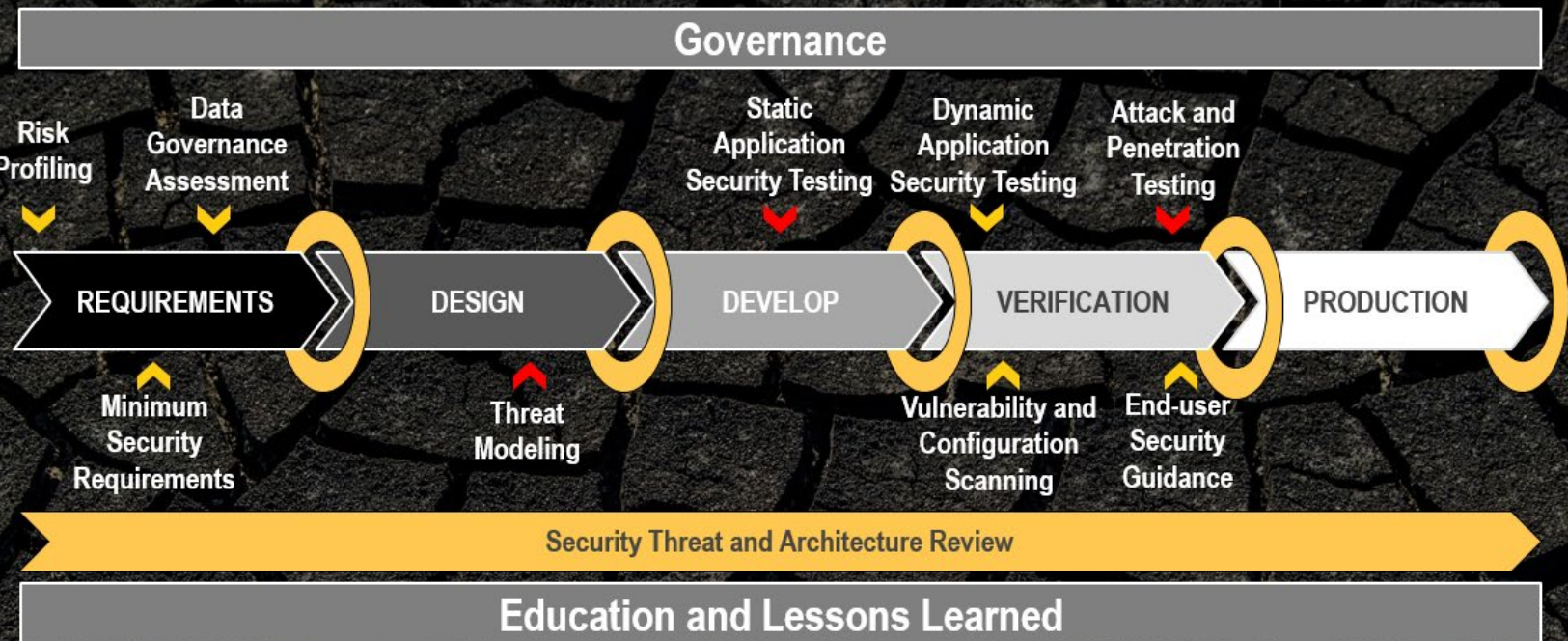
- Expand security awareness



Information Security Operating Framework

Integrating Security into Development Lifecycles

Integrating Security into Development Lifecycles



Activity scaled based on risk Activity required for all products

Defense-in-Depth - People, Policies and Technical Controls

+ Physical –

- + *Physical Access Controls for Critical Areas*

+ Network –

- + *Firewalls and Traffic Filtering*
- + *Intrusion detection and prevention*

+ Computer Hardening –

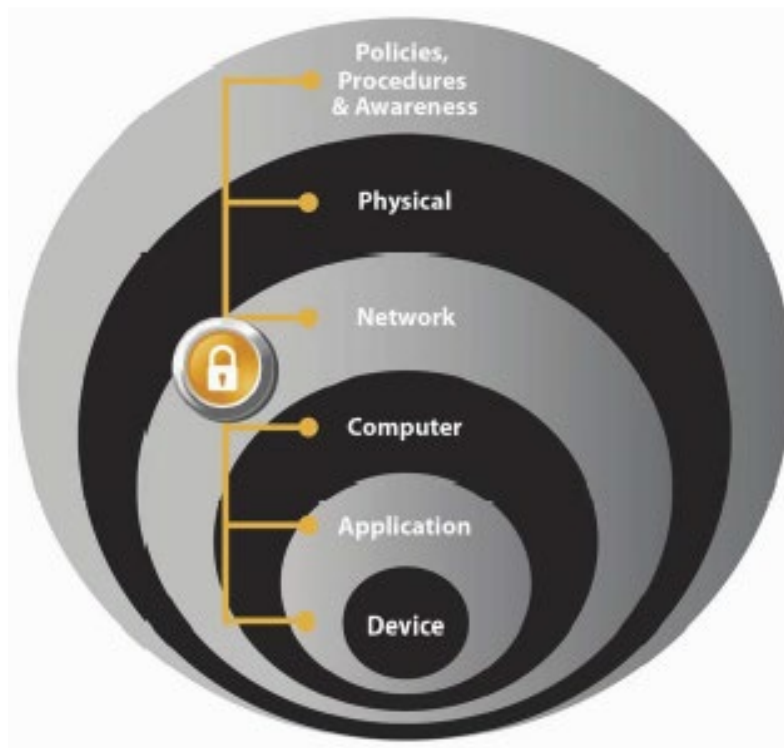
- + *Patching and Anti-Virus*
- + *Remove unused applications/ protocols/services*
- + *Close unnecessary logical and physical ports*

