



OSIsoft Super Regional 2018

**Fairmont Washington D.C. - Georgetown
August 20-22, 2018**



Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

Michael Powell, Cybersecurity Engineer, NCCoE, NIST
Timothy A. Zimmerman, Computer Engineer, EL, NIST



Defined



Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs



Foundations

Collaborative Hub

The NCCoE assembles experts from businesses, academia, and other government agencies to work on critical national problems in cybersecurity. This collaboration is essential to exploring the widest range of concepts.

As a part of the NIST cybersecurity portfolio, the NCCoE has access to a wealth of prodigious expertise, resources, relationships, and experience.

NIST
**National Institute of
Standards and Technology**
U.S. Department of Commerce



NIST Information Technology Laboratory

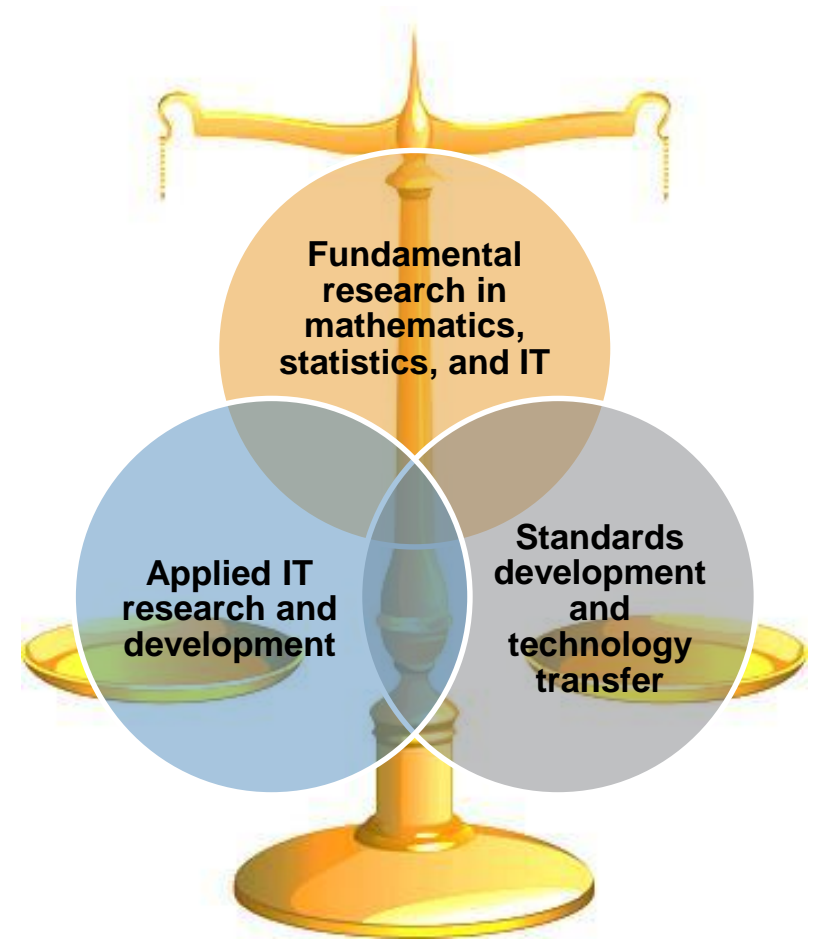
Cultivating Trust in IT and Metrology through measurements, standards and tests

ITL Programs

- Advanced Networking
- Applied and Computational Mathematics
- Cybersecurity
- Information Access
- Software and Systems
- Statistics

Collaborations with

- Industry
- Federal/State/Local Governments
- Academia



NIST Applied Cybersecurity Division (ACD)

- Implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities



Engagement & Business Model

DEFINE



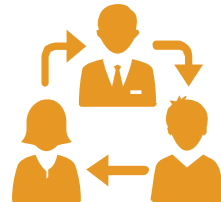
ASSEMBLE



BUILD



ADVOCATE



OUTCOME:

Define a scope of work with industry to solve a pressing cybersecurity challenge

OUTCOME:

Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

OUTCOME:

Build a practical, usable, repeatable implementation to address the cybersecurity challenge

OUTCOME:

Advocate adoption of the example implementation using the practice guide



Body of Work

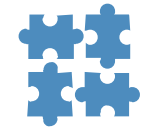


NCCoE Tenets



Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards



Modular

Develop components that can be easily substituted with alternates that offer equivalent input-output specifications



Repeatable

Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results



Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry



Usable

Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations



Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

SP 1800 Series: Cybersecurity Practice Guides

- **Volume A: Executive Summary**
 - High-level overview of the project, including summaries of the challenge, solution, and benefits
- **Volume B: Approach, Architecture, and Security Characteristics**
 - Deep dive into challenge and solution, including approach, architecture, and security mapping to the Cybersecurity Framework and other relevant standards
- **Volume C: How-To Guide**
 - Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

