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

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

© Copyright 2018 OSIsoft, LLC

Defined

© Copyright 2018 OSIsoft, LLC

Mission

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

© Copyright 2018 OSIsoft, LLC

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.

© Copyright 2018 OSIsoft, LLC

NIST Information Technology Laboratory

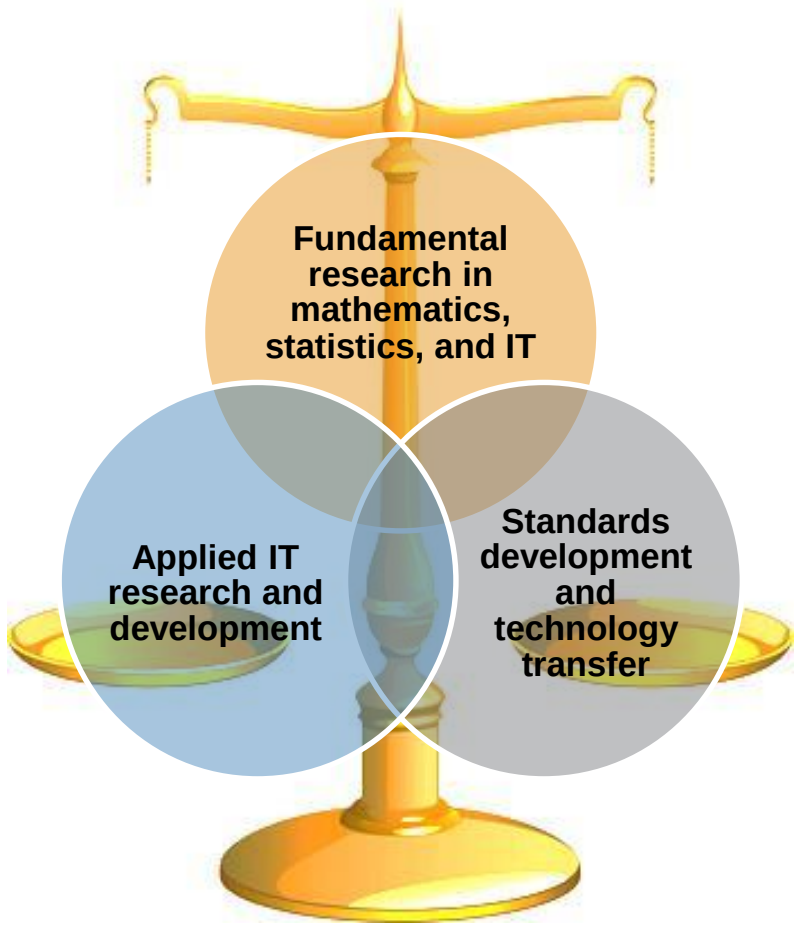
Cultivating Trust in IT and Metrology through measurements, standards and tests

ITL Programs

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

Collaborations with

- Industry
- Federal/State/Local Governments
- Academia



© Copyright 2018 OSIsoft, LLC

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

© Copyright 2018 OSIsoft, LLC

Engagement & Business Model

DEFINE

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

ASSEMBLE

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

BUILD

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

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

© Copyright 2018 OSIsoft, LLC

Body of Work

© Copyright 2018 OSIsoft, LLC

NCCoE Tenets

Standards-based

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

Modular

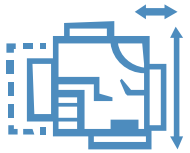
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

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

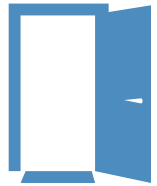
Commercially available

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

© Copyright 2018 OSIsoft, LLC

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

© Copyright 2018 OSIsoft, LLC

Sector-Based Projects

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

© Copyright 2018 OSIsoft, LLC

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.

© Copyright 2018 OSIsoft, LLC

CRADA members

© Copyright 2018 OSIsoft, LLC

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
			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
			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	
			Employ automated mechanisms to support impact analysis.	IR-4(1), SI-4(2)
			High	
			Correlate detected event information and responses to achieve perspective on event impact across the organization.	IR-4(4)

