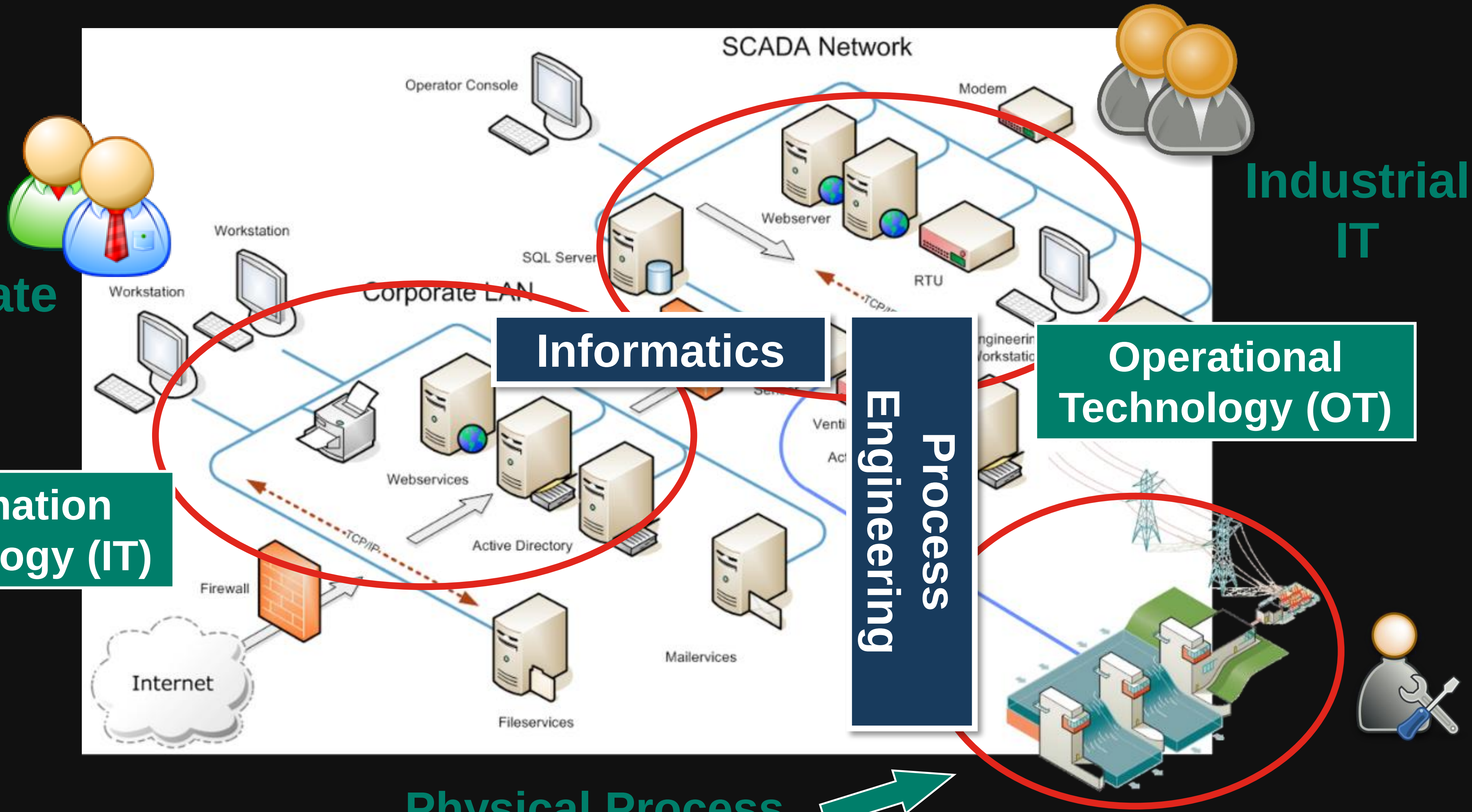
IT vs. OT: Comparing Process Control Room and SOC Operations

Marina Krotofil

COINS summer school on Security Applications, Lesbos, Greece (online)
14-18.06.2021

Industry 4.0 Horror: IT-OT Conversion



Corporate IT

Industrial IT

Informatics

Process Engineering

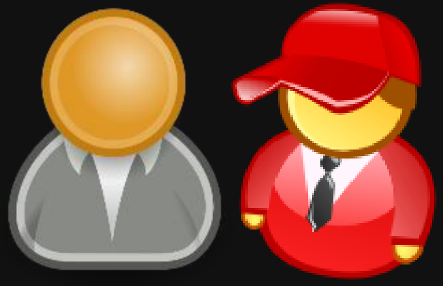
Operational Technology (OT)

Information Technology (IT)

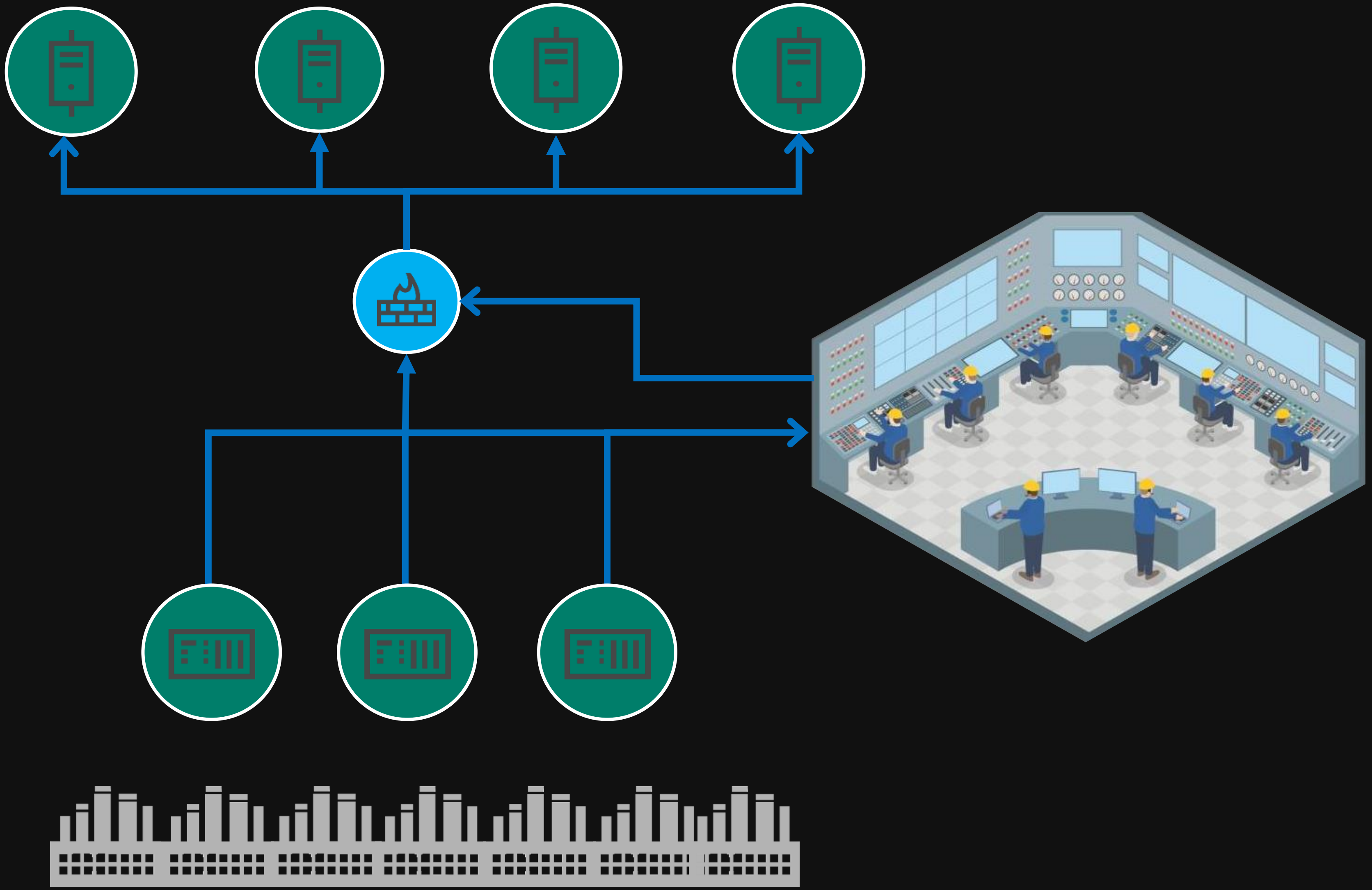
Physical Process

Frequent request from OT operators

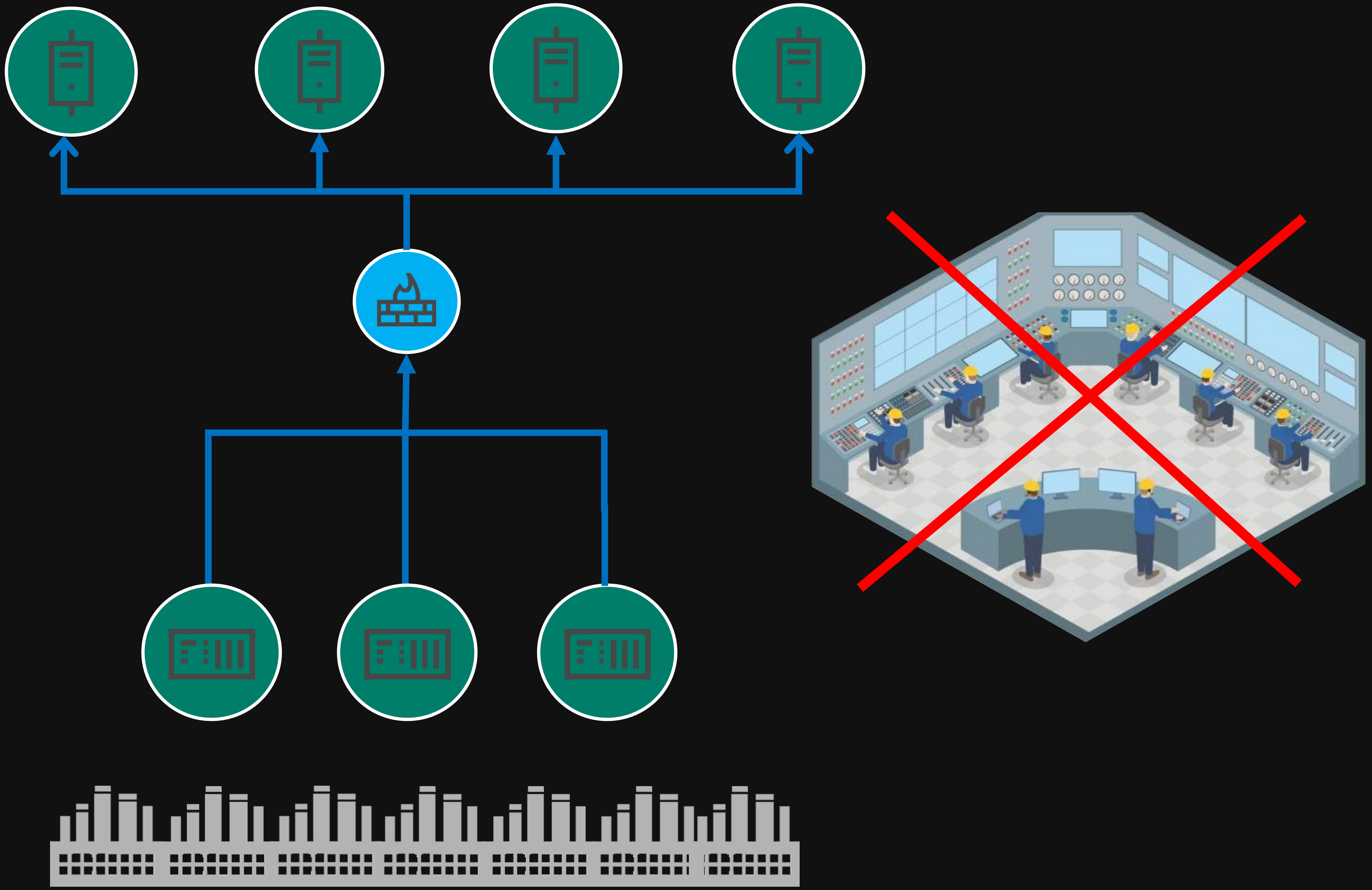
Could you please design an infrastructure in such secure way that no monitoring would be necessary (e.g., network monitoring, log collection & review) 🤞🙏



