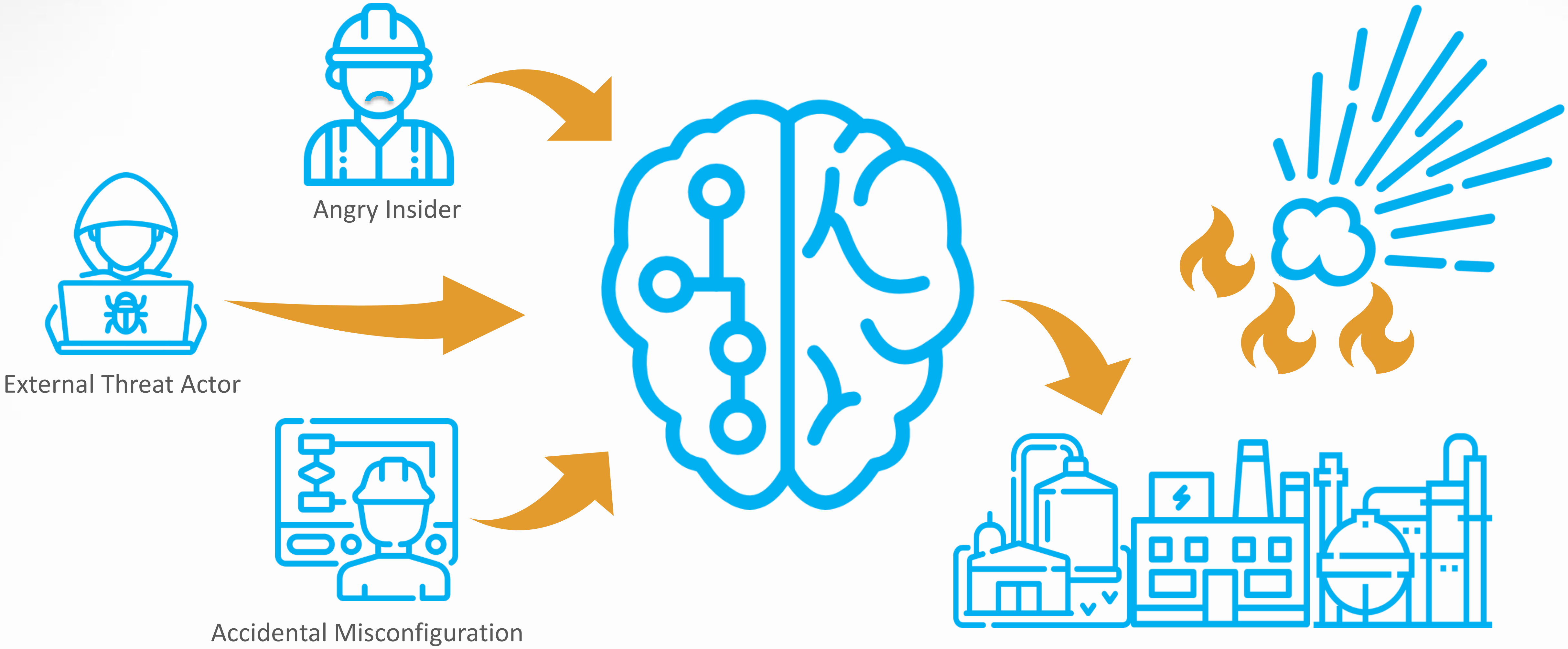
Mind the Gap

Understand the Distance Between
IT & OT Cyber Incident
Forensic Analysis & Safe Restart