CSF Function	CSF Subcategory	SP800-53R4 ^a	IEC/ISO 27001 ^b	CIS CSC ^c	NERC-CIP v5 ^d
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4			
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6

Sector-Based Projects



- **Commerce/Retail**
- **Energy**
- **Financial Services**
- **Healthcare**
- **Hospitality**
- **Manufacturing**
- **Public Safety/First Responder**
- **Transportation**

NISTIR 8219 Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

- The scope of this NIST Interagency Report (NISTIR) is a single cybersecurity capability:
 - The NCCoE deployed commercially available behavioral anomaly detection tools in two distinct but related manufacturing demo environments:
 - collaborative robotics system, and
 - simulated chemical process system.
 - The security characteristics of BAD was mapped to the Cybersecurity Framework. The mapping points manufacturers to specific security controls found in prominent cybersecurity standards.

CRADA members



Mapping of Cybersecurity Framework

Function	Category	Subcategory	Manufacturing Profile	Reference
DETECT	DE.AE	DE.AE-1	Low, Moderate and High	62443-2-1:2009 4.4.3.3
			Ensure that a baseline of network operations and expected data flows for the manufacturing system is developed, documented, and maintained to detect events.	CM-2
		DE.AE-2	Low	62443-2-1:2009 4.3.4.5.6, 62443-3-3:2013 SR 2.8, 2.9
			Review and analyze detected events within the manufacturing system to understand attack targets and methods.	AU-6 , IR-4
		DE.AE-2	Moderate and High	
			Employ automated mechanisms where feasible to review and analyze detected events within the manufacturing system.	AU-6(1) IR-4(1)
		DE.AE-3	Low and Moderate	62443-3-3:2013 SR 6.1
			Ensure that event data is compiled and correlated across the manufacturing system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	IR-5
		DE.AE-3	High	
			Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; manufacturing system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.	AU-6(5)(6) AU-12(1)
		DE.AE-4	Low	
			Determine negative impacts to manufacturing operations, assets, and individuals resulting from detected events, and correlate with risk assessment outcomes.	RA-3
Moderate				
DE.AE-4	Employ automated mechanisms to support impact analysis.	IR-4(1) , SI-4(2)		
	High			
DE.AE-4	Correlate detected event information and responses to achieve perspective on event impact across the organization.	IR-4(4)		

