MANDIANT®

No Place for Alert Fatigue in OT

Using proven strategies to improve

Bhojraj Parmar

Principal Strategic Consultant – ANZ

Mandiant Solutions

MANDIANT®

- Intro (About me and Mandiant)
- Issues (Causes of Alert Fatigue)
- Ideas (Proven Strategies to Improve)
- Interaction (Sharing Knowledge)

By the end of this one hour:

1. Tips for reducing noise for Operational Technology (OT) alerts
2. Ideas for working better with IT/OT teams to reduce Industrial Control Systems (ICS) security alerts
3. Some good questions before considering ICS security tools and
4. be a bit more social *

* COVID19 Restrictions Apply

©2020 Mandiant

About me

Have worked in CNI:

- Energy
- Gas
- Advance Meter Infrastructure
- Gov

Startups, Finance and non-profit

Lived, Worked 17yrs in:

- India
- Israel
- New Zealand
- Spain
- Australia

ICS Exposure:

- Physical security (Biometrics, Access Control)
- Building management system (HVAC)
- Historic artefact monitoring (IoT)
- Irrigation systems
- Lighting management
- Gas Plant Automation Systems
- Electricity Distribution
- Advance Metering Infrastructure

- SANS ICS515
- GRID Certified
- Was part of CSSIE in NZ
- Spoken at multiple events and hosted some training sessions on ICS Security

Some Cool ICS Projects:

- **Implemented ICS Threat Detection System for Power Grid**
- **Led the Security Architecture and Threat Modelling for a DER management and electricity distribution system in AWS**
- **Designed Security for APIs for EV charging stations (OCCP)**
- **Segmented Gas DCS Network**
- **Replaced RS232 connectors with RJ45 and IP based controllers for HVAC**
- **Replaced Irrigation controllers and programmed PLCs**
- **Implemented Network Access Control (NAC) for OT**

©2020 Mandiant

About Mandiant

AM I AT RISK?

- Red/Purple Team
- ICS Health Check

AM I PREPARED?

- Ransomware Readiness Assessment
- Security Program Assessment (SPA)
- Response Readiness Assessment (RRA)

AM I COMPROMISED?

- Compromise Assessment (CA)

I AM BREACHED!

- Incident Response (IR)

PREPARE FOR FUTURE EVENTS

- Cyber Defense Center Development (CDC)
- SOC/CIRT transformation
- Incident Response Retainer
- Crown Jewels Assessment (CJA)
- Deployment & Integration
- Education

©2020 Mandiant

https://www.fireeye.com/services/**freeware**.html

Let's set the record straight

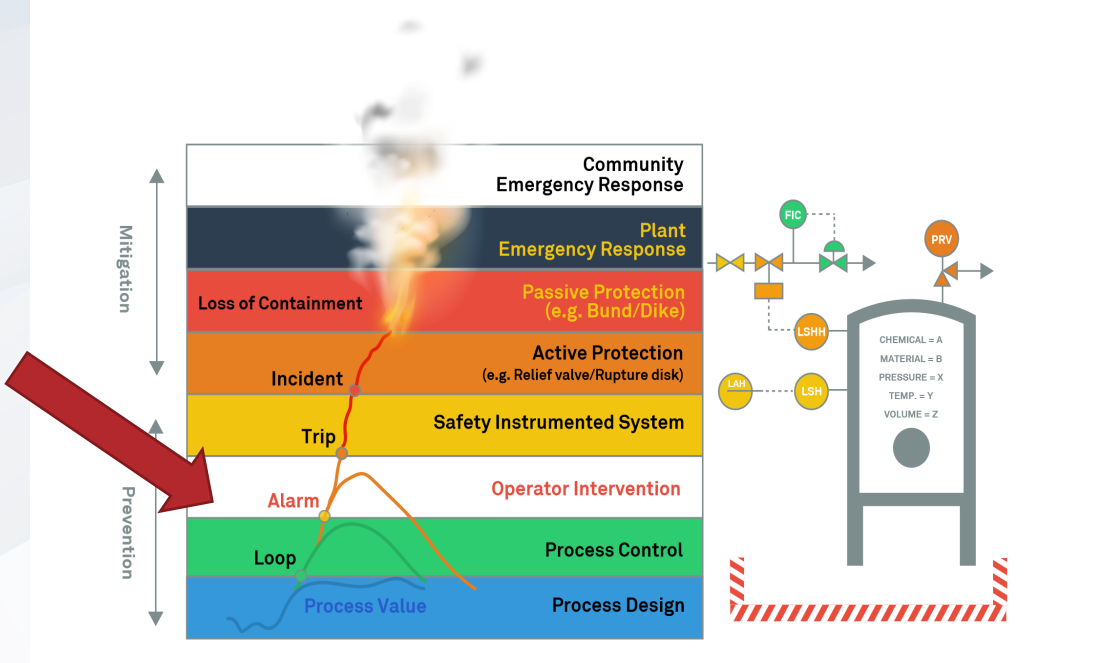
- Every industry has its own flavour of alert/alarm fatigue issues
- Some are more tolerant
- OT, especially CNIs have no place for it
- There are some helpful strategies and standards to use for improvement