Mark Carrigan
Chief Operating Officer, PAS Global, LLC

Insiders, Outsiders, & Mistakes – All Require Forensic Analysis



Angry Insider

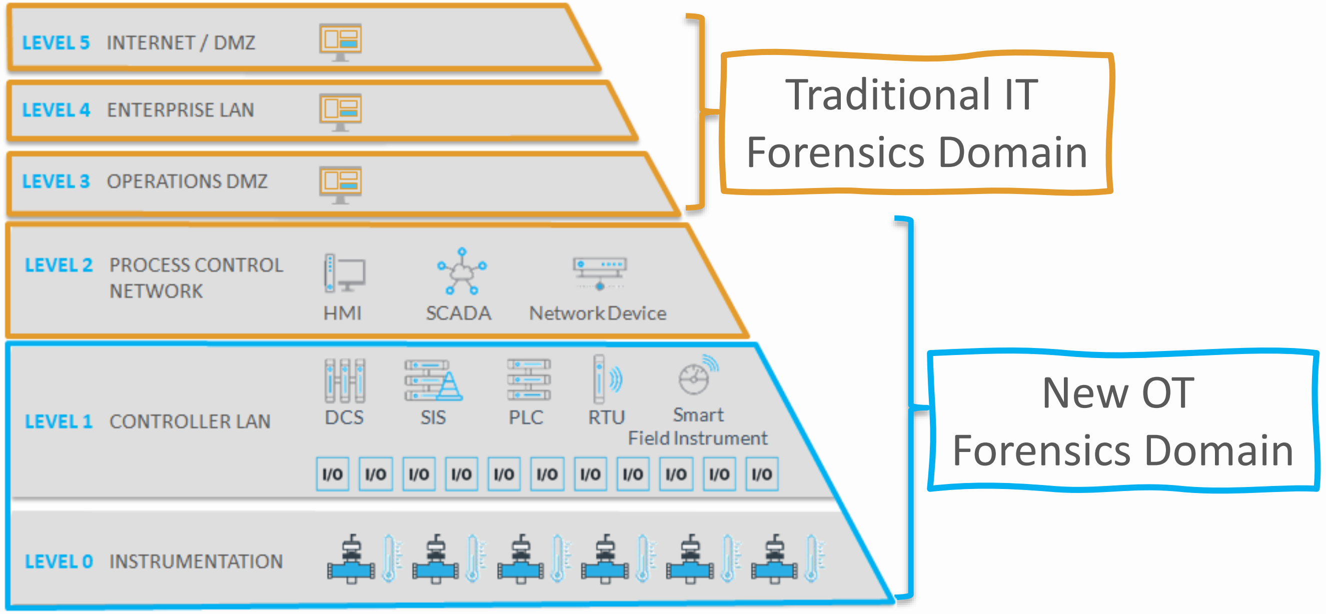
External Threat Actor

Accidental Misconfiguration

Forensic Analysis

Forensic Analysis

> *"…the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."*[1]



Forensic Analysis Process Model[2]

1. Identification and Preparation
2. Identifying Data Sources
3. Prioritizing, Preservation, & Collection
4. Examination
5. Analysis
6. Reporting and Presentation
7. Reviewing Results

Sources:

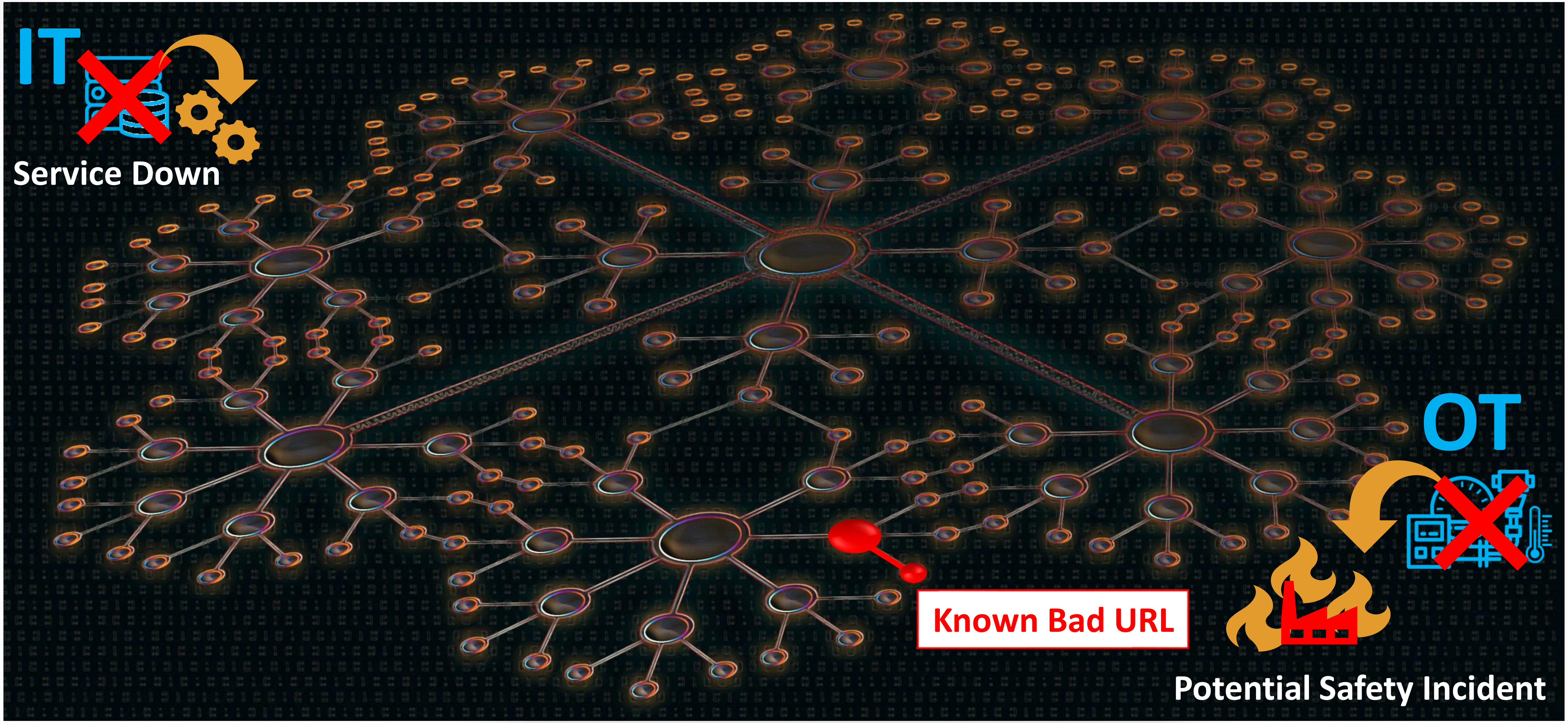
[1] NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response, Karen Kent (NIST), Suzanne Chevalier (BAH), Tim Grance (NIST), Hung Dang (BAH), August 2006