DRAFT

© Copyright 2018 OSIsoft, LLC

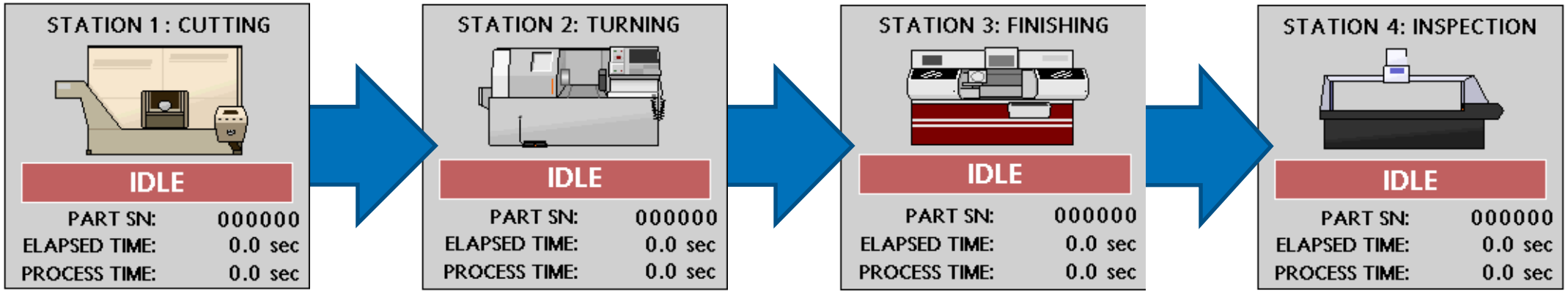
Behavioral Anomalies

- 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

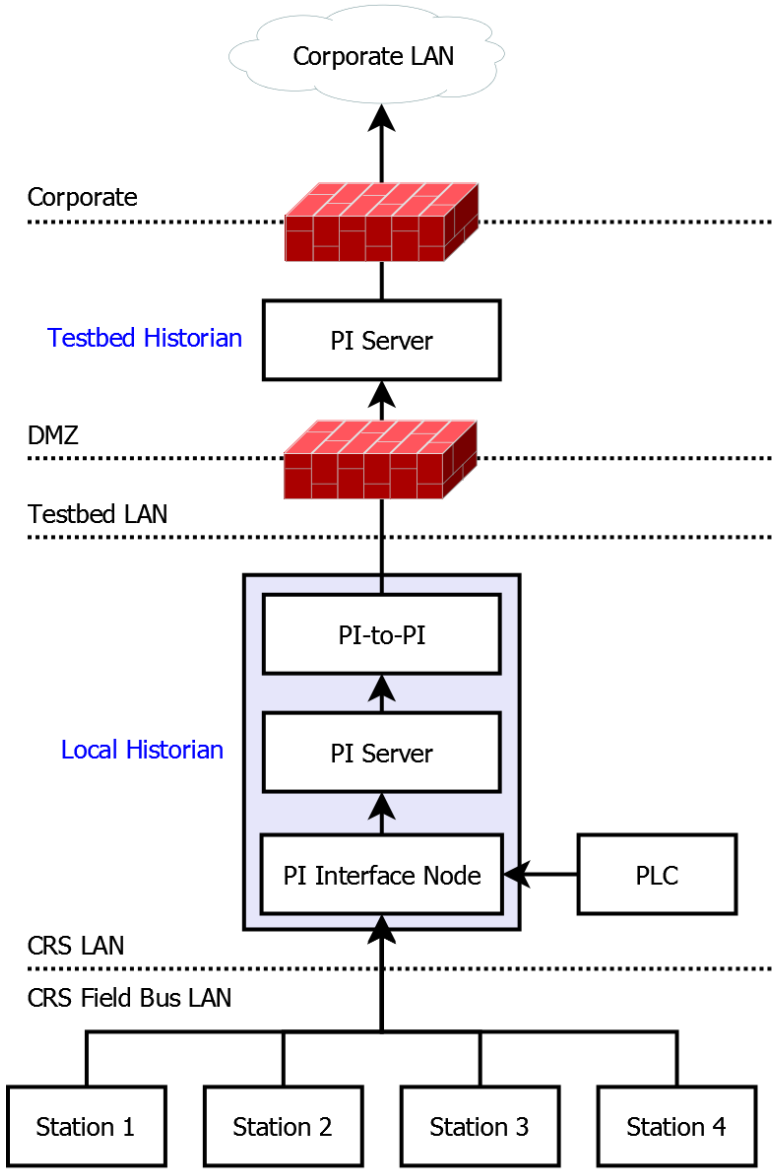
© Copyright 2018 OSIsoft, LLC

PI Implementation on the CSMS Testbed

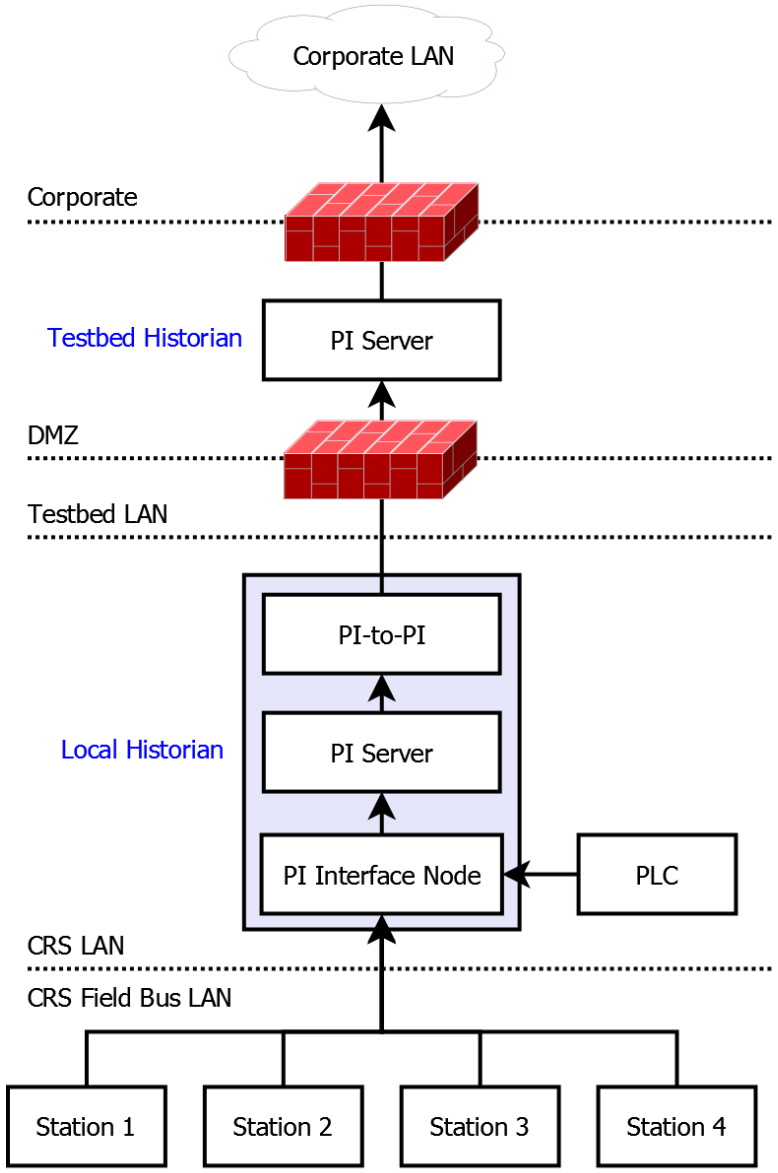
- Discrete process
- Four machining stations
- Two machine-tending robots
- Supervisory PLC
- Modbus TCP