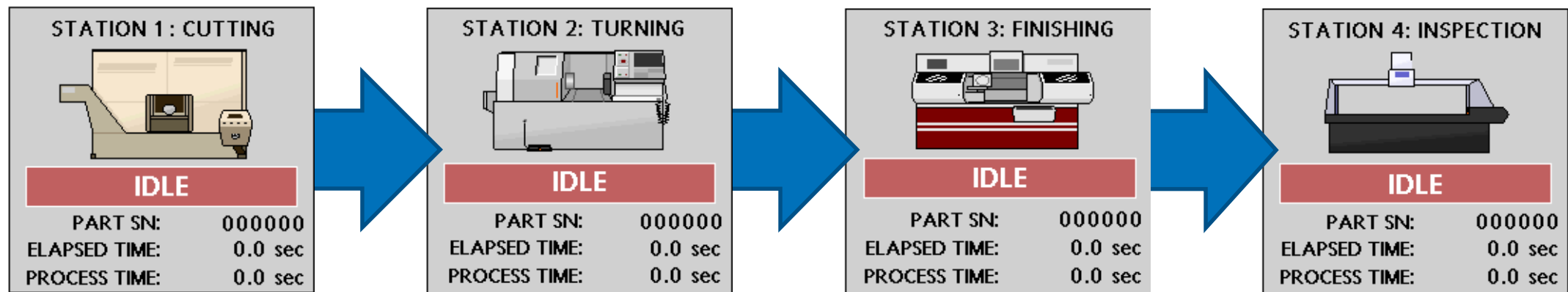
Behavioral Anomalies

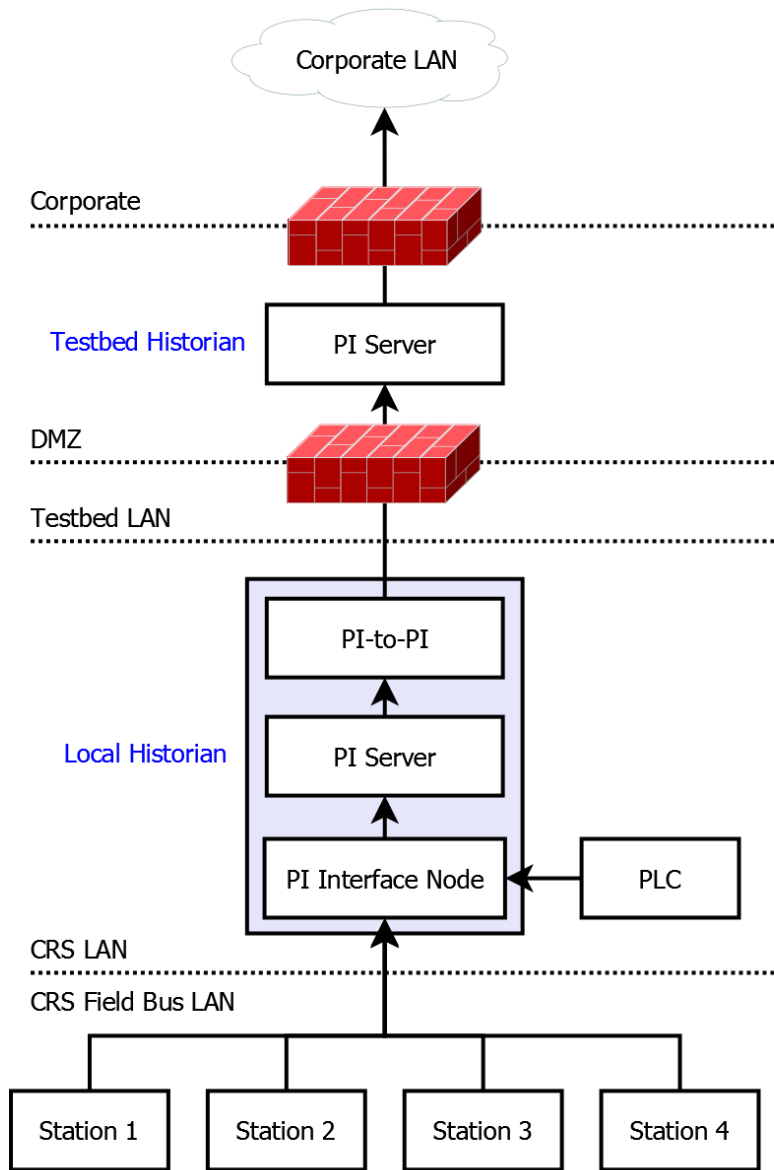
- Abnormal equipment operations
 - High trouble call frequency
- Sensor disruptions
 - Door sensor failure
- Communication disruptions
 - Robot coordination failure
- Environmental changes
 - High workcell temperature
- Data corruption
 - Invalid process variable values

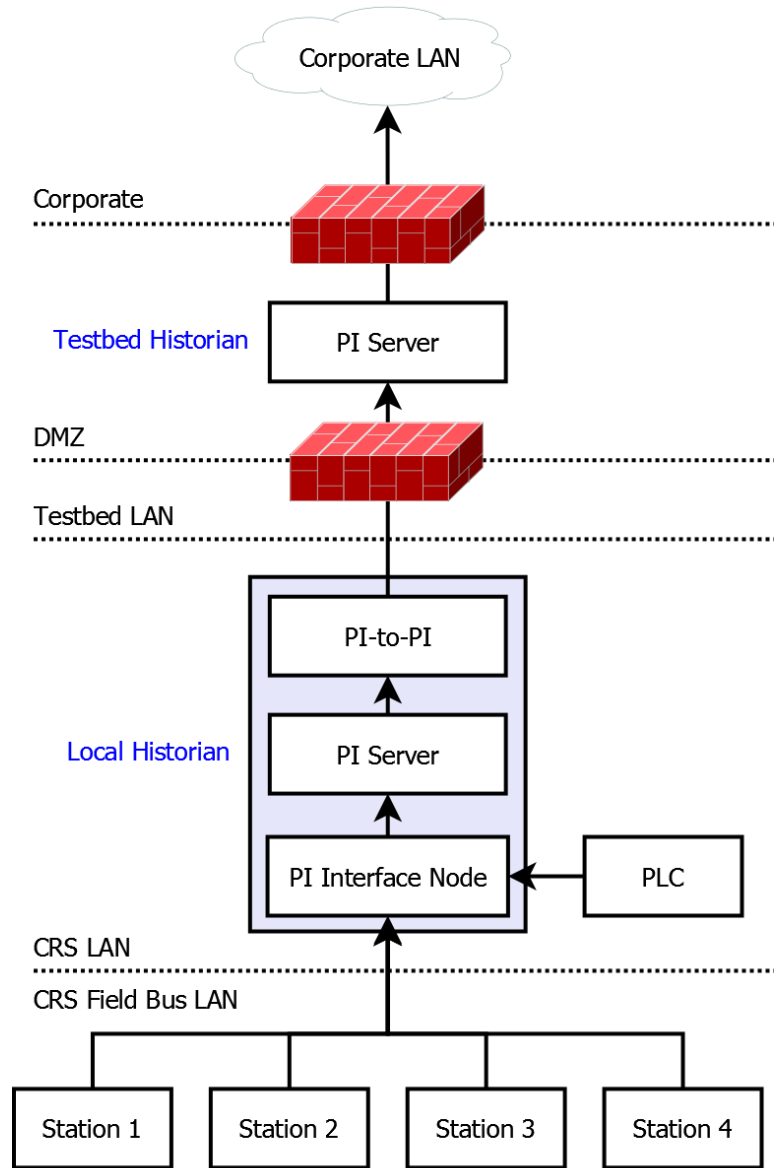
PI Implementation on the CSMS Testbed



- Discrete process
- Four machining stations
- Two machine-tending robots
- Supervisory PLC
- Modbus TCP