[2] Towards a SCADA Forensics Architecture, Tina Wu, Jules Ferdinand Pagna Disso, Kevin Jones, & Adrian Campos, 2013

1. It’s 12 AM
2. A system that controls a safety critical process is malfunctioning
3. You don’t know if it is a technical problem or a cyber attack

Who ya gonna call?

IT vs OT Consequences



Differing Missions

IT

Workstations | Servers | Routers
Switches | Firewalls

Flexible Applications

Security > Availability

New (3-5 years)

Homogeneous

OT

DCS | PLC | SIS | Smart Field Instruments
3rd Party Modules | COM Modules | Control Level Firewalls
Controllers | Foundational Fieldbus Devices | Hart Devices
I/O Cards | Profibus Devices

Designed for Purpose

Availability > Security

Old (20+ years)

Heterogeneous

Building an OT Forensics Foundation

Deep Inventory

Detailed Configuration

Baselines

Change Point Verification*

Documentation

*Example on next slide

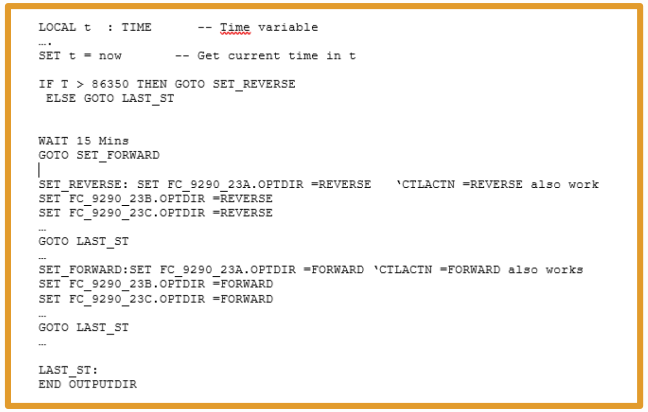
The Reverse

- Control Function Parameter – Output Characteristic
  - Name of parameter unique to each control system
- Binary Setting
  - Determines direct or indirect action based upon error (Setpoint-Process Value)

<u>Flip the Setting, Watch the Fun!</u>

- *Valve that was 20% open will now be 20% closed*
- *Fail safe valve will do the opposite of intended action*