© Copyright 2018 OSIsoft, LLC



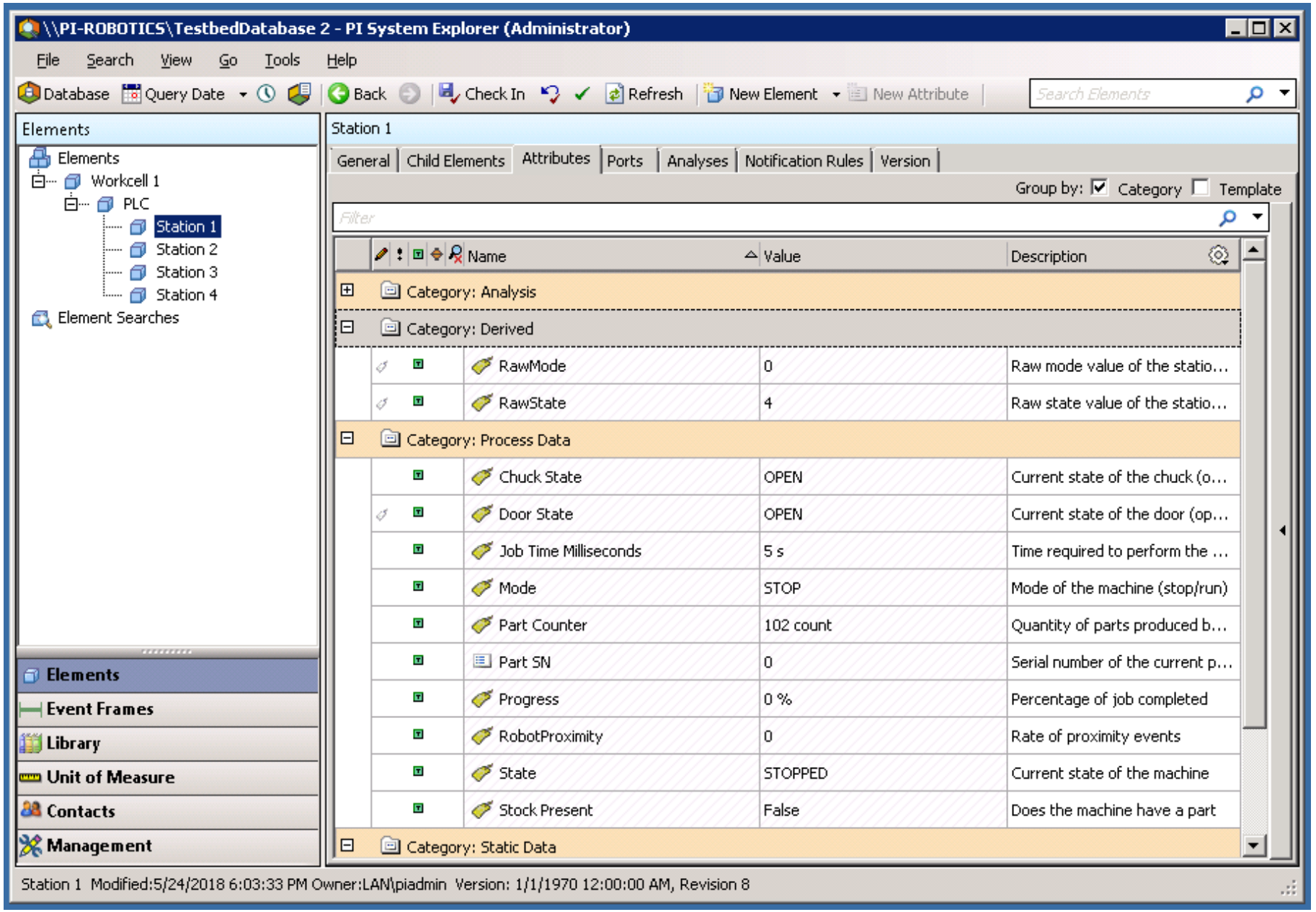
© Copyright 2018 OSIsoft, LLC



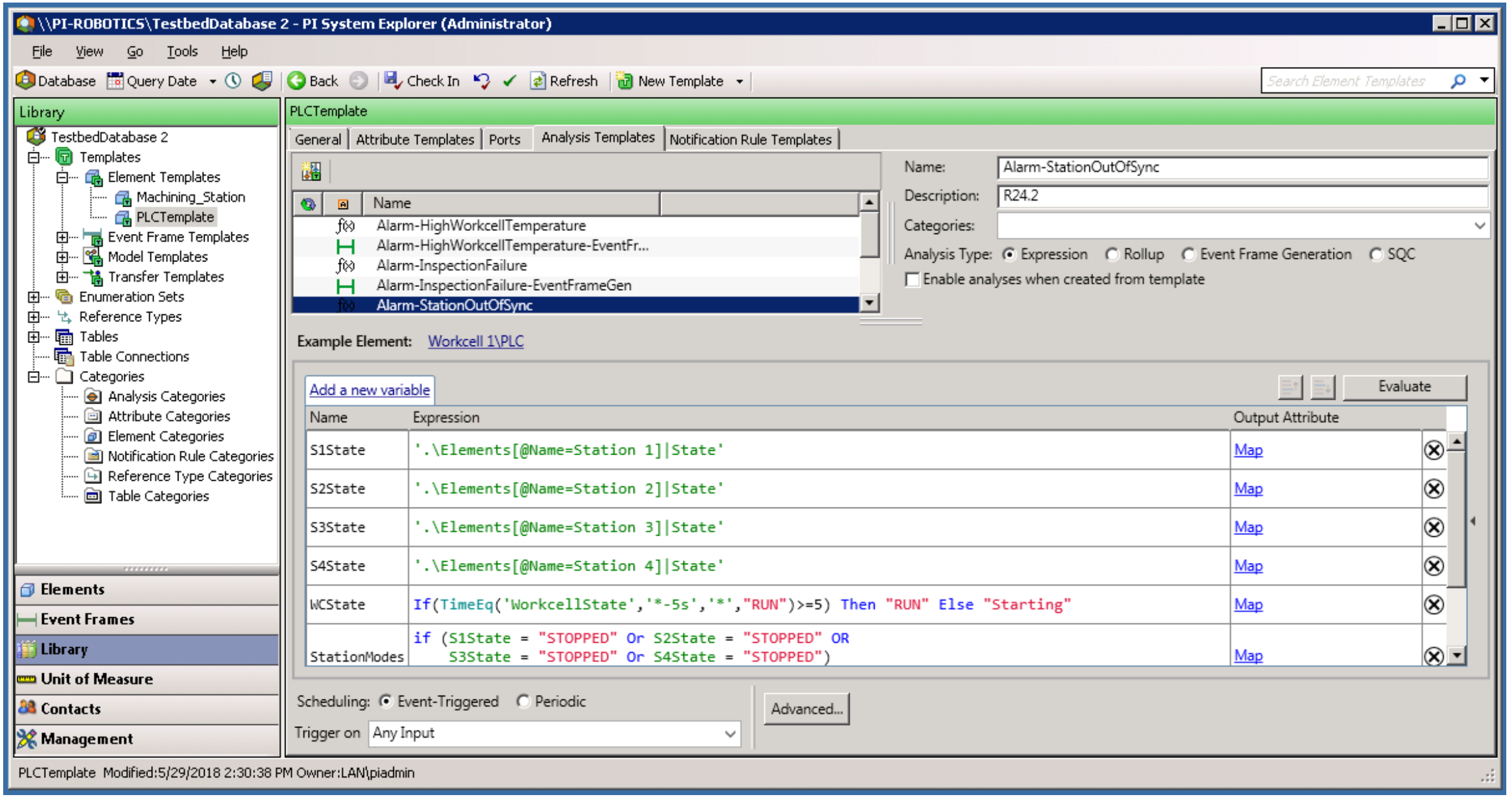
Components:

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

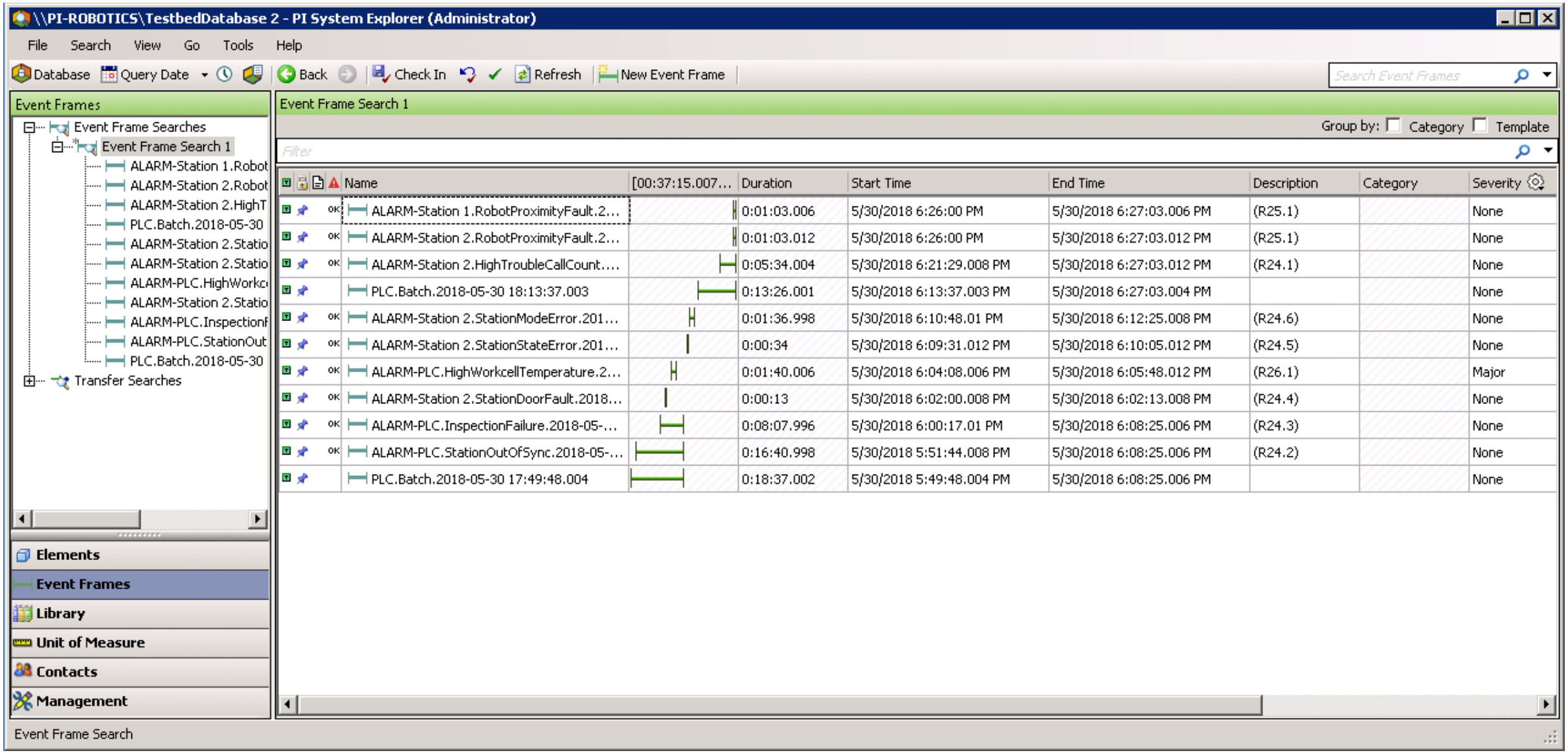
© Copyright 2018 OSIsoft, LLC



© Copyright 2018 OSIsoft, LLC



© Copyright 2018 OSIsoft, LLC



© Copyright 2018 OSIsoft, LLC

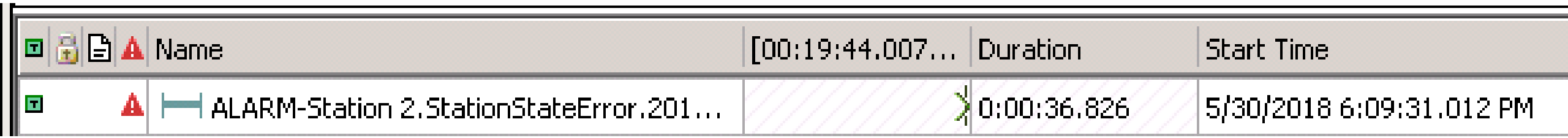
Process-Level Behavioral Anomalies

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;
```



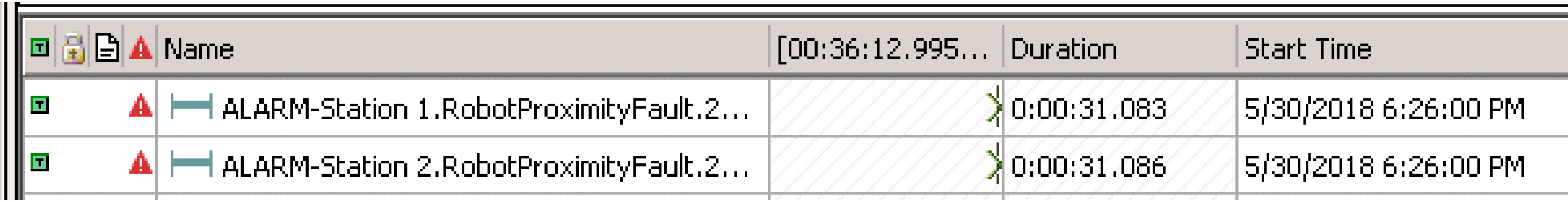