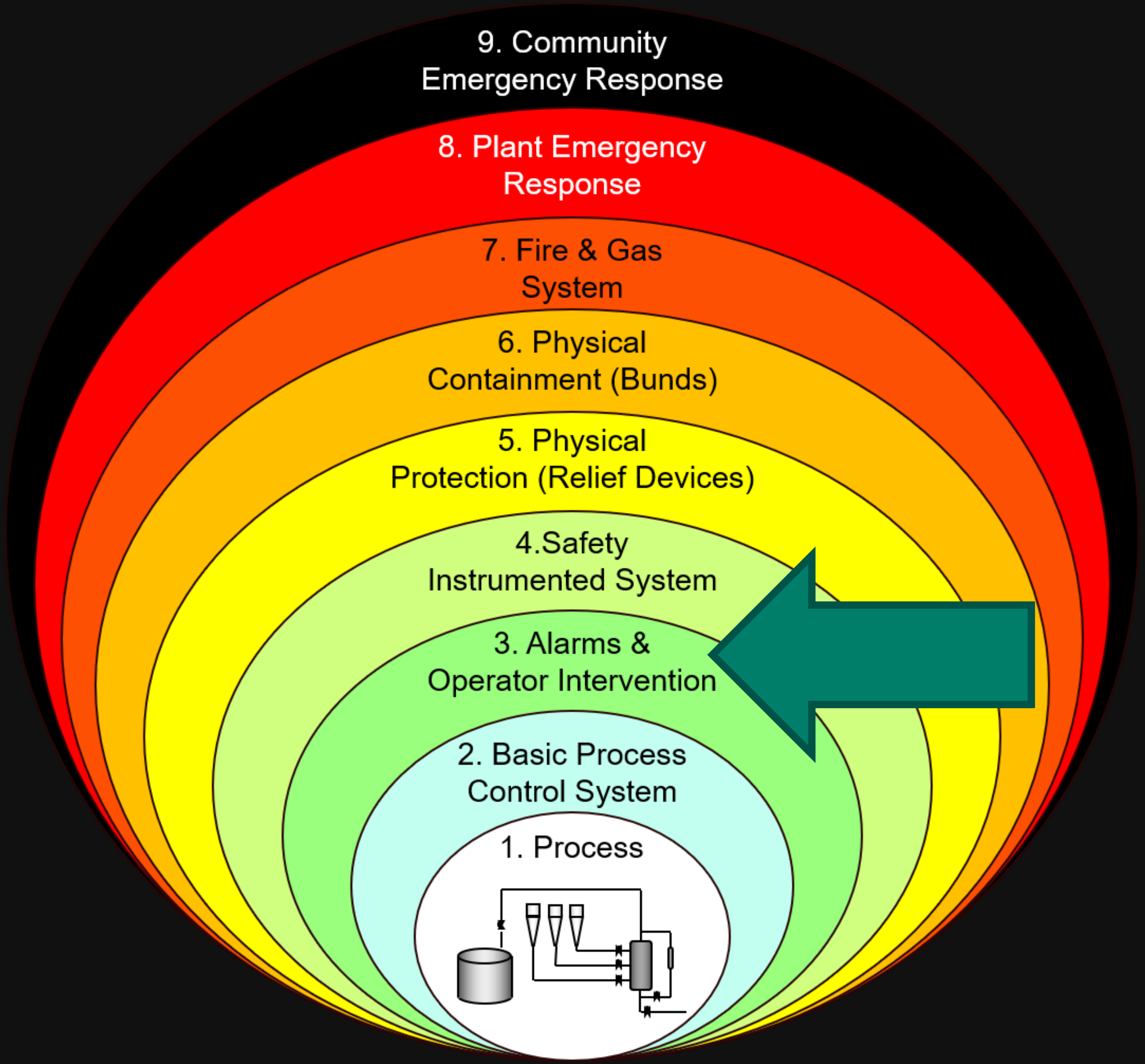
Argument back: 24/7 process monitoring



Argument back: 24/7 process monitoring



Layers of safety protections



9. Community Emergency Response

8. Plant Emergency Response

7. Fire & Gas System

6. Physical Containment (Bunds)

5. Physical Protection (Relief Devices)

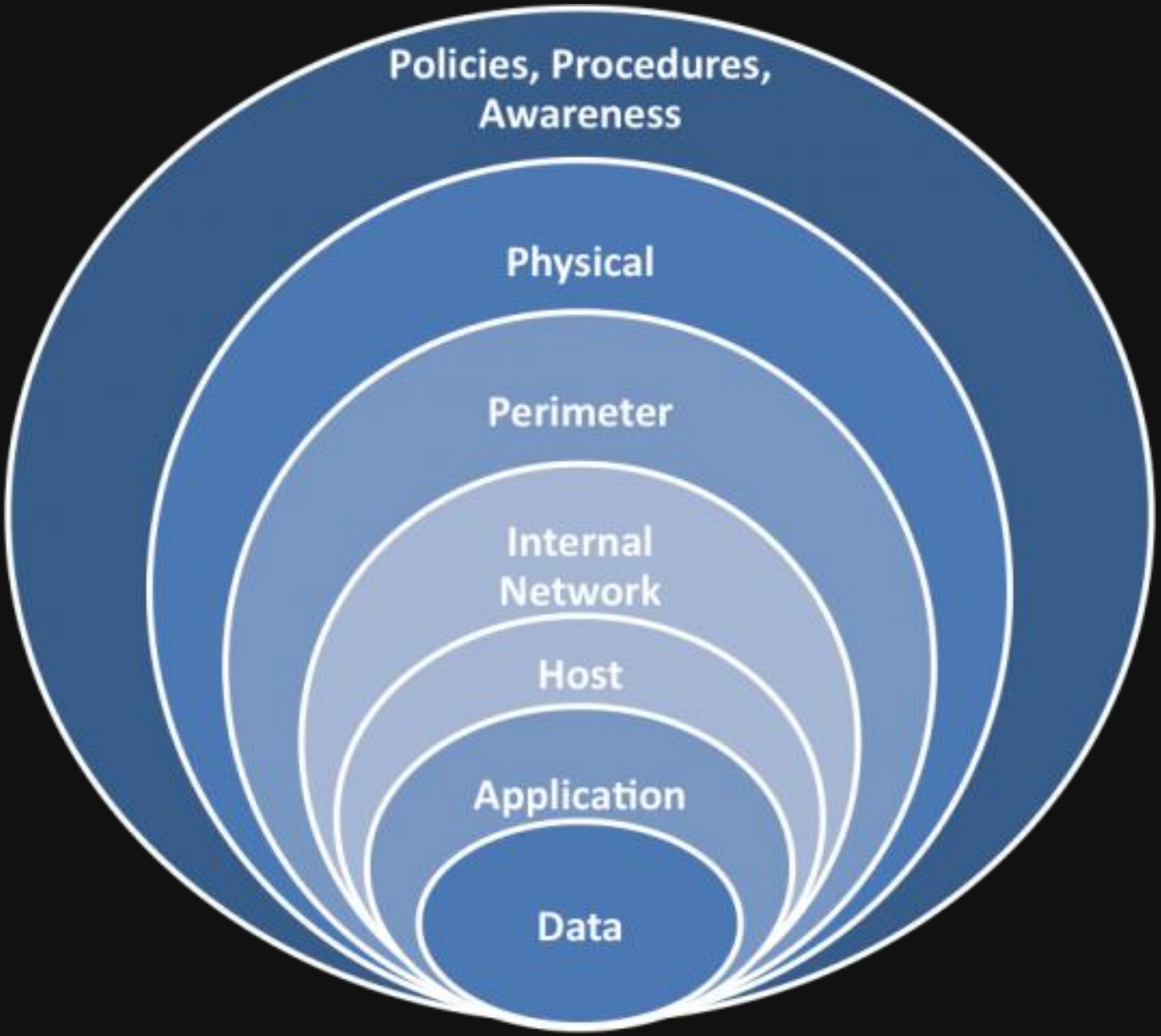
4.Safety Instrumented System

3. Alarms & Operator Intervention

2. Basic Process Control System

1. Process

Layers of security protections



https://commons.wikimedia.org/wiki/File:Video_tape_archive_(6498650083).jpg

Agenda

- SOC vs. Control Room
- IT vs. OT: Alarm tuning
- Corporate SOC vs. OT SOC

IT/OT convergence: SOC analyst and Control Room operator

IT / Analyst

OT / Operator

The only common discussion point?

Every day at work

https://habr.com/ru/company/croc/blog/353324/

https://en.wikipedia.org/wiki/Distributed_control_system#/media/File:Leitstand_2.jpg

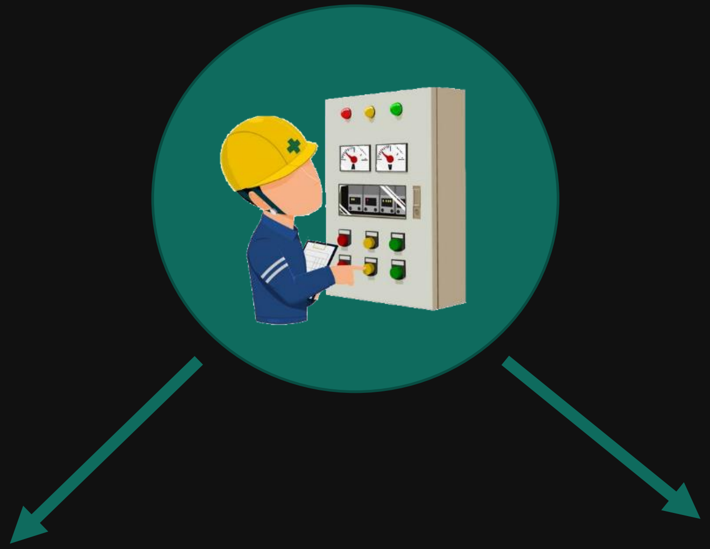
SOC vs. Control Room Operations

SOC analyst and Control Room operator

- Monitoring of IT infrastructure
- Reacts to **Alerts**
- Protects from threats
  (mostly human factor)
- Responsible for security
  - Confidentiality
  - Integrity
  - **Availability**
- Frequently outsourced
- Room for creativity in processes

- Monitoring of physical processes*
- Reacts to **Alarms**
- Protects from hazards
  (mostly natural causes factor)
- Responsible for safety
  - **Uptime**
  - Max of economic profit
  - (Safety and pollution)
- Mostly in-house
- Very standardized processes

*In some cases: Monitoring of supporting infrastructure



Physical process

Supporting infrastructure

SOC analyst and Control Room operator

- Monitoring of IT infrastructure
- Reacts to **Alerts**
- Protects from threats *(mostly human factor)*
- Responsible for security
  - **Confidentiality**
  - Integrity
  - **Availability**
- Frequently outsourced
- Room for creativity in processes

- Monitoring of physical processes*
- Reacts to **Alarms**
- Protects from hazards *(mostly natural causes factor)*
- Responsible for safety
  - **Uptime**
  - **Max of economic profit**
  - (Safety and pollution)
- Mostly in-house
- Very standardized processes

Alert vs. Alarm

- An **Alert** is a signal that draws attention to something. An alert state refers to a longer period of time during which increased attention remains in effect

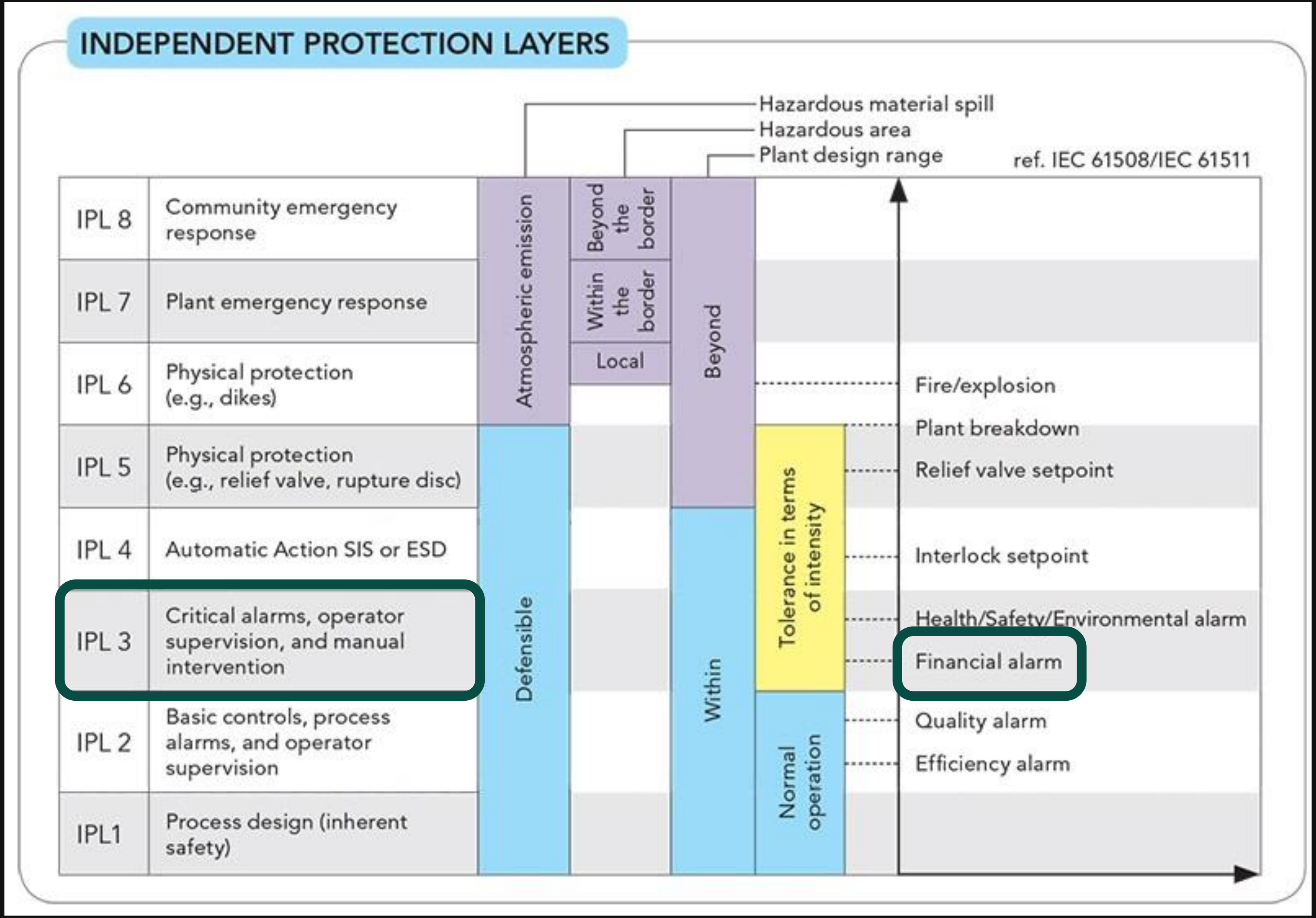
- An **Alarm** is a short warning that draws immediate attention to a danger. It usually does not refer to a longer period of time