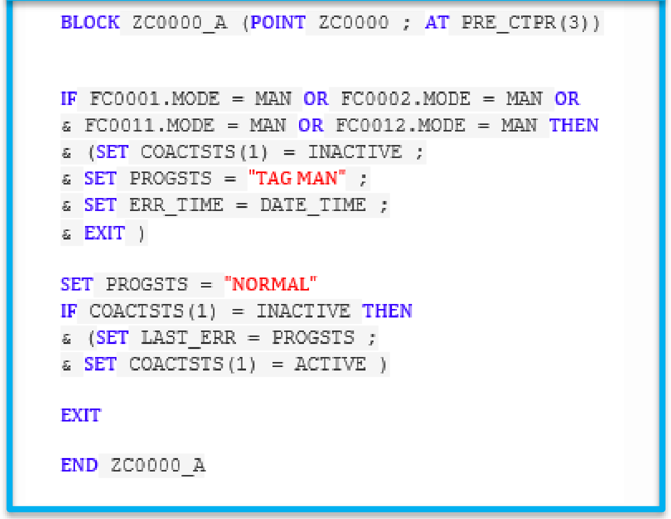
Example



```
LOCAL t  : TIME      -- Time variable
….
SET t = now       -- Get current time in t

IF T > 86350 THEN GOTO SET_REVERSE
 ELSE GOTO LAST_ST


WAIT 15 Mins
GOTO SET_FORWARD

SET_REVERSE: SET FC_9290_23A.OPTDIR =REVERSE   'CTLACTN =REVERSE also work
SET FC_9290_23B.OPTDIR =REVERSE
SET FC_9290_23C.OPTDIR =REVERSE
…
GOTO LAST_ST
…
SET_FORWARD:SET FC_9290_23A.OPTDIR =FORWARD 'CTLACTN =FORWARD also works
SET FC_9290_23B.OPTDIR =FORWARD
SET FC_9290_23C.OPTDIR =FORWARD
…
GOTO LAST_ST
…

LAST_ST:
END OUTPUTDIR
```