© Copyright 2018 OSIsoft, LLC

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

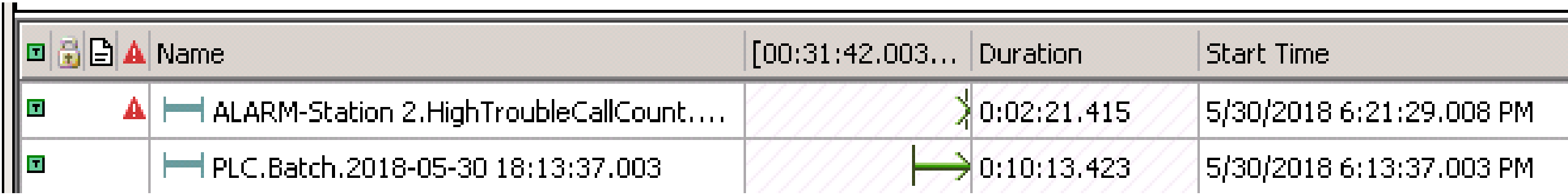
© Copyright 2018 OSIsoft, LLC

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).

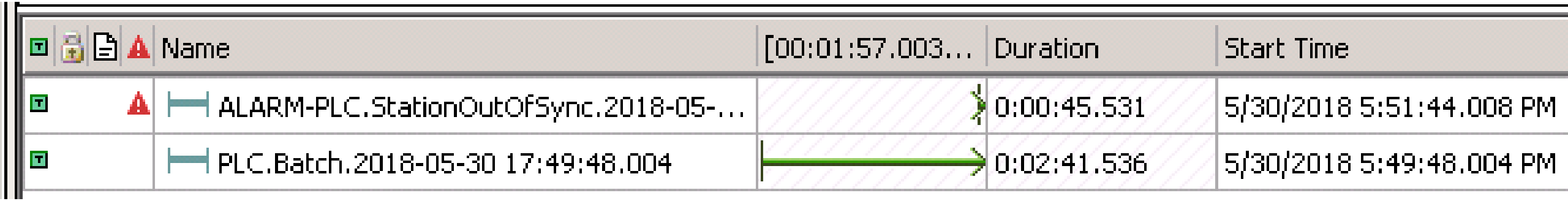
```
Trouble := if ('State' = "TROUBLE" AND
((PrevVal('State','*-1s') = "TROUBLE") = False)) THEN
"TROUBLE" ELSE NoOutput();