Components:

- PI Data Archive
- PI Asset Framework
- PI Process Explorer
- PI Modbus Ethernet Interface
- PI Vision
- SQL Server 2012

\\PI-ROBOTICS\TestbedDatabase 2 - PI System Explorer (Administrator)

File Search View Go Tools Help

Database Query Date Back Check In Refresh New Element New Attribute Search Elements

Elements

- Elements
 - Workcell 1
 - PLC
 - Station 1
 - Station 2
 - Station 3
 - Station 4
 - Element Searches

Station 1

General Child Elements Attributes Ports Analyses Notification Rules Version

Group by: Category Template

Filter

Name	Value	Description
Category: Analysis		
Category: Derived		
RawMode	0	Raw mode value of the statio...
RawState	4	Raw state value of the statio...
Category: Process Data		
Chuck State	OPEN	Current state of the chuck (o...
Door State	OPEN	Current state of the door (op...
Job Time Milliseconds	5 s	Time required to perform the ...
Mode	STOP	Mode of the machine (stop/run)
Part Counter	102 count	Quantity of parts produced b...
Part SN	0	Serial number of the current p...
Progress	0 %	Percentage of job completed
RobotProximity	0	Rate of proximity events
State	STOPPED	Current state of the machine
Stock Present	False	Does the machine have a part
Category: Static Data		

Station 1 Modified:5/24/2018 6:03:33 PM Owner:LAN\piadmin Version: 1/1/1970 12:00:00 AM, Revision 8

\\PI-ROBOTICS\TestbedDatabase 2 - PI System Explorer (Administrator)

File View Go Tools Help

Database Query Date Back Check In Refresh New Template Search Element Templates

Library

- TestbedDatabase 2
 - Templates
 - Element Templates
 - Machining_Station
 - PLCTemplate
 - Event Frame Templates
 - Model Templates
 - Transfer Templates
 - Enumeration Sets
 - Reference Types
 - Tables
 - Table Connections
 - Categories
 - Analysis Categories
 - Attribute Categories
 - Element Categories
 - Notification Rule Categories
 - Reference Type Categories
 - Table Categories

- Elements
- Event Frames
- Library
- Unit of Measure
- Contacts
- Management

PLCTemplate

General Attribute Templates Ports Analysis Templates Notification Rule Templates

Name: Alarm-StationOutOfSync
 Description: R24.2
 Categories:
 Analysis Type: Expression Rollup Event Frame Generation SQC
 Enable analyses when created from template

Example Element: [Workcell 1\PLC](#)

[Add a new variable](#) Evaluate

Name	Expression	Output Attribute
S1State	'.\Elements[@Name=Station 1] State'	Map
S2State	'.\Elements[@Name=Station 2] State'	Map
S3State	'.\Elements[@Name=Station 3] State'	Map
S4State	'.\Elements[@Name=Station 4] State'	Map
WCState	If(TimeEq('WorkcellState', '*-5s', '*'), "RUN") >= 5) Then "RUN" Else "Starting"	Map
StationModes	if (S1State = "STOPPED" Or S2State = "STOPPED" OR S3State = "STOPPED" Or S4State = "STOPPED")	Map

Scheduling: Event-Triggered Periodic Advanced...
 Trigger on: Any Input

PLCTemplate Modified:5/29/2018 2:30:38 PM Owner:LAN\piadmin

\\PI-ROBOTICS\TestbedDatabase 2 - PI System Explorer (Administrator)