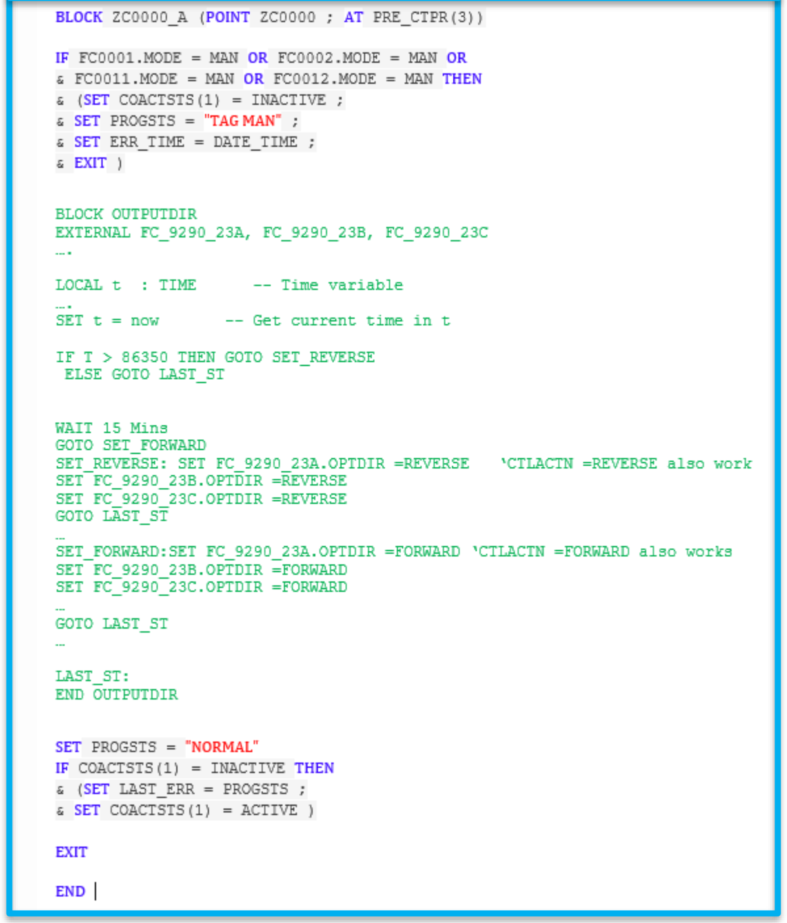
The Reverse

Rev 1



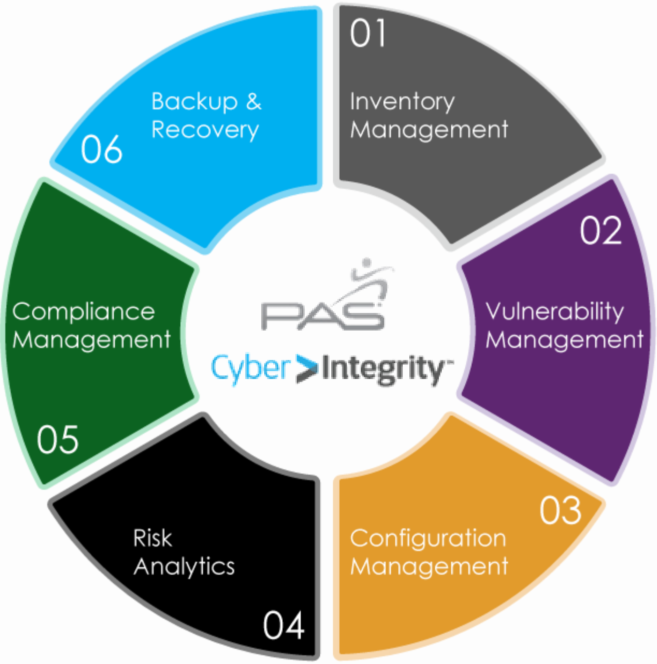
```
BLOCK ZC0000_A (POINT ZC0000 ; AT PRE_CTPR(3))


IF FC0001.MODE = MAN OR FC0002.MODE = MAN OR
& FC0011.MODE = MAN OR FC0012.MODE = MAN THEN
& (SET COACTSTS(1) = INACTIVE ;
& SET PROGSTS = "TAG MAN" ;
& SET ERR_TIME = DATE_TIME ;
& EXIT )

SET PROGSTS = "NORMAL"
IF COACTSTS(1) = INACTIVE THEN
& (SET LAST_ERR = PROGSTS ;
& SET COACTSTS(1) = ACTIVE )

EXIT

END ZC0000_A
```

Rev 2



```
BLOCK ZC0000_A (POINT ZC0000 ; AT PRE_CTPR(3))

IF FC0001.MODE = MAN OR FC0002.MODE = MAN OR
& FC0011.MODE = MAN OR FC0012.MODE = MAN THEN
& (SET COACTSTS(1) = INACTIVE ;
& SET PROGSTS = "TAG MAN" ;
& SET ERR_TIME = DATE_TIME ;
& EXIT )


BLOCK OUTPUTDIR
EXTERNAL FC_9290_23A, FC_9290_23B, FC_9290_23C
….

LOCAL t  : TIME      -- Time variable
….
SET t = now        -- Get current time in t

IF T > 86350 THEN GOTO SET_REVERSE
 ELSE GOTO LAST_ST


WAIT 15 Mins
GOTO SET_FORWARD
SET_REVERSE: SET FC_9290_23A.OPTDIR =REVERSE   ‘CTLACTN =REVERSE also work
SET FC_9290_23B.OPTDIR =REVERSE
SET FC_9290_23C.OPTDIR =REVERSE
GOTO LAST_ST
…
SET_FORWARD:SET FC_9290_23A.OPTDIR =FORWARD ‘CTLACTN =FORWARD also works
SET FC_9290_23B.OPTDIR =FORWARD
SET FC_9290_23C.OPTDIR =FORWARD
…
GOTO LAST_ST
…

LAST_ST:
END OUTPUTDIR


SET PROGSTS = "NORMAL"
IF COACTSTS(1) = INACTIVE THEN
& (SET LAST_ERR = PROGSTS ;
& SET COACTSTS(1) = ACTIVE )

EXIT

END |
```

PAS Cyber Integrity™ Accelerates Forensic Analysis & Response



01 Inventory Management

02 Vulnerability Management

03 Configuration Management

04 Risk Analytics

05 Compliance Management

06 Backup & Recovery

PAS Cyber>Integrity

- Protects OT assets against cyber threats
- Identifies critical endpoint vulnerabilities & risks
- Manages across all major control system manufacturers
- Accelerates forensic analysis & incident response
- Enables rapid recovery
- Prevents unplanned downtime

DCS | SIS | Historian | RTU | Smart Field Instrument | SCADA | PLC | Network Device | HMI/ Operator Station

ABB | AspenTech | Cisco | Emerson | GE | HIMA | Honeywell | Microsoft | OSIsoft | Rockwell | Schneider | Siemens | Schweitzer | Yokogawa | And More

Mark Carrigan
Chief Operating Officer
PAS Global, LLC

mcarrigan@pas.com

PAS®

ICS Cybersecurity. Safety. Compliance.

Thank You