TroubleCount := if (EventCount('Alarm-
TroubleCounterEvent','*-10m','*') >= 5) Then 1 Else 0;
```



© Copyright 2018 OSIsoft, LLC

Operational Errors
Machining Station Out-of-Sync

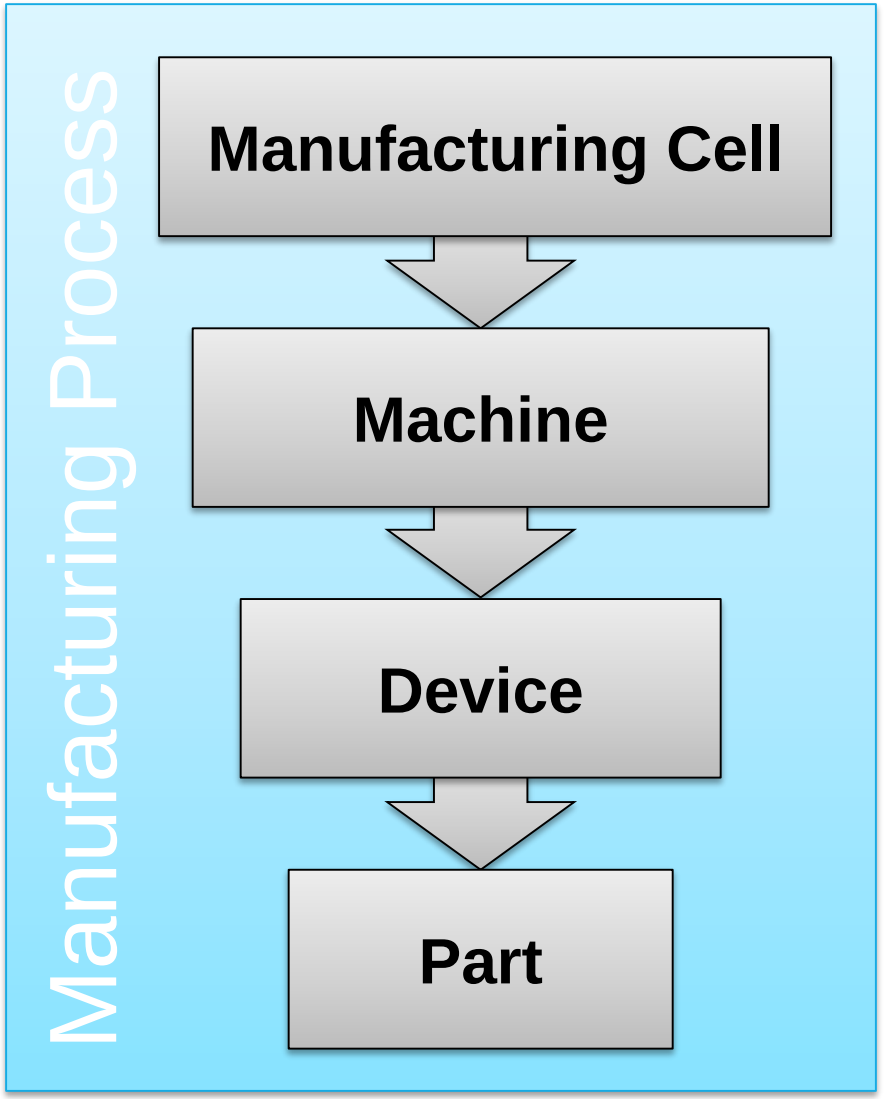
```
WCState := if(TimeEq('WorkcellState','*-5s','*',"RUN")>=5)
then "RUN" else "Starting";