SOC analyst and Control Room operator

- Monitoring of IT infrastructure
- Reacts to **Alerts**
- Protects from threats
  (mostly human factor)
- Responsible for security
  - Confidentiality
  - Integrity
  - **Availability**
- Frequently outsourced
- Room for creativity in processes

- Monitoring of physical processes*
- Reacts to **Alarms**
- Protects from hazards
  (mostly natural causes factor)
- Responsible for safety
  - **Uptime**
  - Max of economic profit
  - (Safety and pollution)
- Mostly in-house
- Very standardized processes

Safety Protection Layers: „Financial Alarms“

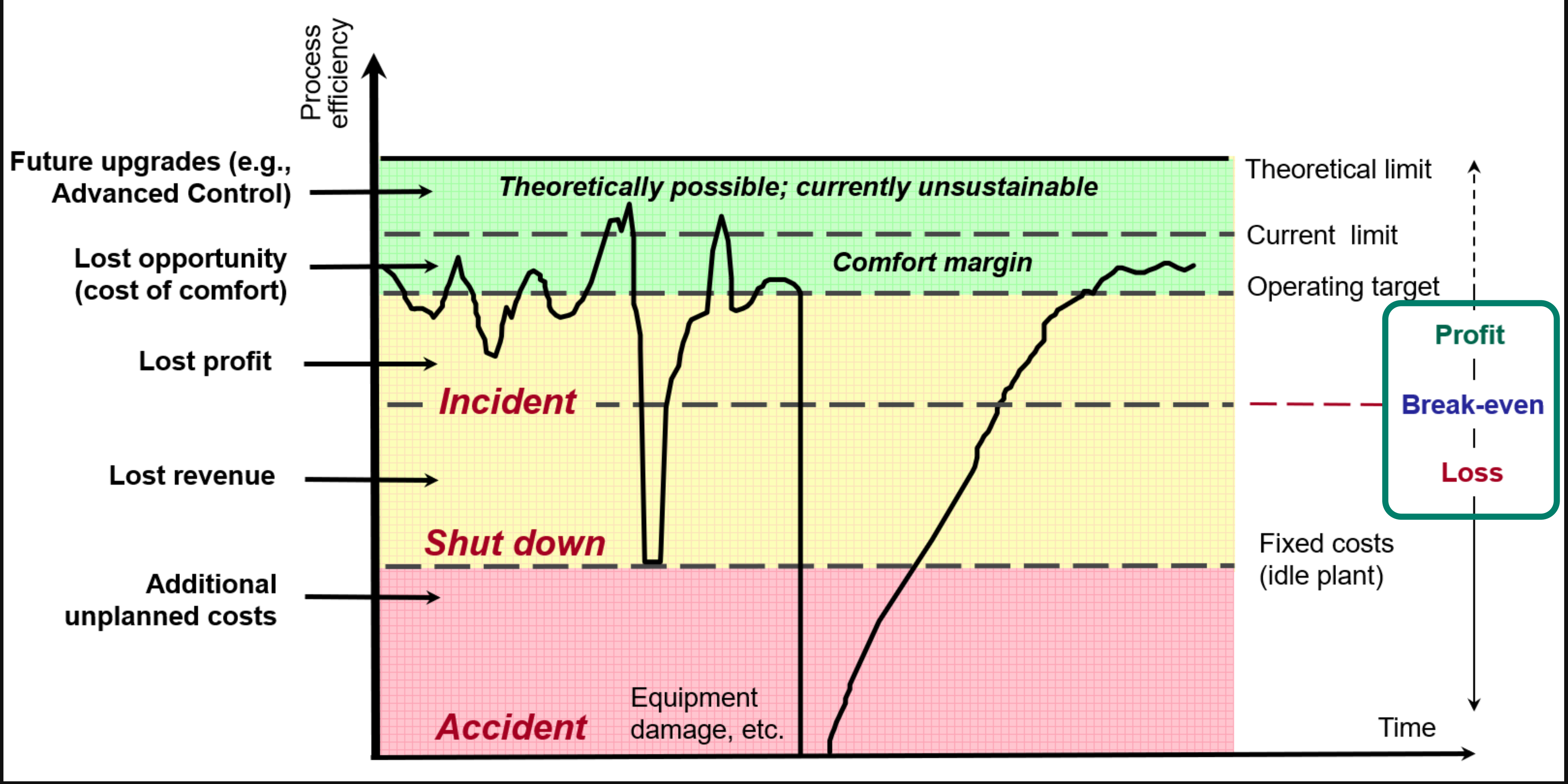


INDEPENDENT PROTECTION LAYERS

IPL 8	Community emergency response
IPL 7	Plant emergency response
IPL 6	Physical protection (e.g., dikes)
IPL 5	Physical protection (e.g., relief valve, rupture disc)
IPL 4	Automatic Action SIS or ESD
IPL 3	Critical alarms, operator supervision, and manual intervention
IPL 2	Basic controls, process alarms, and operator supervision
IPL1	Process design (inherent safety)

ref. IEC 61508/IEC 61511

Maximization of economic profit



https://www.slideserve.com/Antony/the-birth-of-asm

SOC analyst and Control Room operator

- Monitoring of IT infrastructure
- Reacts to **Alerts**
- Protects from threats
  (mostly human factor)
- Responsible for security
  - Confidentiality
  - Integrity
  - **Availability**
- Frequently outsourced
- Room for creativity in processes

- Monitoring of physical processes*
- Reacts to **Alarms**
- Protects from hazards
  (mostly natural causes factor)
- Responsible for safety
  - **Uptime**
  - Max of economic profit
  - (Safety and pollution)
- Mostly in-house
- Very standardized processes

Commonality: Novel Challenges

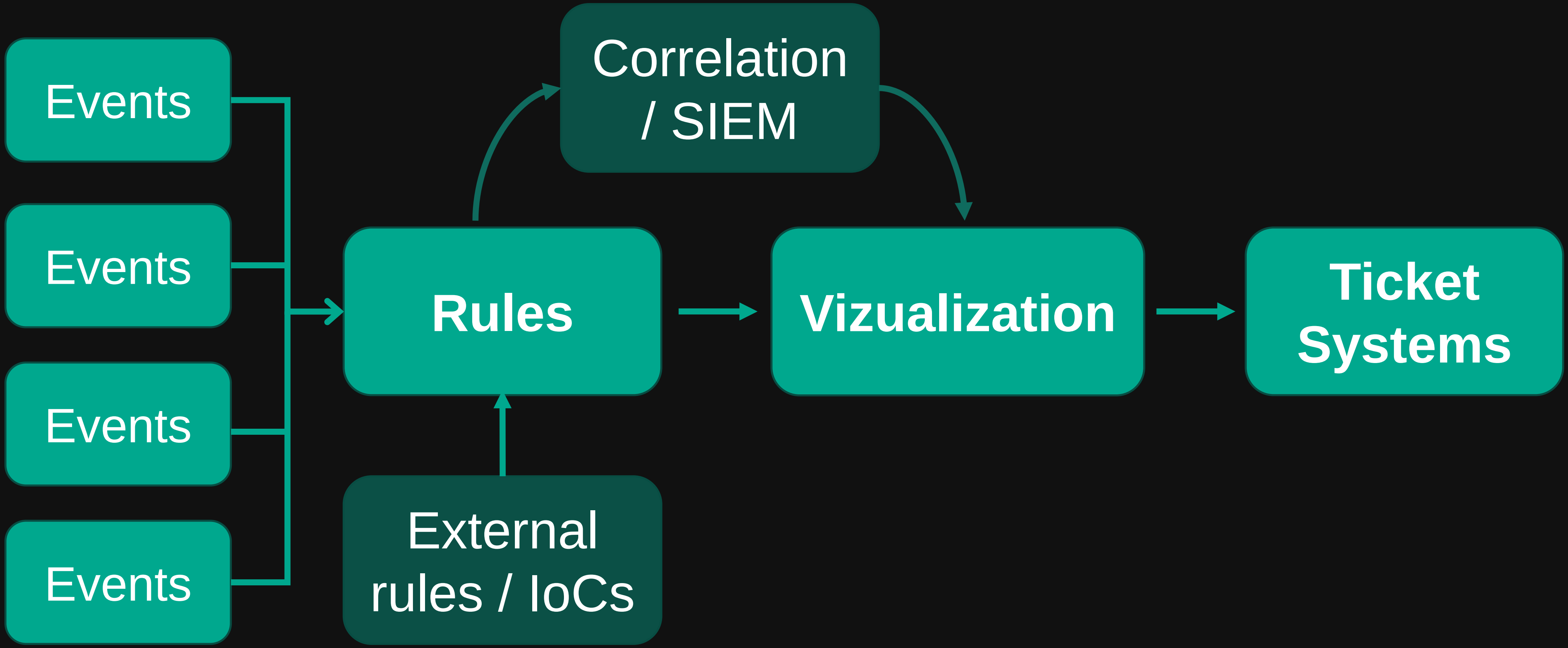
- Typical monitoring object
  - Security controls/infrastructure
- **Unforeseen events which invalidate security assumptions**
  Unexpected interdependencies due to infrastructure complexity

- Typical monitoring object
  - Physical process
- **Unforeseen events which invalidate safety assumptions**
  Unexpected process upsets due to human-in-the-system

Security Operations Center (SOC)

https://i2.wp.com/staging.gbhackers.com/wp-content/uploads/2017/01/BvJniTg-2.png?resize=1068%2C727&ssl=1