File Search View Go Tools Help

Database Query Date Back Check In Refresh New Event Frame Search Event Frames

Event Frame Search 1

Group by: Category Template

Filter

Name	Duration	Start Time	End Time	Description	Category	Severity
ALARM-Station 1.RobotProximityFault.2...	0:01:03.006	5/30/2018 6:26:00 PM	5/30/2018 6:27:03.006 PM	(R25.1)		None
ALARM-Station 2.RobotProximityFault.2...	0:01:03.012	5/30/2018 6:26:00 PM	5/30/2018 6:27:03.012 PM	(R25.1)		None
ALARM-Station 2.HighTroubleCallCount....	0:05:34.004	5/30/2018 6:21:29.008 PM	5/30/2018 6:27:03.012 PM	(R24.1)		None
PLC.Batch.2018-05-30 18:13:37.003	0:13:26.001	5/30/2018 6:13:37.003 PM	5/30/2018 6:27:03.004 PM			None
ALARM-Station 2.StationModeError.201...	0:01:36.998	5/30/2018 6:10:48.01 PM	5/30/2018 6:12:25.008 PM	(R24.6)		None
ALARM-Station 2.StationStateError.201...	0:00:34	5/30/2018 6:09:31.012 PM	5/30/2018 6:10:05.012 PM	(R24.5)		None
ALARM-PLC.HighWorkcellTemperature.2...	0:01:40.006	5/30/2018 6:04:08.006 PM	5/30/2018 6:05:48.012 PM	(R26.1)		Major
ALARM-Station 2.StationDoorFault.2018...	0:00:13	5/30/2018 6:02:00.008 PM	5/30/2018 6:02:13.008 PM	(R24.4)		None
ALARM-PLC.InspectionFailure.2018-05-...	0:08:07.996	5/30/2018 6:00:17.01 PM	5/30/2018 6:08:25.006 PM	(R24.3)		None
ALARM-PLC.StationOutOfSync.2018-05-...	0:16:40.998	5/30/2018 5:51:44.008 PM	5/30/2018 6:08:25.006 PM	(R24.2)		None
PLC.Batch.2018-05-30 17:49:48.004	0:18:37.002	5/30/2018 5:49:48.004 PM	5/30/2018 6:08:25.006 PM			None

Event Frame Search






Process-Level Behavioral Anomalies

Data Corruption

Abnormal Process Variable Values

Two-way communication occurs between the supervisory PLC and the machining stations during normal operations. If a process variable trends outside of the known operational range, this anomaly should be reported.

```
Alarm := if('RawState' < 0 OR 'RawState' > 5) then 1  
else 0;
```













  	Name	[00:19:44.007...	Duration	Start Time
 	ALARM-Station 2.StationStateError.201...		0:00:36.826	5/30/2018 6:09:31.012 PM

Communications Errors

Robot Data Transmission Failure

The unsafe condition that this communication failure can cause warrants investigation by an operator. Substantial damage can occur to both the machining station and robots if this failure is not detected. This anomaly could be an end goal for an attacker with the intent to cause production disruption or financial loss through equipment damage.

```
Alarm := if (('Mode' = "RUN") and (PrevVal('Mode', '*-2m') = "RUN") and (TagMax(';RobotProximity', '*-2m', '*') = 0)) then 1 else 0;
```








   	Name	[00:36:12.995...	Duration	Start Time
	  ALARM-Station 1.RobotProximityFault.2...		 0:00:31.083	5/30/2018 6:26:00 PM
	  ALARM-Station 2.RobotProximityFault.2...		 0:00:31.086	5/30/2018 6:26:00 PM

Concerning Trends

Trouble Call Frequency Increase

Trouble calls are generated automatically by a machining station when it detects an anomaly during manufacturing operations (e.g., broken tooling, coolant failure).

```
Trouble := if ('State' = "TROUBLE" AND  
(PrevVal('State', '*-1s') = "TROUBLE") = False) THEN  
"TROUBLE" ELSE NoOutput();  
  
TroubleCount := if (EventCount('Alarm-  
TroubleCounterEvent', '*-10m', '*') >= 5) Then 1 Else 0;
```

   	Name	[00:31:42.003...	Duration	Start Time
 	ALARM-Station 2.HighTroubleCallCount....		0:02:21.415	5/30/2018 6:21:29.008 PM
	PLC.Batch.2018-05-30 18:13:37.003		0:10:13.423	5/30/2018 6:13:37.003 PM