+ Application –

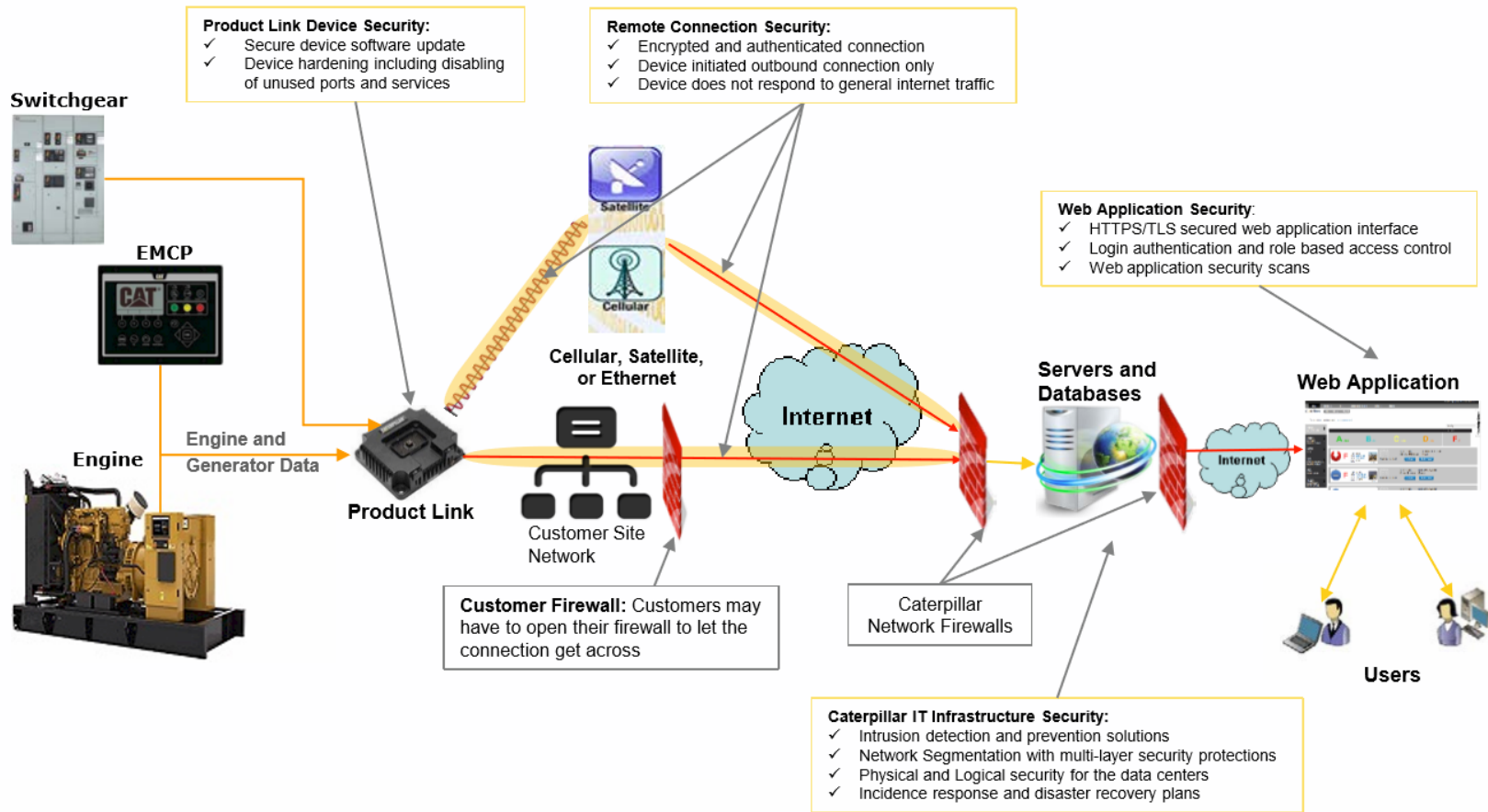
- + *Authentication, Authorization, and Accounting*

+ Device Hardening –

- + *Encryption*



End to End Security Architecture



System Considerations

+ **Products and Services**

- + Does it meet all the connection needs?
- + Transform Data into Value
- + Flexible
- + Expandable

+ **Support**

- + 24/7
- + Regional or World-Wide
- + Expertise level

+ **Commercial Plan/Cost**

- + Initial
- + Ongoing

+ **Company**

- + Expertise
- + Reliability
- + Security
- + History
- + Sustainability







THANK YOU

Eric Ditman
Sr. Digital Program Manager
Ditman_Eric_J@Cat.com
309-698-5275