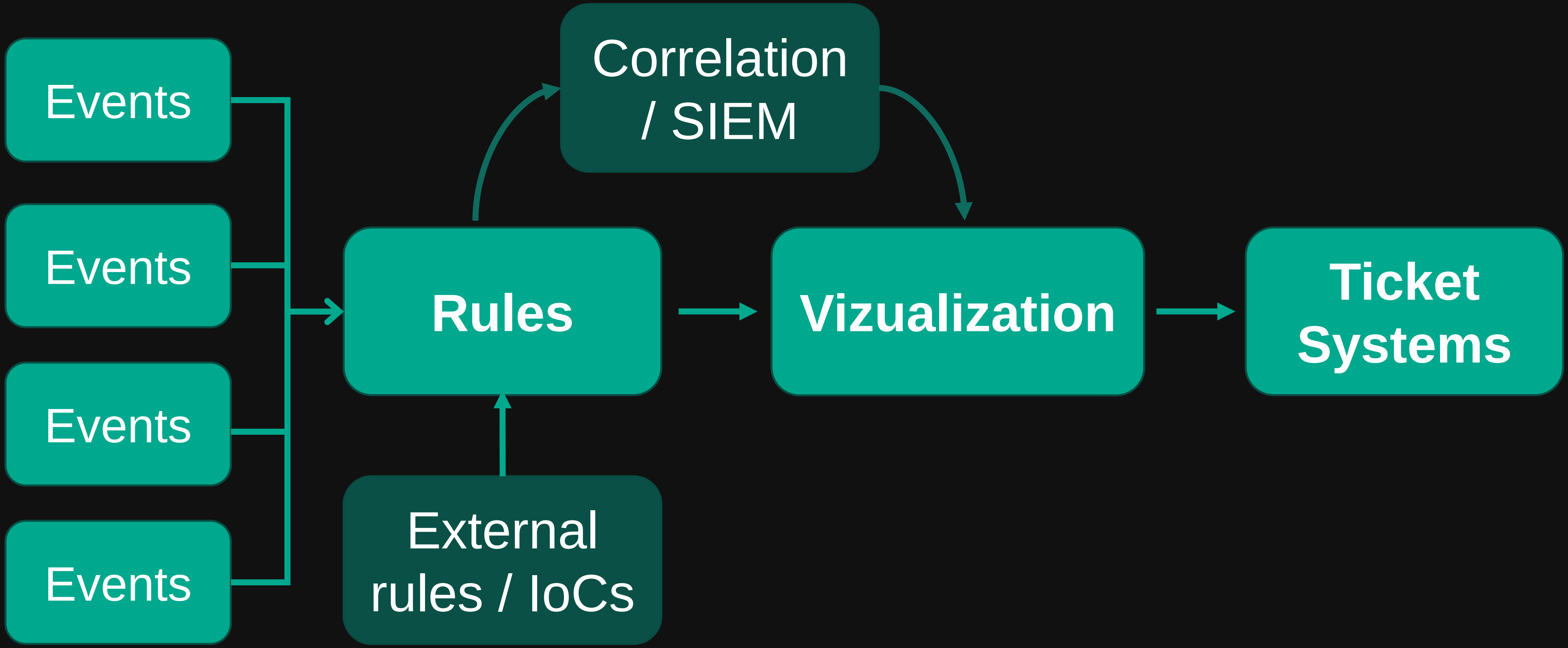
SOC: Typical components



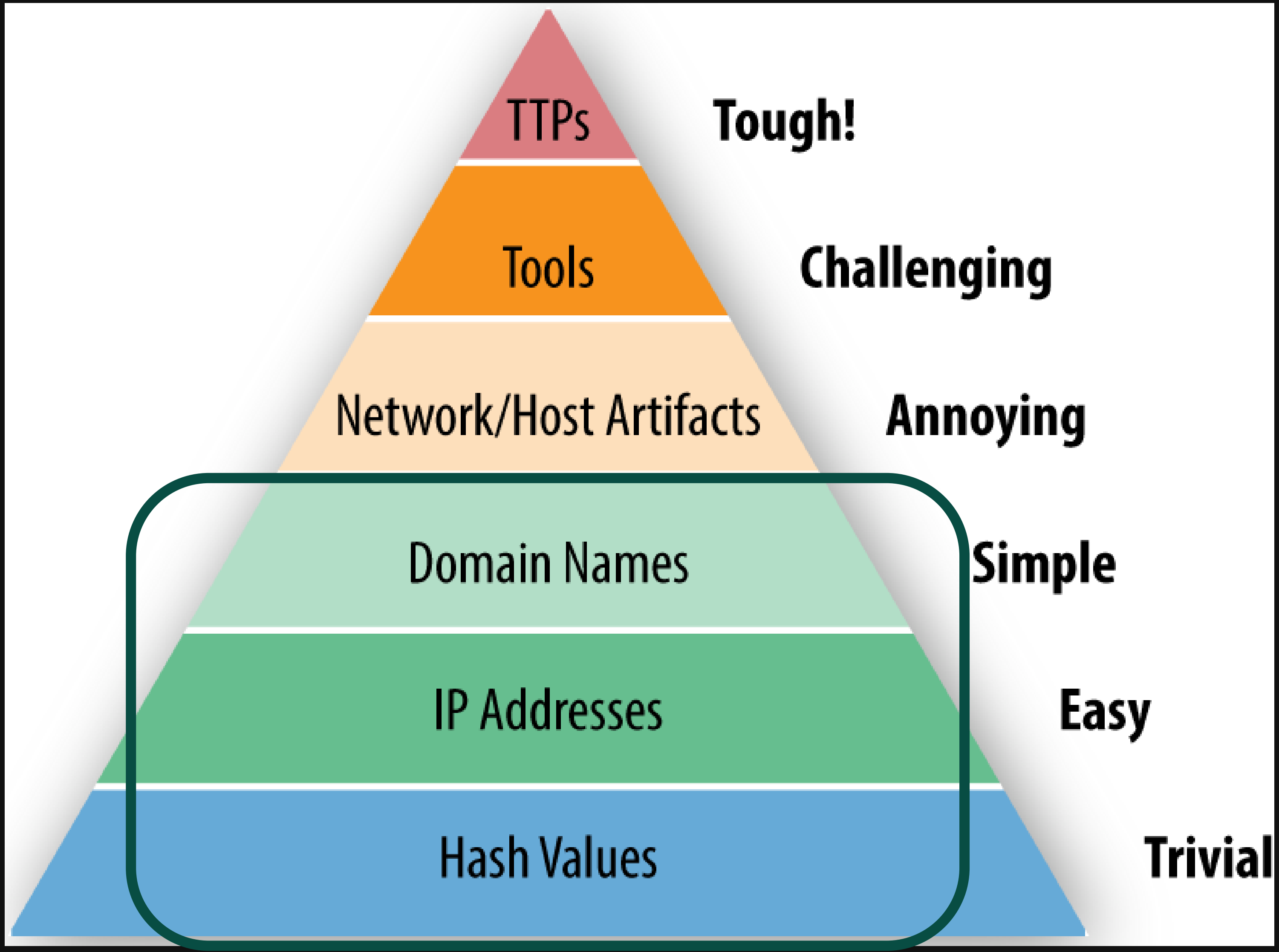
SOC: Sources of events

- Security infrastructure (endpoint security, IDPS, DLP, VPN, FW, honeypots, etc.)
- Network infrastructure (routers, switches, AP, DBs (SQL/Oracle, LDAP, Radius))
- Client endpoints (security and windows events, application logs)
- Web and email servers
- Servers (OS and application logs)
- Virtualization infrastructure
- Usage of user / service accounts
- Non-log information (asset inventory, vulnerability reports, network maps, configs)
- Etc.

SOC: Typical components

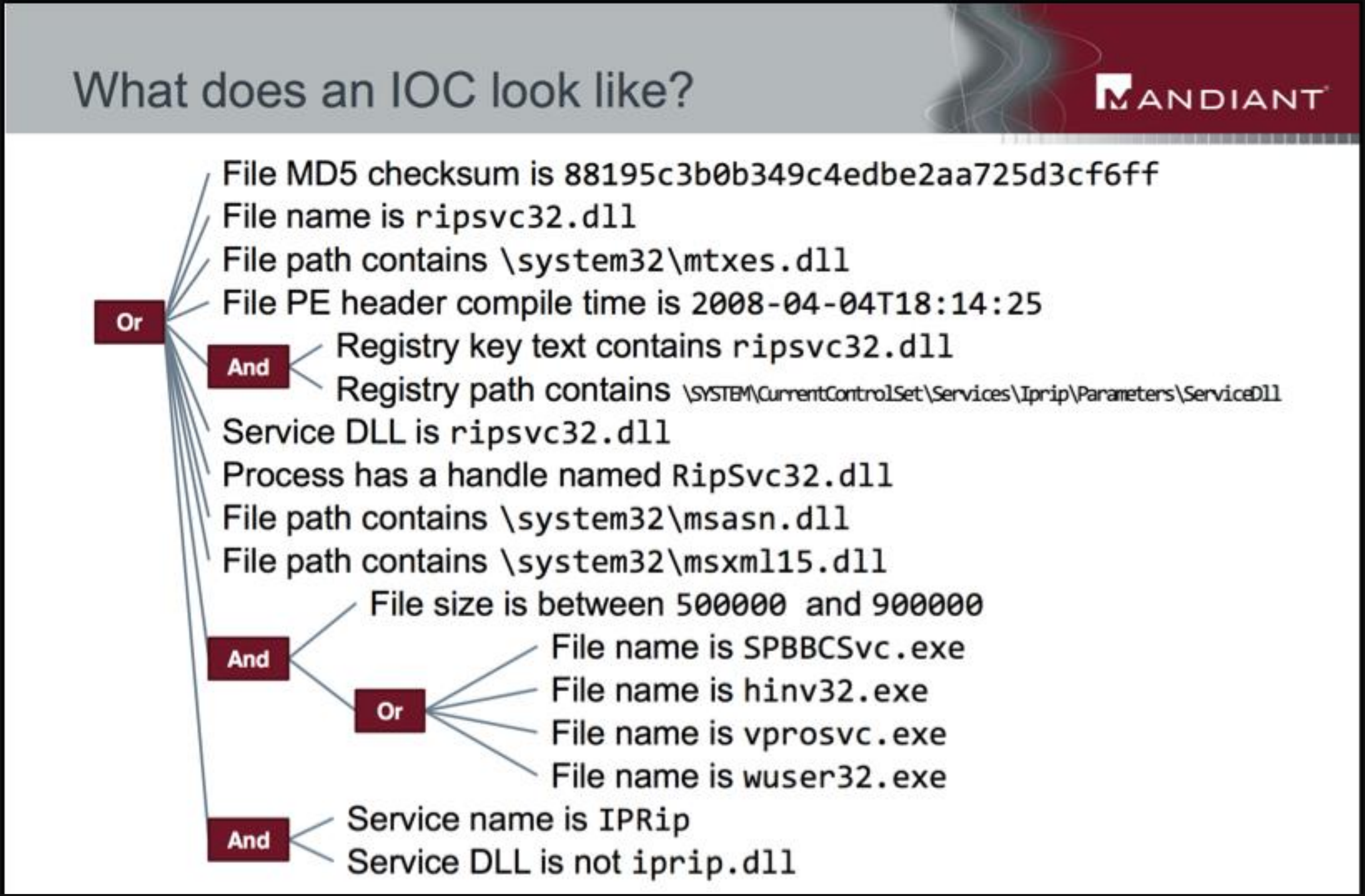


Detection rules: Pyramid of pain



https://www.oreilly.com/library/view/intelligence-driven-incident-response/9781491935187/ch04.html

Indicators of compromise

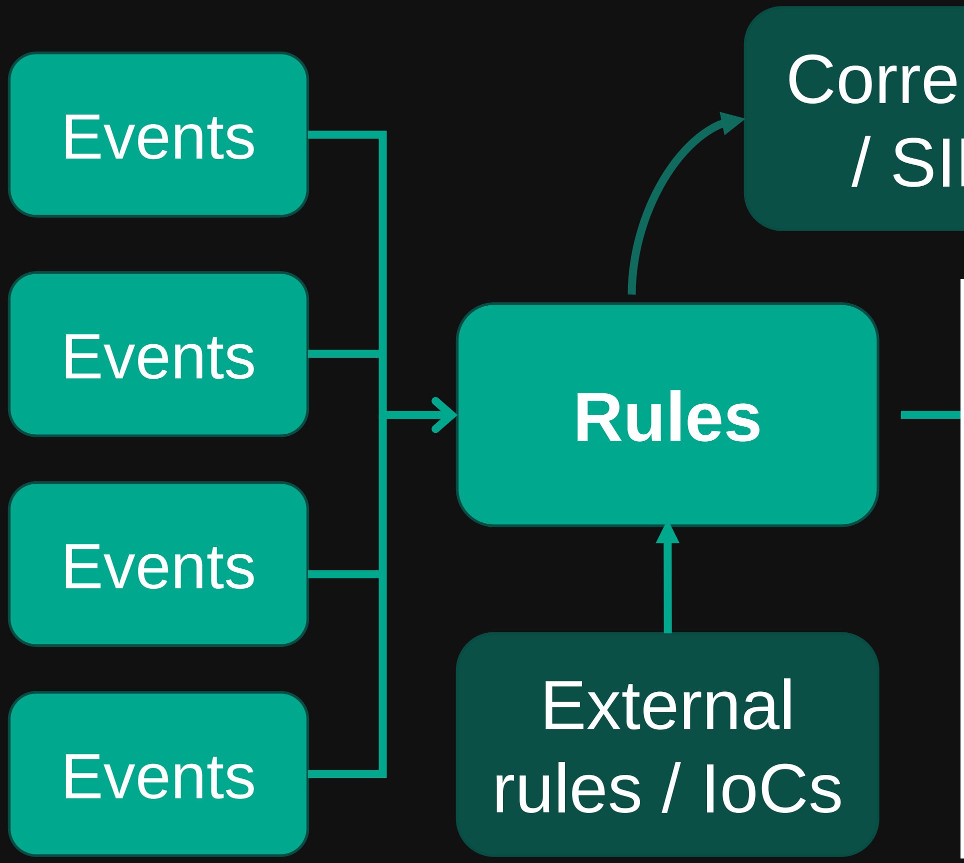


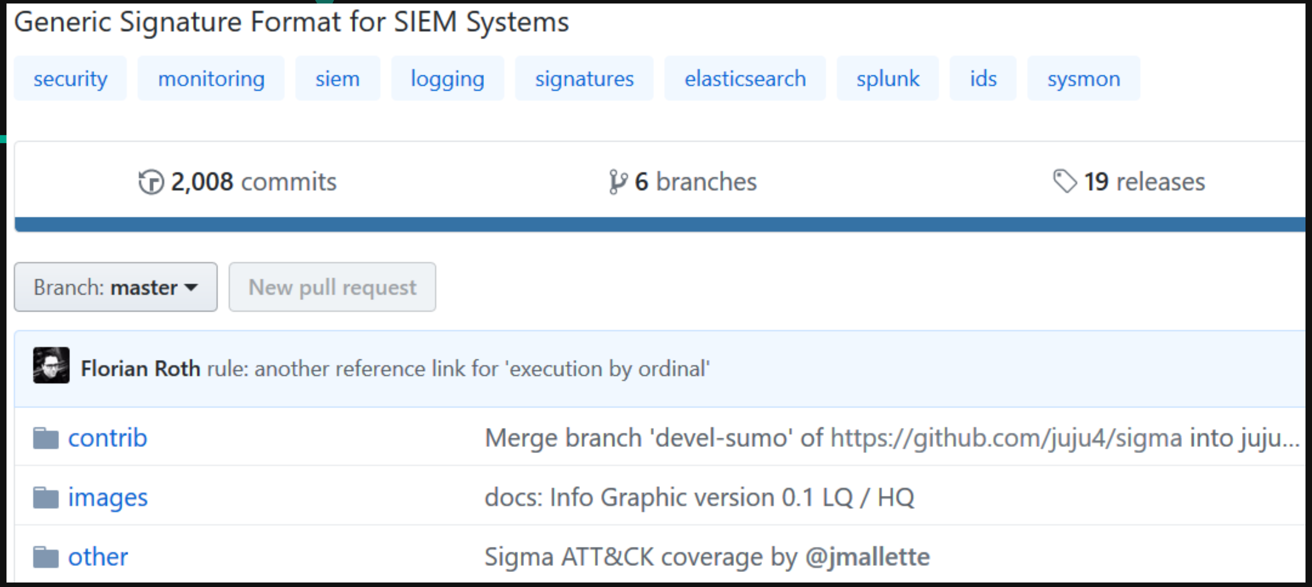
What does an IOC look like?