©2020 Mandiant

Alert/Alarm

Definition of Alarm:
Alarms " Audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response"

(ISA-18.2, IEC 62682)



©2020 Mandiant

Source: https://www.exida.com/ebooks/alarm-shelving-exida-ebook.pdf

Issues – Language (Taxonomy)

IT SOC

- Typosquatting
- ShimCacheMutex

OT Eng/Ops

- LAD Diagram
- Goose
- Ripple

©2020 Mandiant

Issues – Context

Most ICS threat detection systems will only see this alert

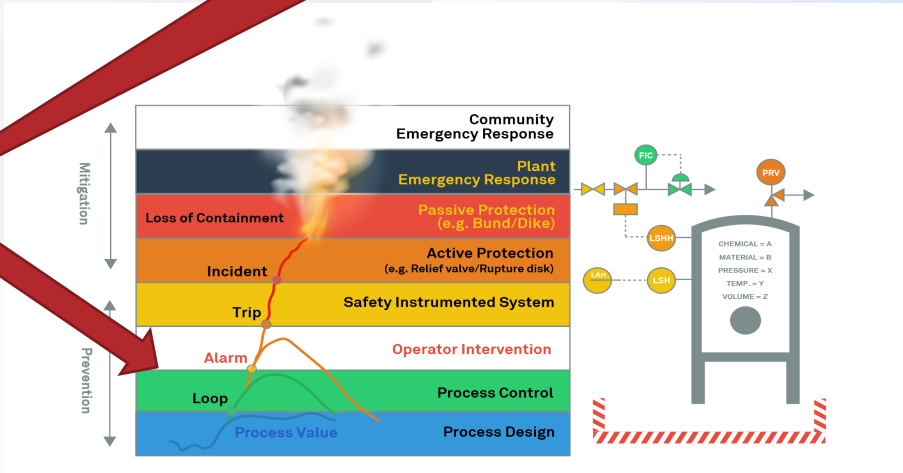
OT Assets and Process

- Cause and Effect

Door open alert – at a substation during a weekend (2 alerts)

A lot of Modbus traffic from an engineering workstation to IEDs (10 Alerts)

Some protection relays repeatedly cutting off power in the distribution zone of the same substation (10 Alarms)



©2020 Mandiant

Issues – Risk Awareness

- IT security alerts: commodity malware activity – risk is somewhat clear – cred/data theft, ransomware, bot or spy.
- OT security alerts: Modbus function 8 (Diagnostic) or 5 (Write) detected - the level of risk is depended on the asset and process
- Lack of Crown Jewels (asset and process) context in these alerts is a significant gap in the industry