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;
```



© Copyright 2018 OSIsoft, LLC

Manufacturing Process Analytics

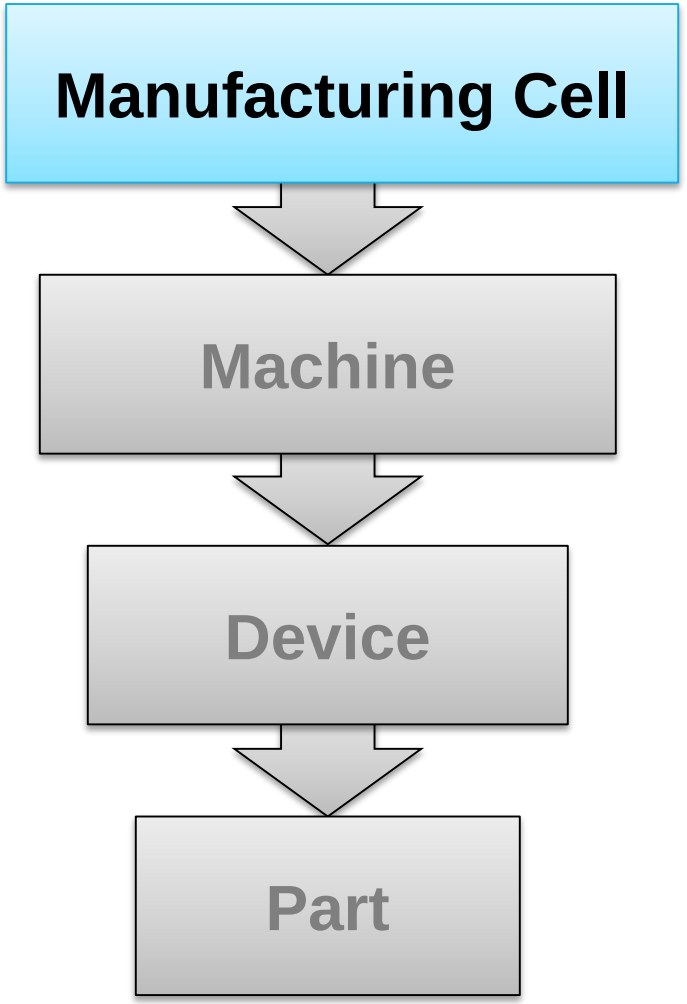
Useful Process-Level Analytics



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

© Copyright 2018 OSIsoft, LLC

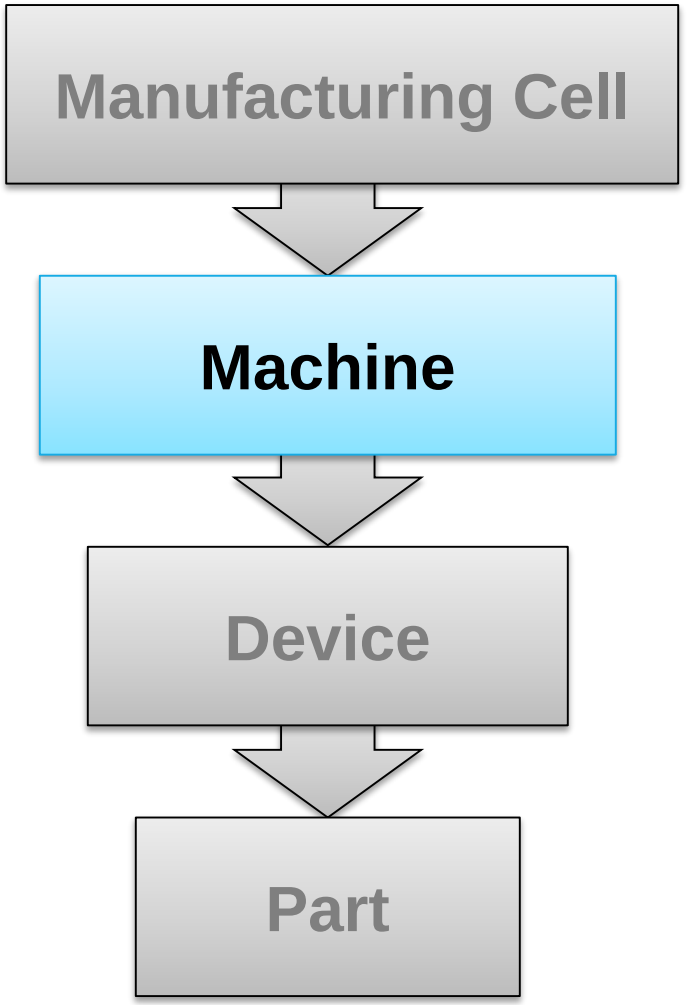
Useful Process-Level Analytics



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

© Copyright 2018 OSIsoft, LLC

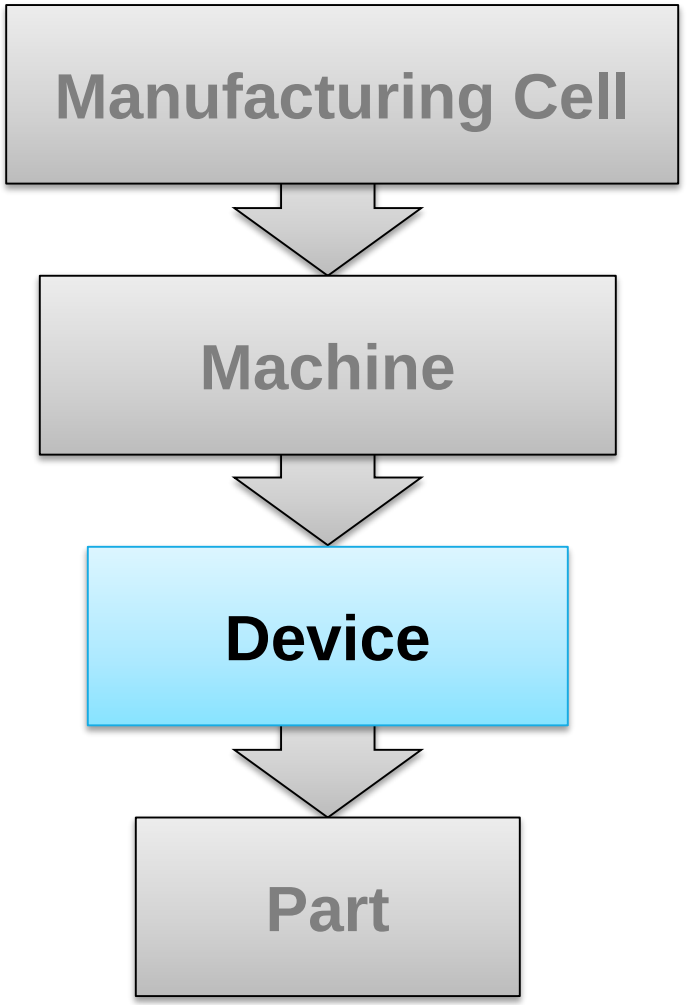
Useful Process-Level Analytics



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

© Copyright 2018 OSIsoft, LLC

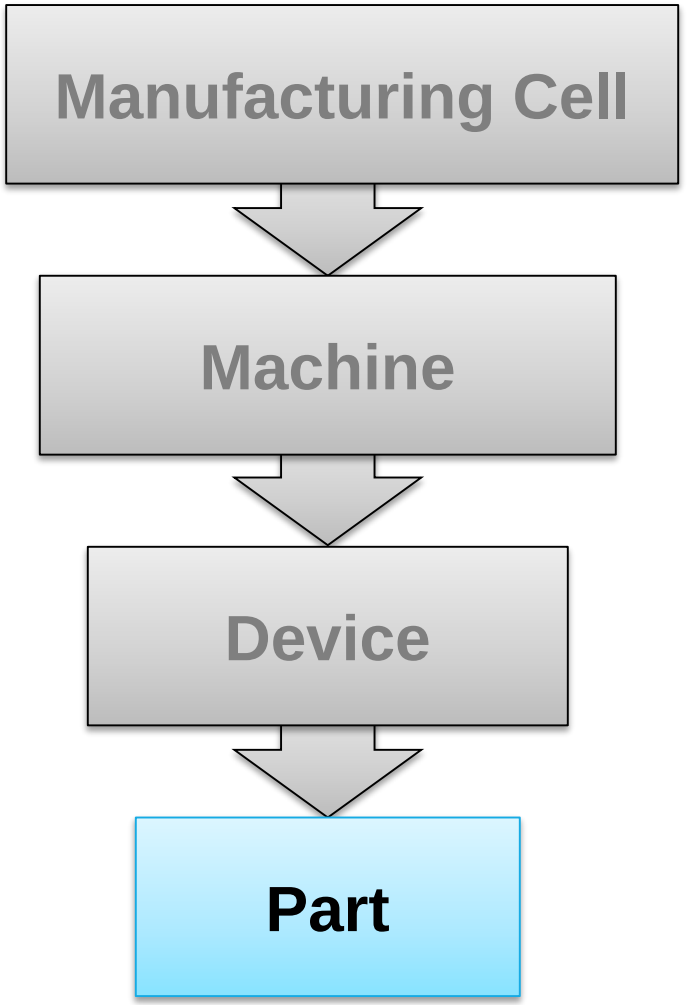
Useful Process-Level Analytics



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

© Copyright 2018 OSIsoft, LLC

Useful Process-Level Analytics



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

© Copyright 2018 OSIsoft, LLC

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*

© Copyright 2018 OSIsoft, LLC

Acknowledgements

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