- Or
  - File MD5 checksum is 88195c3b0b349c4edbe2aa725d3cf6ff
  - File name is ripsvc32.dll
  - File path contains \system32\mtxes.dll
  - File PE header compile time is 2008-04-04T18:14:25
  - And
    - Registry key text contains ripsvc32.dll
    - Registry path contains \SYSTEM\CurrentControlSet\Services\Iprip\Parameters\ServiceDll
  - Service DLL is ripsvc32.dll
  - Process has a handle named RipSvc32.dll
  - File path contains \system32\msasn.dll
  - File path contains \system32\msxml15.dll
  - And
    - File size is between 500000 and 900000
    - Or
      - File name is SPBBCSvc.exe
      - File name is hinv32.exe
      - File name is vprosvc.exe
      - File name is wuser32.exe
  - And
    - Service name is IPRip
    - Service DLL is not iprip.dll

https://threatpost.com/misunderstanding-indicators-of-compromise/117560/

SOC: Typical components

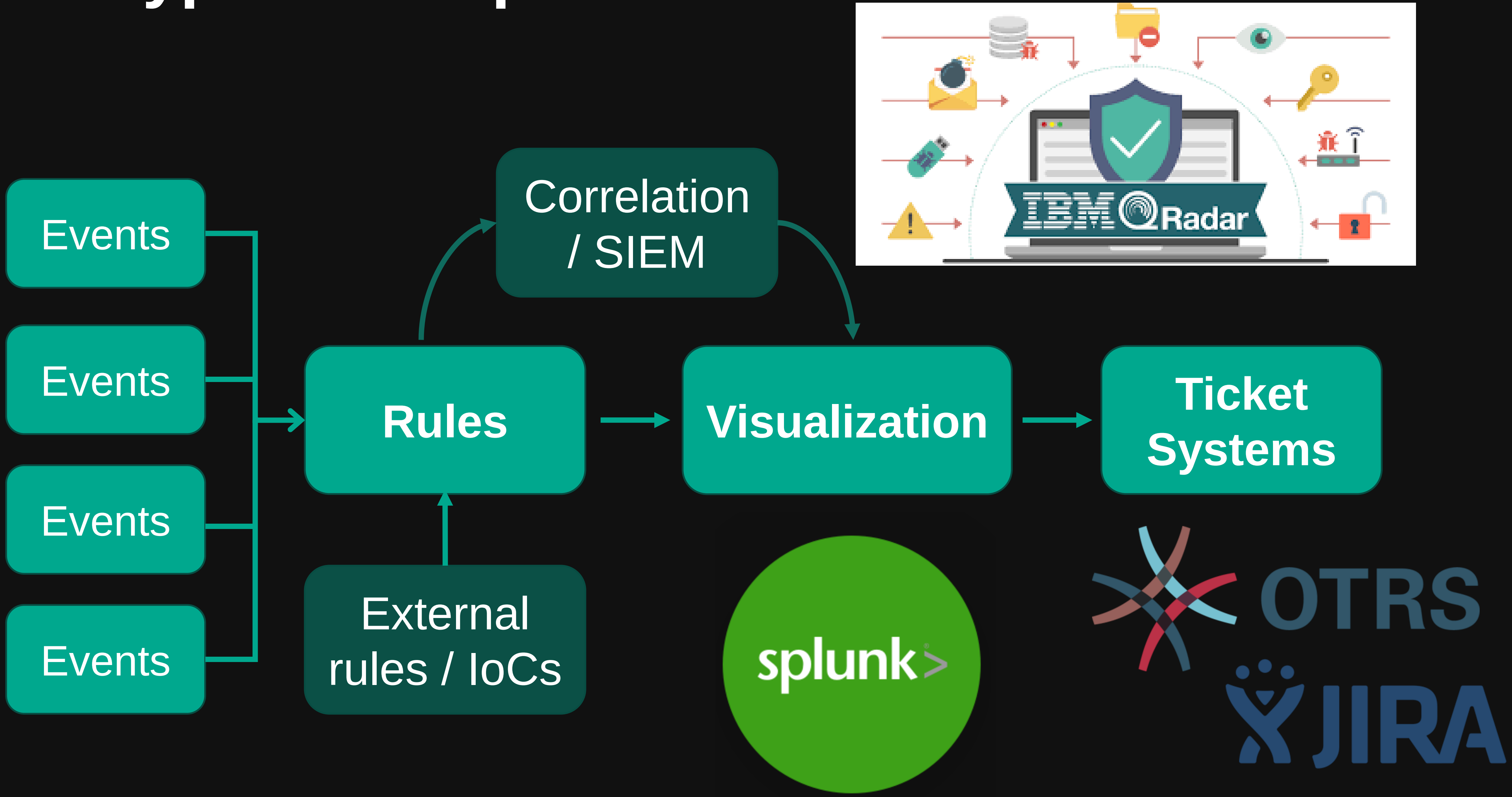



Generic Signature Format for SIEM Systems

Florian Roth rule: another reference link for 'execution by ordinal'

contrib	Merge branch 'devel-sumo' of https://github.com/juju4/sigma into juju...
images	docs: Info Graphic version 0.1 LQ / HQ
other	Sigma ATT&CK coverage by @jmallette

SOC: Typical components



Events

Events

Events

Events

Rules

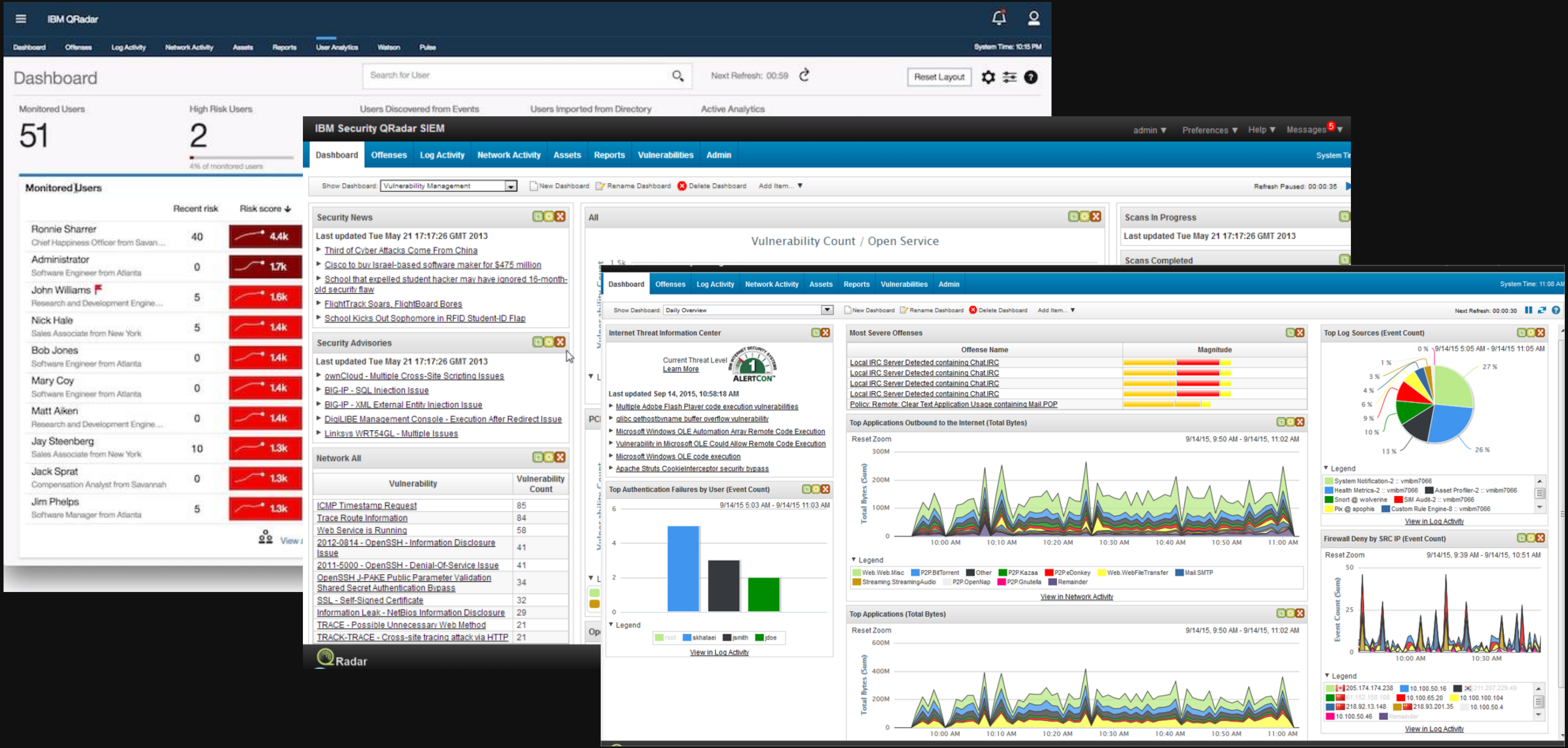
Correlation / SIEM

External rules / IoCs

Visualization

Ticket Systems

Correlation engine: Qradar (IBM)



Monitored Users

	Recent risk	Risk score ↓
Ronnie Sharrer Chief Happiness Officer from Savan...	40	4.4k
Administrator Software Engineer from Atlanta	0	1.7k
John Williams Research and Development Engine...	5	1.6k
Nick Hale Sales Associate from New York	5	1.4k
Bob Jones Software Engineer from Atlanta	0	1.4k
Mary Coy Software Engineer from Atlanta	0	1.4k
Matt Aiken Research and Development Engine...	0	1.4k
Jay Steenberg Sales Associate from New York	10	1.3k
Jack Sprat Compensation Analyst from Savannah	0	1.3k
Jim Phelps Software Manager from Atlanta	5	1.3k

Security News

Last updated Tue May 21 17:17:26 GMT 2013

- Third of Cyber Attacks Come From China
- Cisco to buy Israel-based software maker for $475 million
- School that expelled student hacker may have ignored 16-month-old security flaw
- FlightTrack Soars, FlightBoard Bores
- School Kicks Out Sophomore in RFID Student-ID Flap

Security Advisories

Last updated Tue May 21 17:17:26 GMT 2013

- ownCloud - Multiple Cross-Site Scripting Issues
- BIG-IP - SQL Injection Issue
- BIG-IP - XML External Entity Injection Issue
- DigiLIBE Management Console - Execution After Redirect Issue
- Linksys WRT54GL - Multiple Issues

Network All

Vulnerability	Vulnerability Count
ICMP Timestamp Request	85
Trace Route Information	84
Web Service is Running	58
2012-0814 - OpenSSH - Information Disclosure Issue	41
2011-5000 - OpenSSH - Denial-Of-Service Issue	41
OpenSSH J-PAKE Public Parameter Validation Shared Secret Authentication Bypass	34
SSL - Self-Signed Certificate	32
Information Leak - NetBios Information Disclosure	29
TRACE - Possible Unnecessary Web Method	21
TRACK-TRACE - Cross-site tracing attack via HTTP	21

Internet Threat Information Center

Last updated Sep 14, 2015, 10:58:18 AM

- Multiple Adobe Flash Player code execution vulnerabilities
- glibc gethostbyname buffer overflow vulnerability
- Microsoft Windows OLE Automation Array Remote Code Execution
- Vulnerability in Microsoft OLE Could Allow Remote Code Execution
- Microsoft Windows OLE code execution
- Apache Struts CookieInterceptor security bypass

Top Authentication Failures by User (Event Count)

Most Severe Offenses

Offense Name	Magnitude
Local IRC Server Detected containing Chat.IRC	
Local IRC Server Detected containing Chat.IRC	
Local IRC Server Detected containing Chat.IRC	
Local IRC Server Detected containing Chat.IRC	
Policy: Remote: Clear Text Application Usage containing Mail.POP	

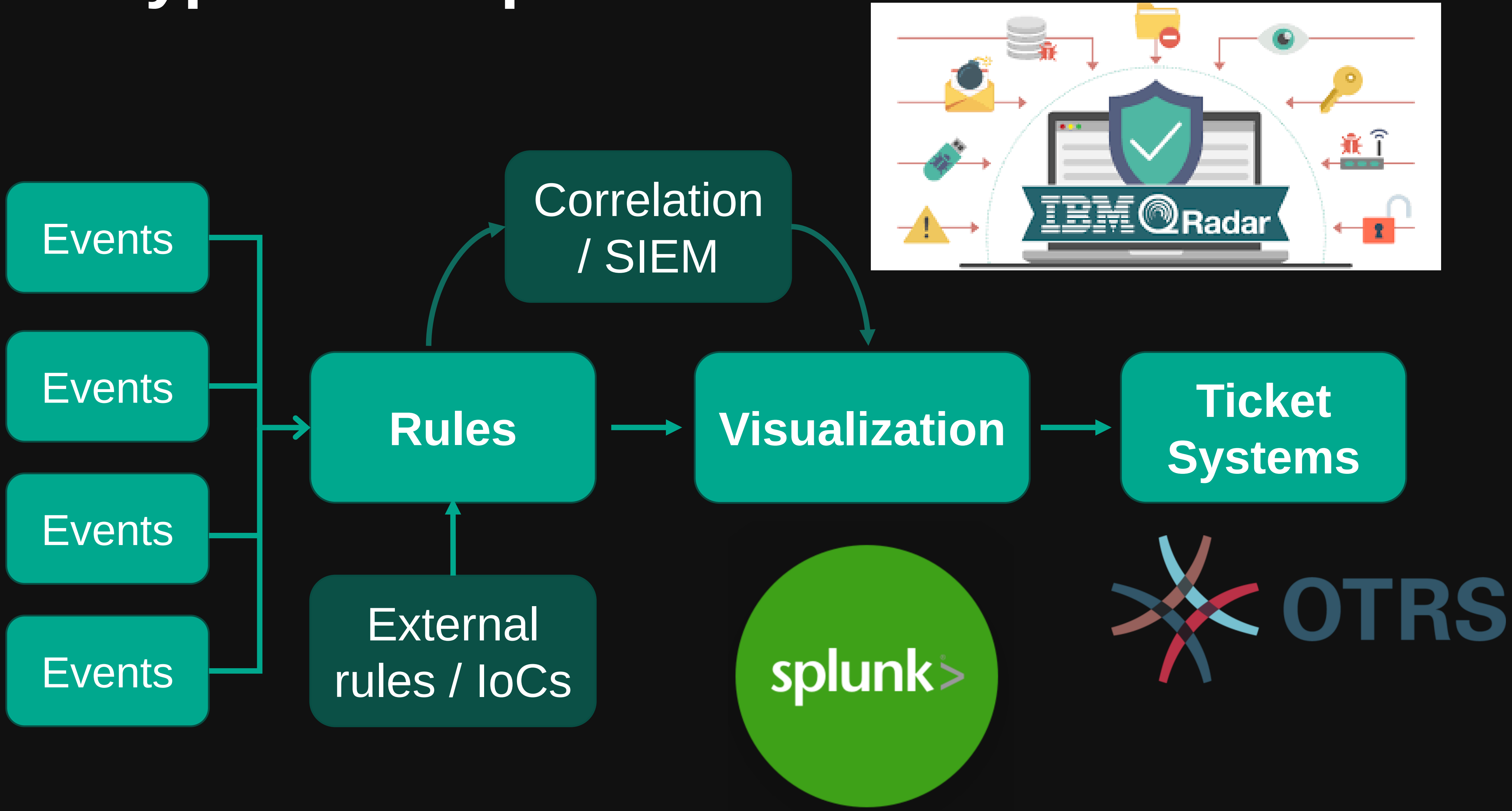
Top Applications Outbound to the Internet (Total Bytes)