©2020 Mandiant

Issues – Volume

For those who love numbers

- Average Triage time 10 or more minutes *

- More than half of IT and security professionals consider their security operations center (SOC) ineffectual, and the long hours, alert overload, and incomplete visibility into their IT infrastructure has 65% considering quitting their jobs

- Ponemon Institute Research: Improving the Effectiveness of the SOC – June 2019

©2020 Mandiant

* https://www.criticalstart.com/wp-content/uploads/CS_MDR_Survey_Report.pdf

Issues – Volume

For those who love numbers

IT Security Alerts

Events/Resources	Estimates
EOI Per Day	100
EOI Per Hour	2
Minimum Triage Time (m)	15
Analyst Shift (hr)	8
Number of Shifts (p/day)	3
Triaged EOI's p/shift	32
Required Analysts (p/day)	3

OT Security Alerts

Events/Resources	Estimates
EOI Per Day	100
EOI Per Hour	2
Minimum Triage Time (m)	30*
Analyst Shift (hr)	8
Number of Shifts (p/day)	3
Triaged EOI's p/shift	16
Required Analysts (p/day)	6

* More coordination, risk awareness and context needed

©2020 Mandiant

Let's try this – Get a pen and paper

Write Any Four Names

(One name at a time)

Please time yourself and post it in chat

1. Sally
2. Karen
3. Tony
4. Jim

Write the Same Four Names

(One letter at a time)

Please time yourself again and post it in chat

1.	S	a	l	l	y
2.	K	a	r	e	n
3.	T	o	n	y	
4.	J	i	m		

©2020 Mandiant

Proven Strategies - Checklists? Or Frameworks!

Some alarm management standards to consider:

ISA 18.2 - 2016 (Alarm Management for OT) +

NIST SP 800-94 (Alert Management for Security - **IDPS**)

Alarm Rationalisation + Alarm Shelving + Usecase Creation + Testing = Better Alerts = Less Alert Fatigue

©2020 Mandiant

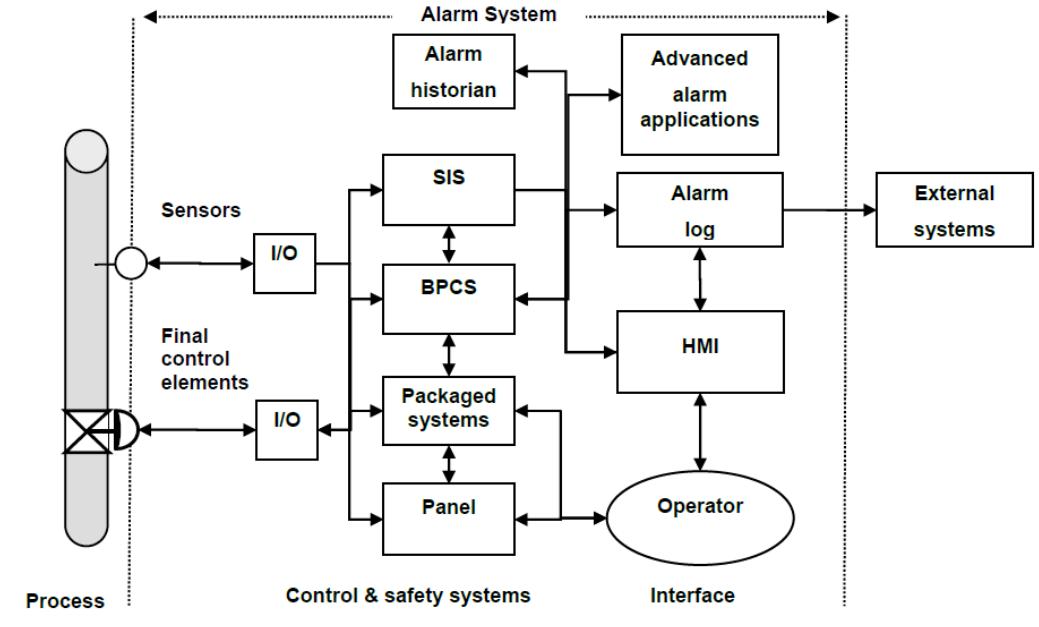
Proven Strategies - Alert/Alarm Management Standards

ISA 18.2-2016

"The primary function within the alarm system is to notify operators of abnormal process conditions or equipment malfunctions and support the response."