Operational Errors

Machining Station Out-of-Sync

```
WCState := if(TimeEq('WorkcellState', '*-5s', '*', "RUN") >=5)
then "RUN" else "Starting";

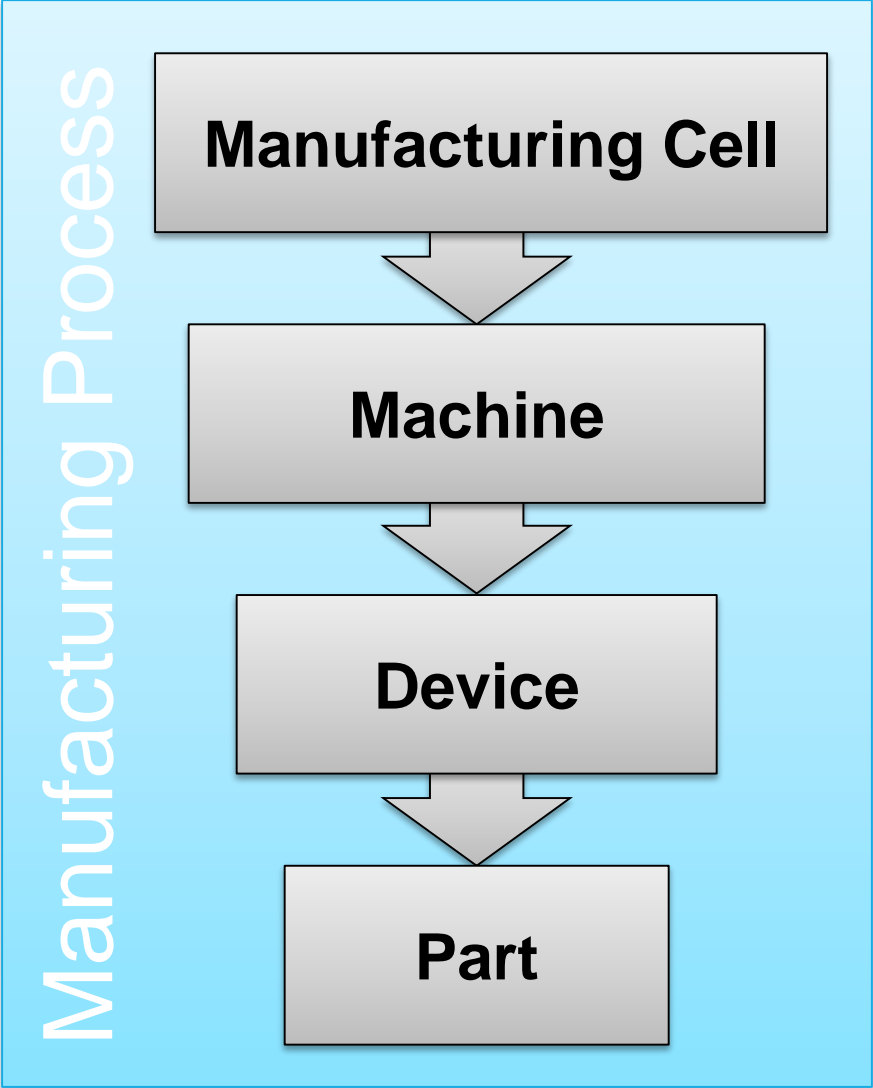
StationsSync := if (S1State = "STOPPED" OR S2State =
"STOPPED" OR S3State = "STOPPED" OR S4State = "STOPPED")
then 1 else 0;

Alarm := if (StationsSync = 1 And WCState = "RUN") then 1
else 0;
```

   	Name	[00:01:57.003...	Duration	Start Time
 	 ALARM-PLC.StationOutOfSync.2018-05-...		 0:00:45.531	5/30/2018 5:51:44.008 PM
	 PLC.Batch.2018-05-30 17:49:48.004		 0:02:41.536	5/30/2018 5:49:48.004 PM