Top Applications (Total Bytes)

Top Log Sources (Event Count)

Firewall Deny by SRC IP (Event Count)

SOC: Typical components



Events

Events

Events

Events

Rules

External rules / IoCs

Correlation / SIEM

Visualization

Ticket Systems

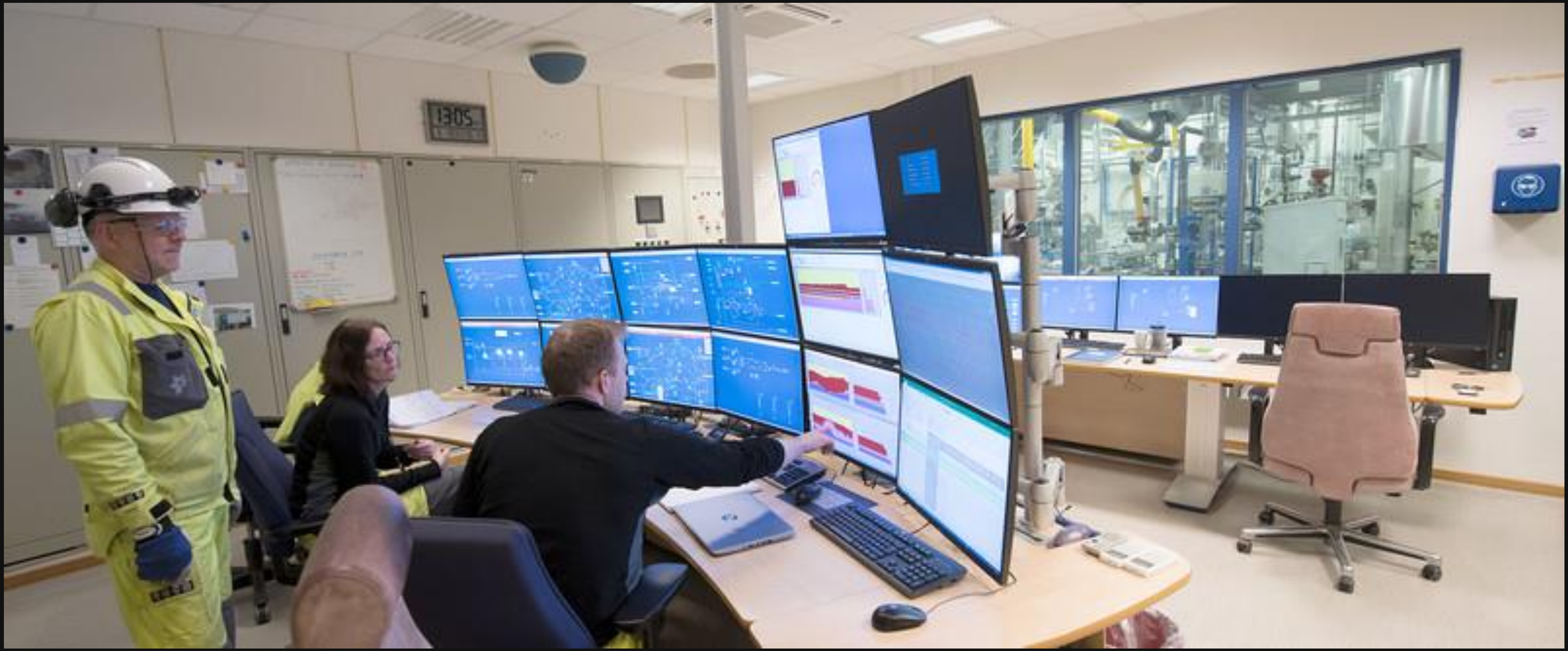
SOC: “Tiers of Ticket Response”

Distribution of responsibilities between tiers may vary:

- Tier 1 – Alert analyst (frequently outsourced)
- Tier 2 – Incident Responder (sometimes outsourced)
- Tier 3 – Subject Matter Expert/ Hunter
  - SOC Engineer
  - Incident responder
  - Reverse engineer
  - Threat intelligence analyst

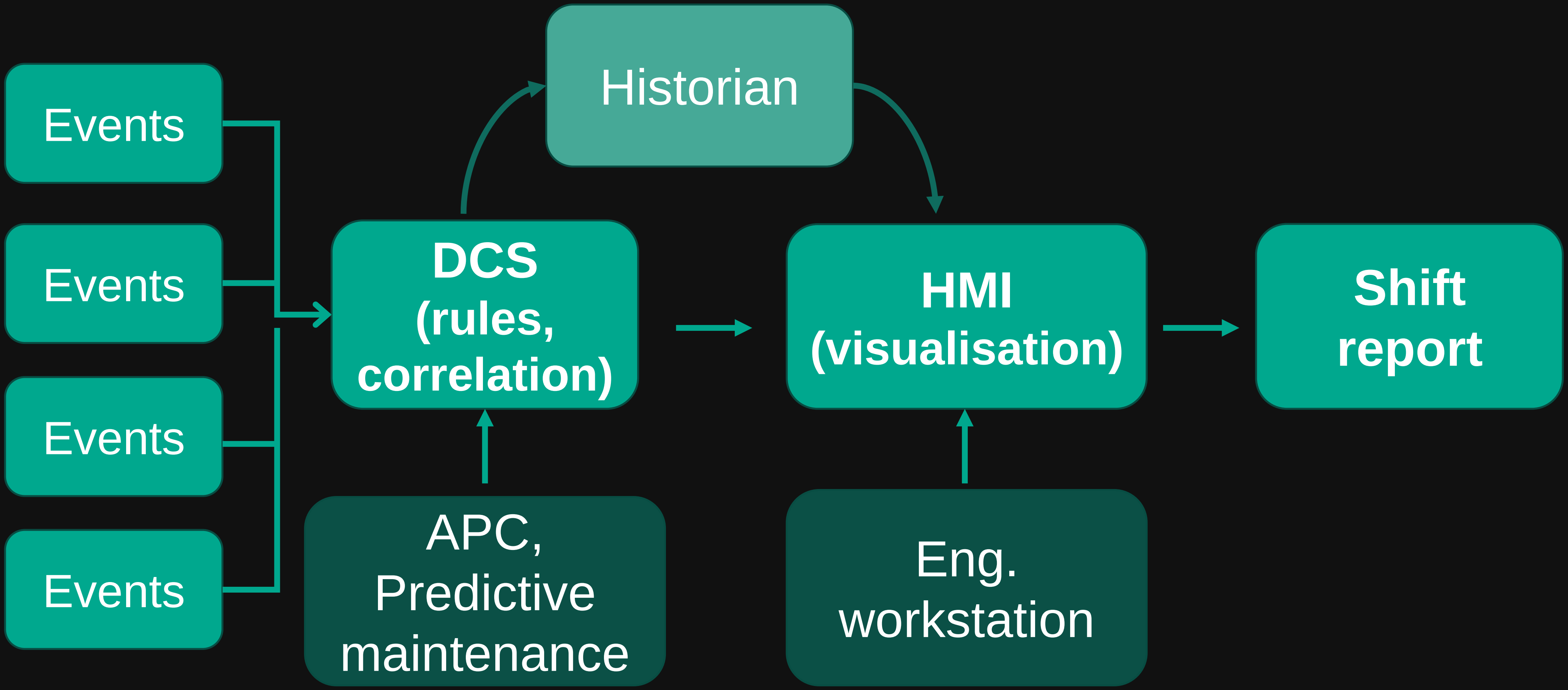
Responce times for each tier are defined by SLAs

Control Room in an industrial plant



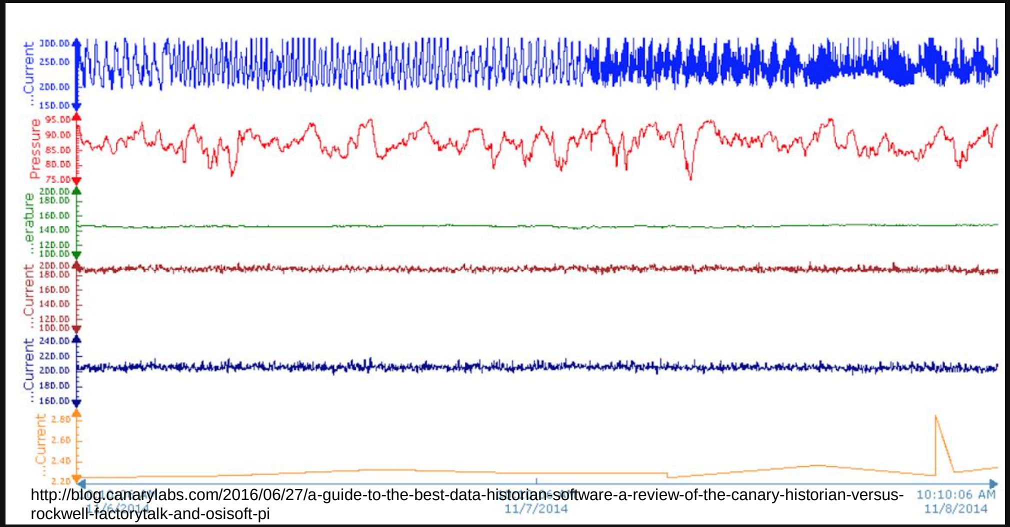
https://eng.heroya-industripark.no/var/site/storage/images/media/images/statoil2/statoil-kontrollrom/67513-1-nor-NO/statoil-kontrollrom_size-medium.jpg

Control room: Typical components

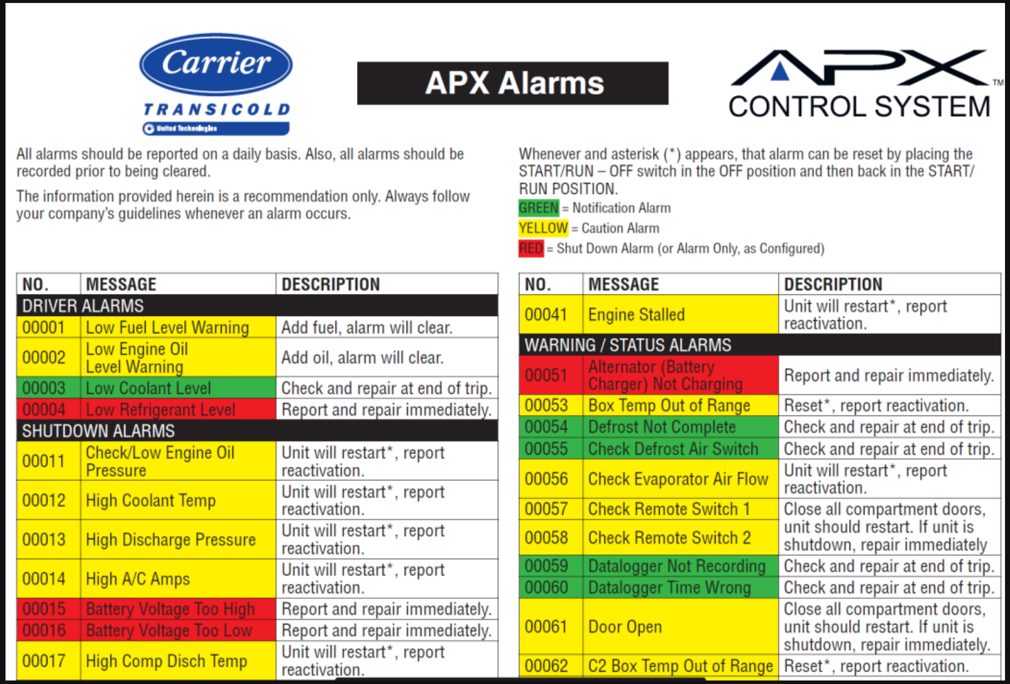


OT: Sources of data

- **Process data**
  - Process measurements
  - Pre-alarm, low (LL) / high (HH) limits
  - Rate of change
- Equipment status, diagnostics
- Safety systems
- Alarms from packaged units
- F&G systems
- Video surveillance feed



http://blog.canarylabs.com/2016/06/27/a-guide-to-the-best-data-historian-software-a-review-of-the-canary-historian-versus-rockwell-factorytalk-and-osisoft-pi



Carrier TRANSICOLD United Technologies

APX Alarms

APX CONTROL SYSTEM™

All alarms should be reported on a daily basis. Also, all alarms should be recorded prior to being cleared.