NIST SP 800-94 (Feb 2007)

"Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices."



NOTE Other packaged systems (i.e., fire and gas systems) can be included in the control system.

Figure 1 – Alarm system dataflow

Copyright © 2016 ISA. All rights reserved. **ISA 18.2-2016**

 ©2020 Mandiant

Source: Chris Sistrunk - Tuning ICS Security Alerts: An Alarm Management Approach

Proven Strategies - Alert/Alarm Management Standards

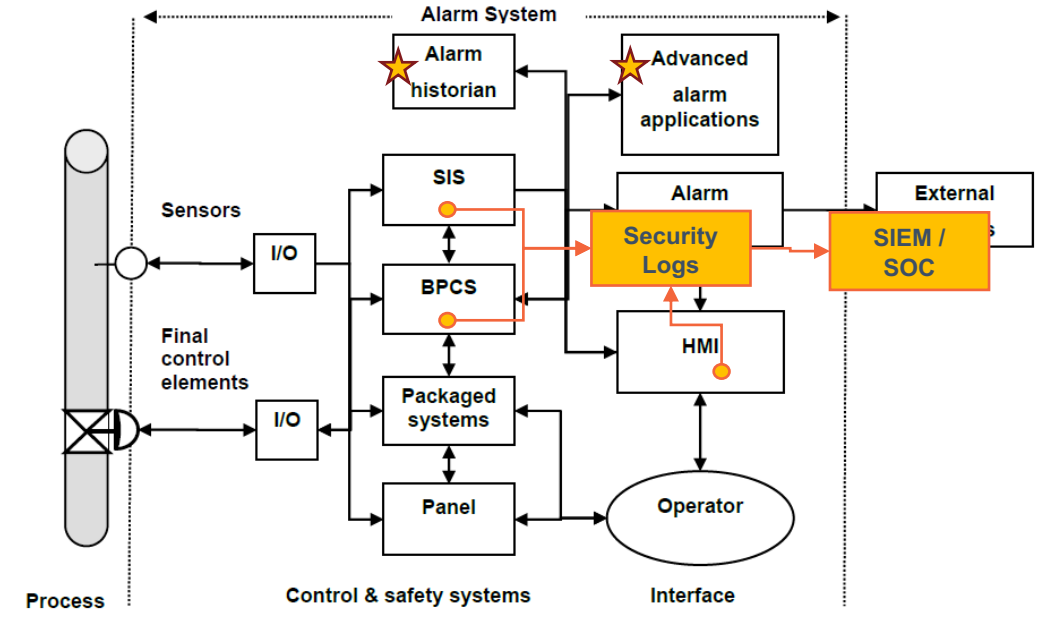
ISA 18.2-2016

"The primary function within the alarm system is to notify operators of abnormal process conditions or equipment malfunctions and support the response."

NIST SP 800-94

(Feb 2007)

"Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices."



NOTE Other packaged systems (i.e., fire and gas systems) can be included in the control system.

Figure 1 – Alarm system dataflow

Copyright © 2016 ISA. All rights reserved. **ISA 18.2-2016**

Source: Chris Sistrunk - Tuning ICS Security Alerts: An Alarm Management Approach

Proven Strategies – Context of Crown Jewels

Threat Modeling to reduce uncertainty

- Risk = Effect of uncertainty on objectives

  - ISO/IEC 27000:2018

- Crown Jewels Analysis (CJA) is a process for identifying those cyber assets that are most critical to the accomplishment of an organization's mission.