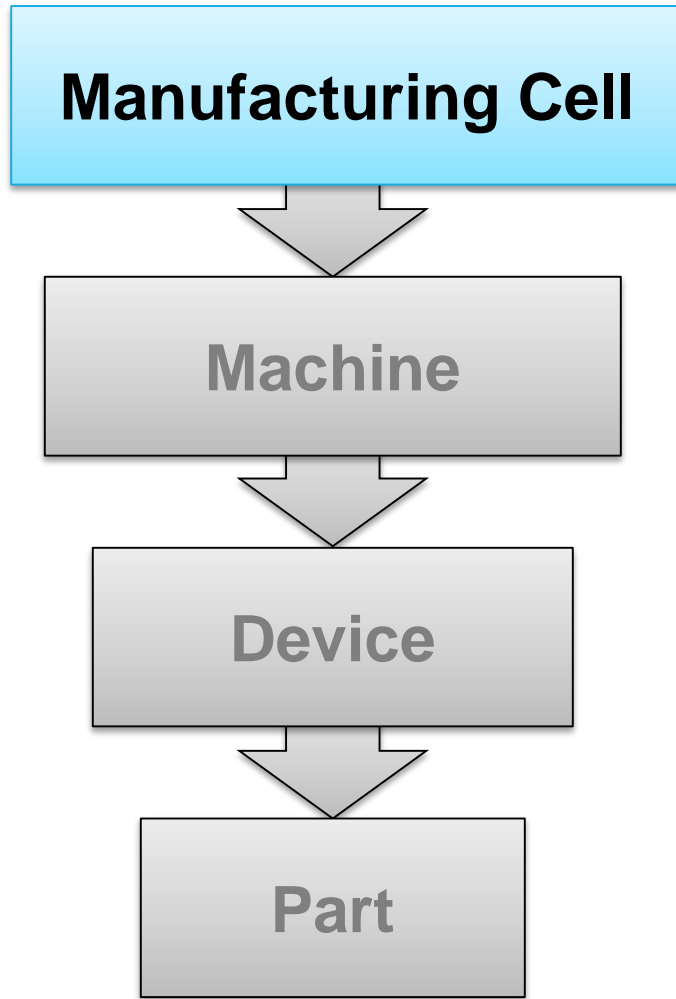
Manufacturing Process Analytics

Useful Process-Level Analytics



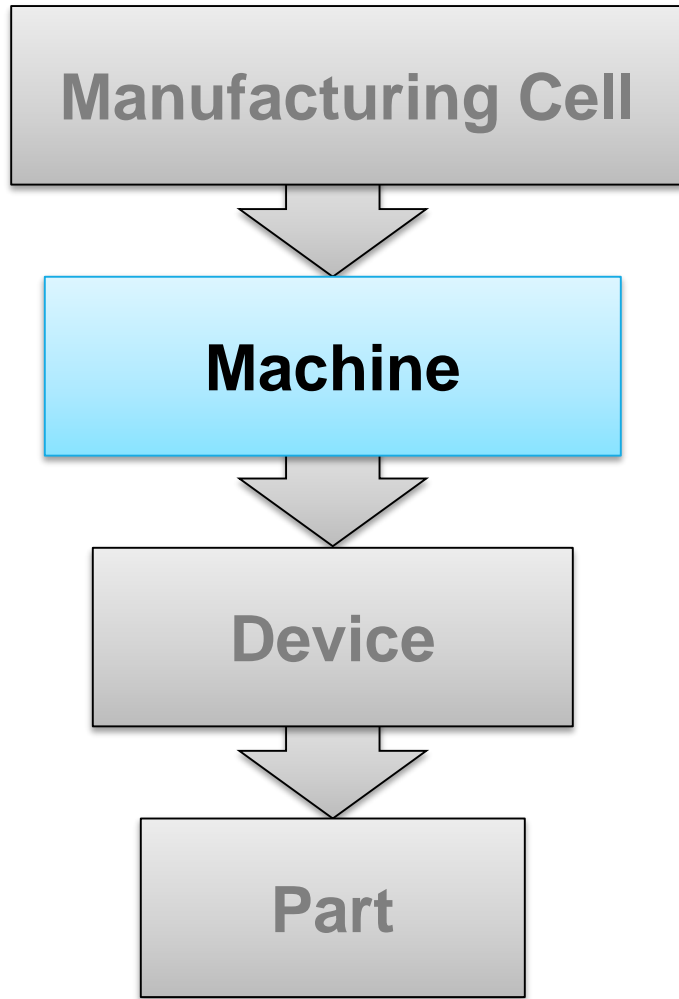
Mikell P. Groover. "Automation, Production Systems and Computer-Integrated Manufacturing". Third Edition. Pearson Education. 2008.

Useful Process-Level Analytics



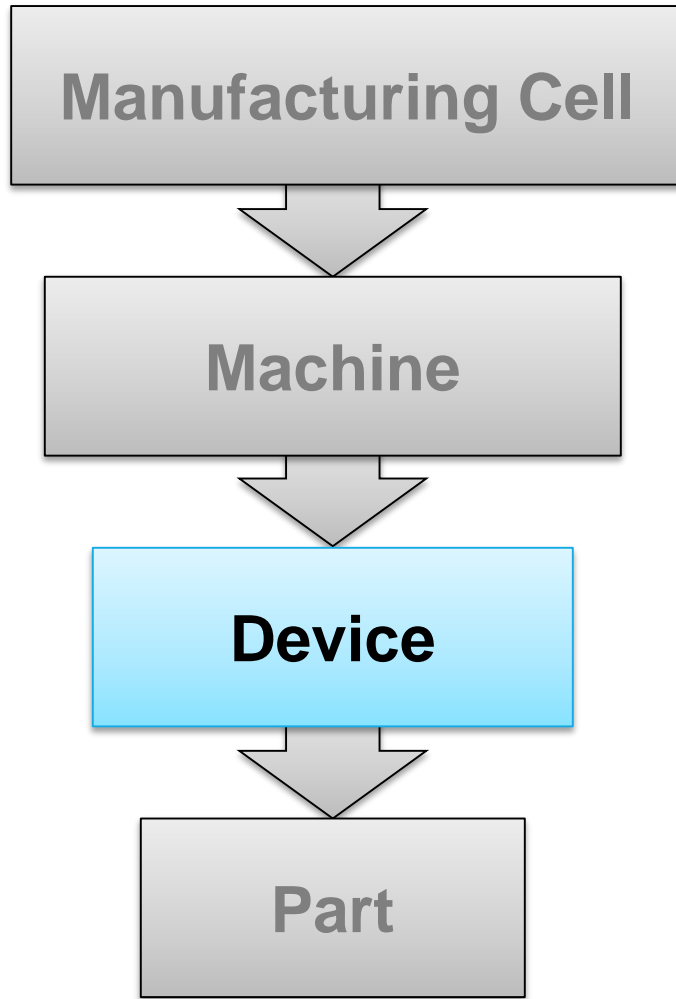
- **Workcell coordination**
- **Environmental sensing**
- **M2M interactions**
- **Operator interventions**
- **KPI**