The information provided herein is a recommendation only. Always follow your company's guidelines whenever an alarm occurs.

Whenever and asterisk (*) appears, that alarm can be reset by placing the START/RUN – OFF switch in the OFF position and then back in the START/RUN POSITION.

🟩 GREEN = Notification Alarm

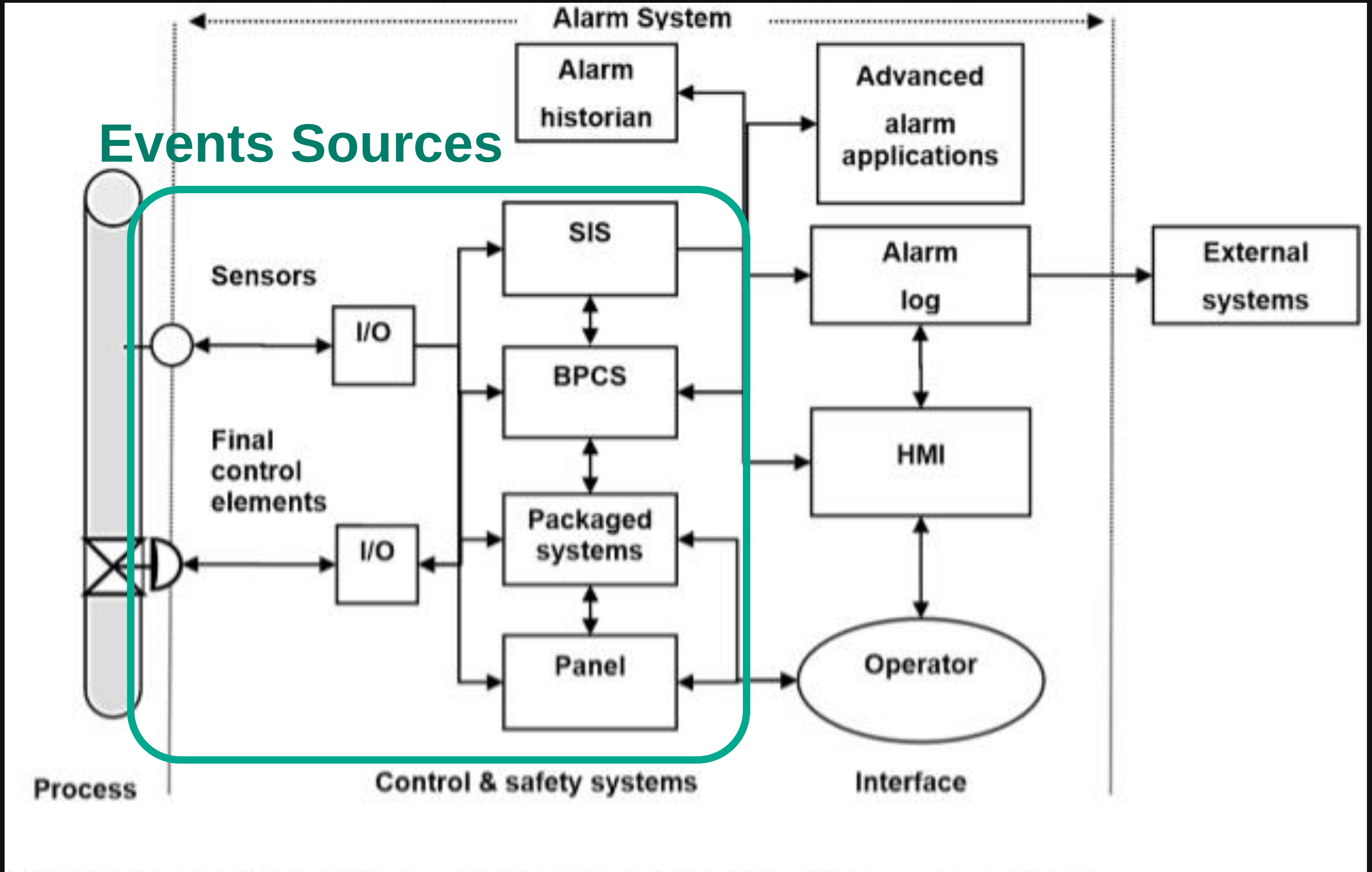
🟨 YELLOW = Caution Alarm

🟥 RED = Shut Down Alarm (or Alarm Only, as Configured)

NO.	MESSAGE	DESCRIPTION
DRIVER ALARMS		
🟨 00001	Low Fuel Level Warning	Add fuel, alarm will clear.
🟨 00002	Low Engine Oil Level Warning	Add oil, alarm will clear.
🟩 00003	Low Coolant Level	Check and repair at end of trip.
🟥 00004	Low Refrigerant Level	Report and repair immediately.
SHUTDOWN ALARMS		
🟨 00011	Check/Low Engine Oil Pressure	Unit will restart*, report reactivation.
🟨 00012	High Coolant Temp	Unit will restart*, report reactivation.
🟨 00013	High Discharge Pressure	Unit will restart*, report reactivation.
🟨 00014	High A/C Amps	Unit will restart*, report reactivation.
🟥 00015	Battery Voltage Too High	Report and repair immediately.
🟥 00016	Battery Voltage Too Low	Report and repair immediately.
🟨 00017	High Comp Disch Temp	Unit will restart*, report reactivation.

NO.	MESSAGE	DESCRIPTION
🟨 00041	Engine Stalled	Unit will restart*, report reactivation.
WARNING / STATUS ALARMS		
🟥 00051	Alternator (Battery Charger) Not Charging	Report and repair immediately.
🟨 00053	Box Temp Out of Range	Reset*, report reactivation.
🟩 00054	Defrost Not Complete	Check and repair at end of trip.
🟩 00055	Check Defrost Air Switch	Check and repair at end of trip.
🟨 00056	Check Evaporator Air Flow	Unit will restart*, report reactivation.
🟨 00057	Check Remote Switch 1	Close all compartment doors, unit should restart. If unit is shutdown, repair immediately
🟨 00058	Check Remote Switch 2	
🟩 00059	Datalogger Not Recording	Check and repair at end of trip.
🟩 00060	Datalogger Time Wrong	Check and repair at end of trip.
🟨 00061	Door Open	Close all compartment doors, unit should restart. If unit is shutdown, repair immediately.
🟨 00062	C2 Box Temp Out of Range	Reset*, report reactivation.

Control room: Events Sources

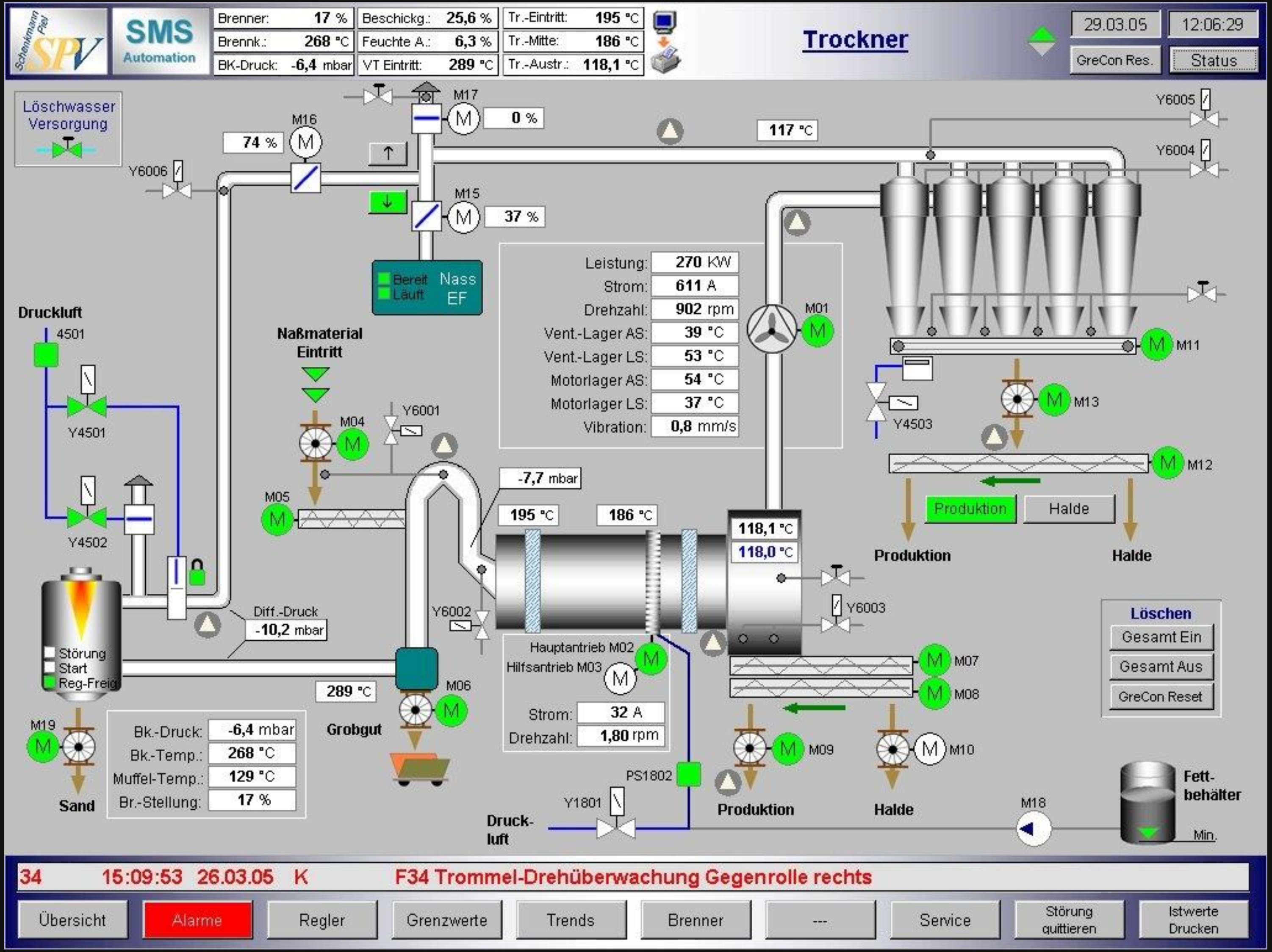


NOTE Other packaged systems (i.e., fire and gas systems) can be included in the control system.

Figure 1 – Alarm system dataflow

ANSI/ISA-18.2-2016 Management of Alarm Systems for the Process Industries

Visualization: Human Machine Interface (HMI)



Brenner: 17 %
Brennk.: 268 °C
BK-Druck: -6,4 mbar
Beschickg.: 25,6 %
Feuchte A.: 6,3 %
VT Eintritt: 289 °C
Tr.-Eintritt: 195 °C
Tr.-Mitte: 186 °C
Tr.-Austr.: 118,1 °C

Trockner

29.03.05 12:06:29

Leistung: 270 KW
Strom: 611 A
Drehzahl: 902 rpm
Vent.-Lager AS: 39 °C
Vent.-Lager LS: 53 °C
Motorlager AS: 54 °C
Motorlager LS: 37 °C
Vibration: 0,8 mm/s

Hauptantrieb M02
Hilfsantrieb M03
Strom: 32 A
Drehzahl: 1,80 rpm

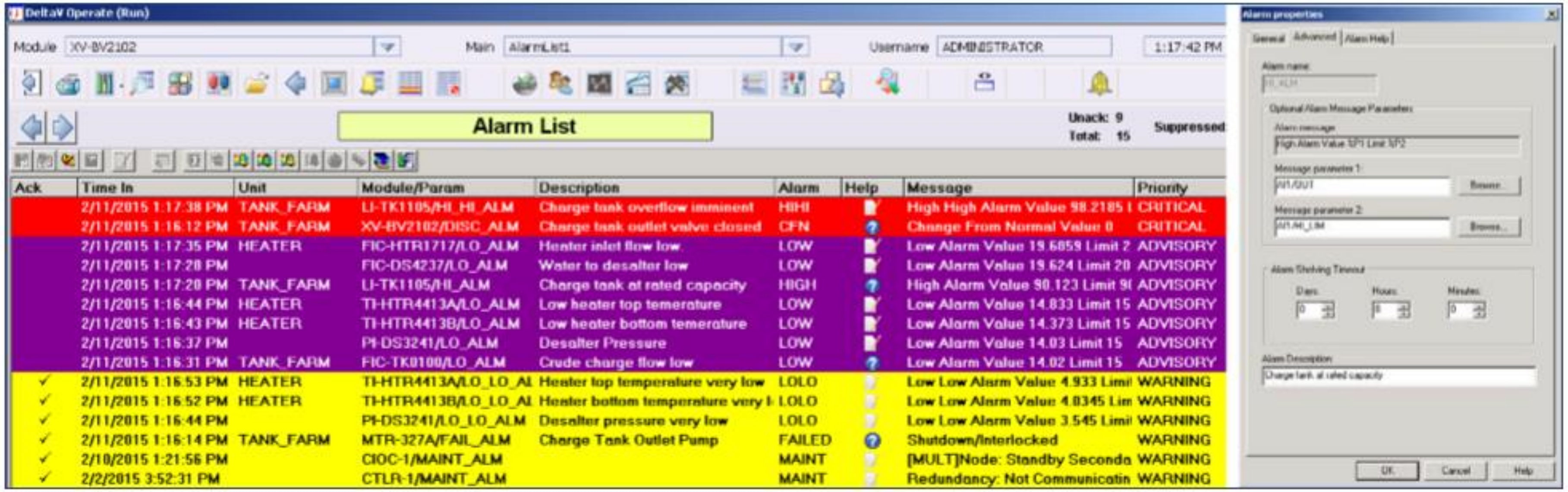
Bk.-Druck: -6,4 mbar
Bk.-Temp.: 268 °C
Muffel-Temp.: 129 °C
Br.-Stellung: 17 %