  - MITRE

- "Threats abuse vulnerabilities of assets to generate harm for the organisation"

  - ISO 27005

©2020 Mandiant

Proven Strategies – Context of Crown Jewels

A great example of a recent detection

Attack on Israel's civilian water system

"The control room watches them all the time — are they swimming faster or slower?"

https://www.timesofisrael.com/alongside-high-tech-systems-these-fish-stop-iran-hacking-israels-water-supply/

Fish swim in a tanks of drinking water to monitor quality at the Eshkol water purification site in Beersheba (Screencapture/Channel 12)

©2020 Mandiant

Proven Strategies – More Tools? Or Training

Tools are like kids – sweet, noisy and hyper – you must train them! When selecting ask the right questions:

- Will it consider the full context of cause and effect?
- What value it provides over my current toolset?
- NSM + IDS + HMI log + SIS + BCPS = more value then ICS threat detection system?

Don't put the ICS security alerts on your HMIs for operators to consume

©2020 Mandiant

Proven Strategies – Build Usecases

- Develop high fidelity usecases with business context
  – these are not the same as detection rules

Detection Usecase

- Doors opened during weekend
  – No field services operate (context)
- Modbus (8 or 5) function should not be used from the specific Eng Wks
  – Process/Authorisation Issue (context)
  – No change scheduled (context)
  – RTUs used control relays (risk)
- Protection relays alerting
  – outage (alert)

©2020 Mandiant

Proven Strategies – Have a Plan

Develop and Practice – Incident Response Plan

NIST SP 800-61R2 – Figure 3-1. Incident Response Life Cycle

Playbook

©2020 Mandiant

Proven Strategies – Social (Build on Strengths)

"Ask more of the ICS Community, deliver more to them."

I am asking you to do more and for all the vendors on this meetup – we need to deliver more to the OT community and a significant part of that is **Education**

Cybersecurity and Infrastructure Security Agency (CISA) – Securing Industrial Controls Systems: A Unified Initiative

©2020 Mandiant

Recap

- **Don’t tackle everything at the same time – get rid of one noisy alert at a time**
- **More eyes (logs) – doesn't mean better sight (visibility)**
- **Expecting a tool to tell you what’s wrong is like – staring at the flashlight**
- **Proven Strategies**
  - Use standards
  - Shelve and rationalise alarms – the same approach for security alerts
  - Create usecases and practicing IRP (playbooks included)
  - Ask the right questions when choosing tools
  - Invest in cross training and education

©2020 Mandiant

*** Alarm Shelving Book** https://www.exida.com/ebooks/alarm-shelving-exida-ebook.pdf

Useful Links

ISA18.2-2016 Alarm Management Standard > aka **IEC 62682**

- https://www.isa.org/intech/201606standards/

ISA-TR18.2.2-2016 Alarm Identification and Rationalization

- https://www.isa.org/intech-plus/2017/november/beyond-alarm-management/
- https://www.rockwellautomation.com/resources/downloads/rockwellautomation/pdf/events/automation-fair/2011/psug/afpsug11_ed16.pdf
- https://en.wikipedia.org/wiki/Alarm_management
- https://www.fireeye.com/services/freeware.html
- https://www.automation.com/library/articles-white-papers/alarm-monitoring-management/keeping-the-peace-and-quiet
- https://www.exida.com/ebooks/alarm-shelving-exida-ebook.pdf

NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)

- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
  - Tuning, 2-3, 3-3, 3-4, 4-11, 5-10, 6-5, 7-6
- https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_Fact_Sheet_S508C.pdf
- Chris Sistrunk: https://www.youtube.com/watch?v=OzRIF_mYEZk

©2020 Mandiant

References

Discussion / Interaction

Proven Strategies

- Use standards
- Shelve and rationalise alarms – the same approach for security alerts
- Create usecases and practicing IRP (playbooks included)
- Ask the right questions when choosing tools
- Invest in cross training and education