© Copyright 2018 OSIsoft, LLC

Questions

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

State your **name & company**

Please don't forget to…

complete the Post Event Survey

© Copyright 2018 OSIsoft, LLC

Contact Information

Michael Powell

Cybersecurity

michael.powell@nist.gov

NIST

Timothy A. Zimmerman

Computer Engineer

timothy.zimmerman@nist.gov

NIST

© Copyright 2018 OSIsoft, LLC

Thank You


謝謝
KEA LEBOHA
TAPADH LEIBH
고맙습니다
БАЯРЛАЛАА
MISAOTRA ANAO
DZIĘKUJĘ CI
NGIYABONGA
TEŞEKKÜR EDERIM
GRÁCIES
OBRIGADO
شكرا
SALAMAT
DANKIE
TERIMA KASIH
DANKON
TANK
TAPADH LEAT
KÖSZÖNÖM
СПАСИБО
MULȚUMESC
OSIsoft
РАКМЕТ СІЗГЕ
FAAFETAI
GO RAIBH MAITH AGAT
ESKERRIK ASKO
HVALA
HVALA
ХВАЛА ВАМ
БЛАГОДАРЯ
GRACIAS
THANKYOU
TEŞEKKÜR EDERIM
ТИ БЛАГОДАРАМ
MAHADSANID
TAK
DANKE
DANK JE
ΕΥΧΑΡΙΣΤΩ
GRATIAS TIBI
ДЯКУЙ
GRAZIE
RAHMAT
MERCI
AČIÚ
SALAMAT
MAHALO IĀ 'OE
TAKK SKAL DU HA
DI OU MÈSI
HATUR NUHUN
GRAZZI
ÞAKKA ÞÉR
ありがとうございました
ĎAKUJEM
PAXMAT САГА
SIPAS JI WERE
TERIMA KASIH
MATUR NUWUN
CẢM ƠN BẠN
FALEMINDERIT
UA TSAUG RAU KOJ
WAZVIITA
ТИ БЛАГОДАРАМ
СИПОС