Useful Process-Level Analytics



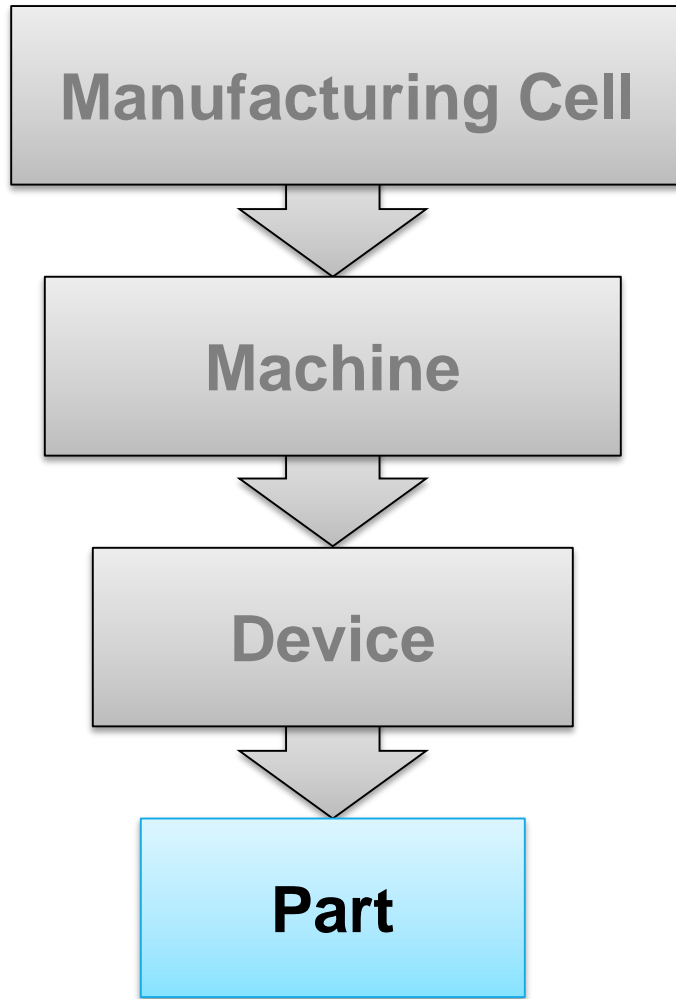
- **Production rates**
- **Cycle times**
- **Trouble call frequency**
- **Critical events**
- **Health Metrics**

Useful Process-Level Analytics



- **Sensor activity**
- **Actuator activity**
- **Process variables/registers**
- **Error codes**

Useful Process-Level Analytics



- **Quality metrics**
- **Inspection measurements**
- **Serial number tracking**
- **Production Time**

Conclusion

- The goal of this build:
 - demonstrate behavioral anomaly detection techniques that businesses can implement and use to strengthen the cybersecurity of their manufacturing processes.
- The behavioral anomaly detection project demonstrated three different detection methods:
 - network based,
 - agent-based, and
 - operational historian/sensor based.
- [NISTIR 8219](#) *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*

Acknowledgements

- **Paul Geraci, Andrew Duke, David Black, and Dennis Hui from OSIssoft for their technical assistance and working with us during our extremely short two-week deadline.**

Questions

Please wait for the **microphone** before asking your questions



State your **name & company**

Please don't forget to...

complete the Post
Event Survey

Contact Information



Michael Powell

Cybersecurity

michael.powell@nist.gov

NIST



Timothy A. Zimmerman

Computer Engineer

timothy.zimmerman@nist.gov

NIST



Thank You



謝謝

KEA LEBOHA

TAPADH LEIBH

고맙습니다

БАЯРЛАЛАА

MISAOTRA ANAO

OBRIGADO شكرا

DANKON TANK TAPADH LEAT

SALAMAT

DZIEKUJE CI

NGIYABONGA

TEŞEKKÜR EDERİM

DANKIE

TERIMA KASIH

GRÀCIES

СПАСИБО

РАКМЕТ СИЗГЕ



OSIsoft®

MULTUMESC

HVALA

FAAFETAI

ESKERRIK ASKO

HVALA ХВАЛА ВАМ

TEŞEKKÜR EDERİM

THANK YOU

DANK JE

ΕΥΧΑΡΙΣΤΩ GRATIAS TIBI

AČIŮ

SALAMAT

MAHALO IĀ 'ŌE

TAKK SKALDU HA

ДЗЯКУЙ

GRAZIE

DI OU MÈSI

ĎAKUJEM

MATUR NUWUN

KÖSZÖNÖM

GO RAIBH MAITH AGAT

БЛАГОДАРЯ GRACIAS

ТИ БЛАГОДАРАМ

TAK DANKE

MAHADSANID

РАНМАТ

MERCI

HATUR NUHUN

GRAZZI

PAKKA PĒR

PAХМАТ САГА

CẢM ƠN BẠN

WAZVIITA

FALEMINDERIT

ありがとうございました

SIPAS JI WERE

TERIMA KASIH

UA TSAUG RAU KOJ

ТИ БЛАГОДАРАМ

СИПОС