Diff.-Druck -10,2 mbar

34 15:09:53 26.03.05 K F34 Trommel-Drehüberwachung Gegenrolle rechts

https://1.bp.blogspot.com/-4f6UFLToOpI/Ti3jII9fLzI/AAAAAAAAAYY/oQXHuuAr2c8/s1600/wincc-flexible-runtime-screen-02-1024.jpg

HMI alarms



Module XV-BV2102

Main AlarmList1

Username ADMINISTRATOR

1:17:42 PM

Unack: 9
Total: 15

Suppressed

Ack	Time In	Unit	Module/Param	Description	Alarm	Help	Message	Priority
	2/11/2015 1:17:38 PM	TANK_FARM	LI-TK1105/HI_HI_ALM	Charge tank overflow imminent	HIHI	📄	High High Alarm Value 98.2185 l	CRITICAL
	2/11/2015 1:16:12 PM	TANK_FARM	XV-BV2102/DISC_ALM	Charge tank outlet valve closed	CFN	?	Change From Normal Value 0	CRITICAL
	2/11/2015 1:17:35 PM	HEATER	FIC-HTR1717/LO_ALM	Heater inlet flow low	LOW	📄	Low Alarm Value 19.6859 Limit 2	ADVISORY
	2/11/2015 1:17:28 PM		FIC-DS4237/LO_ALM	Water to desalter low	LOW	📄	Low Alarm Value 19.624 Limit 20	ADVISORY
	2/11/2015 1:17:20 PM	TANK_FARM	LI-TK1105/HI_ALM	Charge tank at rated capacity	HIGH	?	High Alarm Value 90.123 Limit 9(	ADVISORY
	2/11/2015 1:16:44 PM	HEATER	TI-HTR4413A/LO_ALM	Low heater top temerature	LOW	📄	Low Alarm Value 14.833 Limit 15	ADVISORY
	2/11/2015 1:16:43 PM	HEATER	TI-HTR4413B/LO_ALM	Low heater bottom temerature	LOW	📄	Low Alarm Value 14.373 Limit 15	ADVISORY
	2/11/2015 1:16:37 PM		PI-DS3241/LO_ALM	Desalter Pressure	LOW	📄	Low Alarm Value 14.03 Limit 15	ADVISORY
	2/11/2015 1:16:31 PM	TANK_FARM	FIC-TK0100/LO_ALM	Crude charge flow low	LOW	?	Low Alarm Value 14.02 Limit 15	ADVISORY
✓	2/11/2015 1:16:53 PM	HEATER	TI-HTR4413A/LO_LO_Al	Heater top temperature very low	LOLO		Low Low Alarm Value 4.933 Limi	WARNING
✓	2/11/2015 1:16:52 PM	HEATER	TI-HTR4413B/LO_LO_Al	Heater bottom temperature very l	LOLO		Low Low Alarm Value 4.8345 Lim	WARNING
✓	2/11/2015 1:16:44 PM		PI-DS3241/LO_LO_ALM	Desalter pressure very low	LOLO		Low Low Alarm Value 3.545 Limi	WARNING
✓	2/11/2015 1:16:14 PM	TANK_FARM	MTR-327A/FAIL_ALM	Charge Tank Outlet Pump	FAILED	?	Shutdown/Interlocked	WARNING
✓	2/10/2015 1:21:56 PM		CIOC-1/MAINT_ALM		MAINT		[MULT]Node: Standby Seconda	WARNING
✓	2/2/2015 3:52:31 PM		CTLR-1/MAINT_ALM		MAINT		Redundancy: Not Communicatin	WARNING

Alarm name: HI_ALM

Optional Alarm Message Parameters

Alarm message: High Alarm Value %P1 Limit %P2

Message parameter 1: AI1/OUT

Message parameter 2: AI1/HI_LIM

Alarm Shelving Timeout

Days: 0 Hours: 8 Minutes: 0

Alarm Description: Charge tank at rated capacity

Alarm descriptions allow precise identification of module alarms.

white-paper-alarm-management-deltav-en-57058.pdf

https://habr.com/ru/company/croc/blog/353324/

SOC vs. Control Room: Alarm Tuning

Definition of “expensive” differs in IT and OT

Definition of “urgency” differs in IT and OT

Definition of “urgency” differs in IT and OT

On average, companies **take** about **197 days** to identify and **69 days** to contain a **breach** according to IBM.

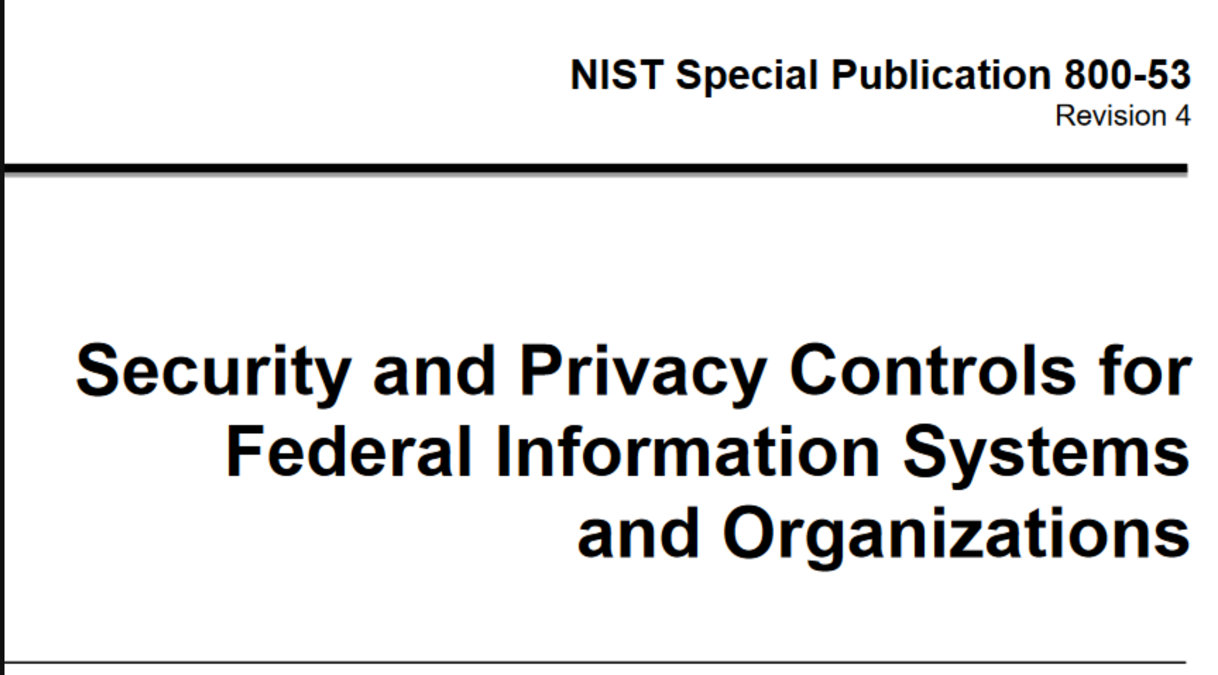
https://www.ibm.com/downloads/cas/AEJYBPWA

Definition of “urgency” differs in IT and OT

At 1:23 pm reactor cooling problem identified. At 1:33 pm the reactor burst and its contents exploded, killing 4 and injuring 38 people

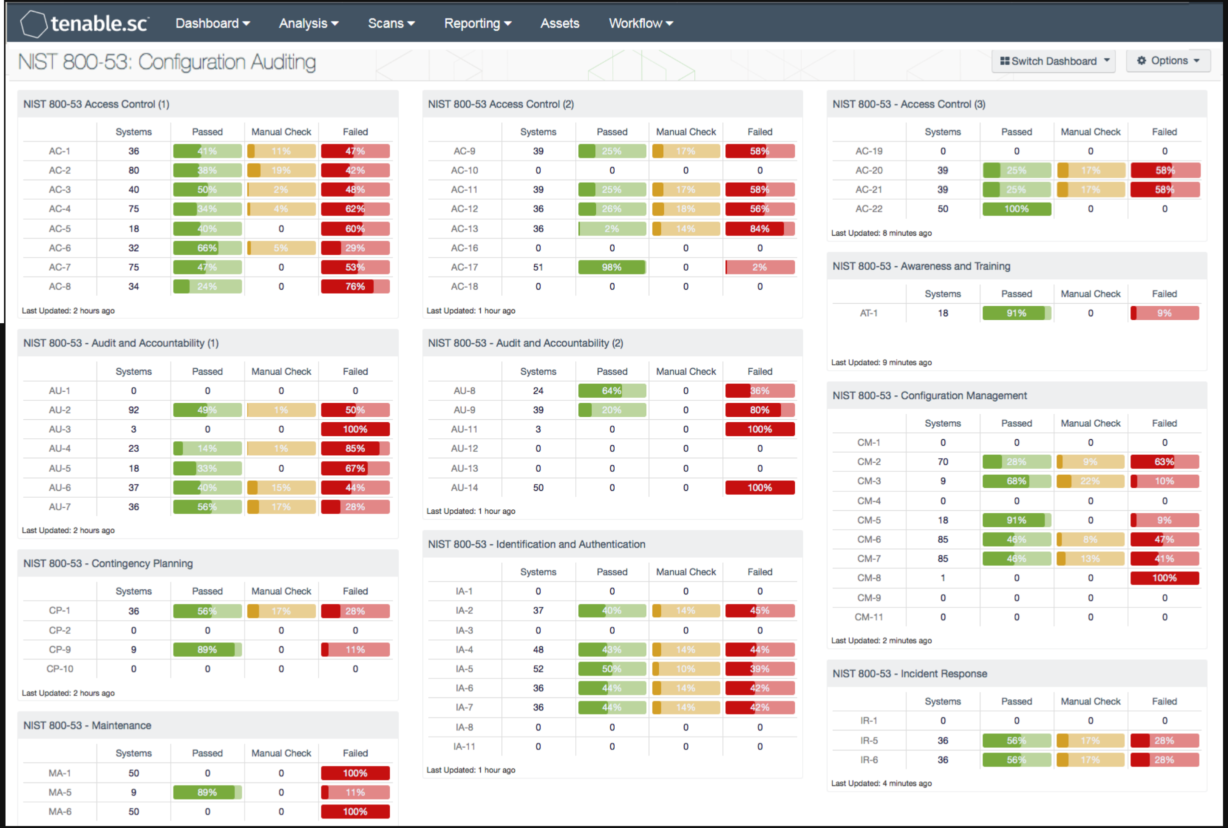
https://www.csb.gov/t2-laboratories-inc-reactive-chemical-explosion/

IT alert prioritization: Criticality of security control



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations



NIST 800-53: Configuration Auditing

NIST 800-53 Access Control (1)

	Systems	Passed	Manual Check	Failed
AC-1	36	41%	11%	47%
AC-2	80	38%	19%	42%
AC-3	40	50%	2%	48%
AC-4	75	34%	4%	62%
AC-5	18	40%	0	60%
AC-6	32	66%	5%	29%
AC-7	75	47%	0	53%
AC-8	34	24%	0	76%

Last Updated: 2 hours ago

NIST 800-53 - Audit and Accountability (1)

	Systems	Passed	Manual Check	Failed
AU-1	0	0	0	0
AU-2	92	49%	1%	50%
AU-3	3	0	0	100%
AU-4	23	14%	1%	85%
AU-5	18	33%	0	67%
AU-6	37	40%	15%	44%
AU-7	36	56%	17%	28%

Last Updated: 2 hours ago

NIST 800-53 - Contingency Planning

	Systems	Passed	Manual Check	Failed
CP-1	36	56%	17%	28%
CP-2	0	0	0	0
CP-9	9	89%	0	11%
CP-10	0	0	0	0

Last Updated: 2 hours ago

NIST 800-53 - Maintenance

	Systems	Passed	Manual Check	Failed
MA-1	50	0	0	100%
MA-5	9	89%	0	11%
MA-6	50	0	0	100%

NIST 800-53 Access Control (2)

	Systems	Passed	Manual Check	Failed
AC-9	39	25%	17%	58%
AC-10	0	0	0	0
AC-11	39	25%	17%	58%
AC-12	36	26%	18%	56%
AC-13	36	2%	14%	84%
AC-16	0	0	0	0
AC-17	51	98%	0	2%
AC-18	0	0	0	0

Last Updated: 1 hour ago

NIST 800-53 - Audit and Accountability (2)

	Systems	Passed	Manual Check	Failed
AU-8	24	64%	0	36%
AU-9	39	20%	0	80%
AU-11	3	0	0	100%
AU-12	0	0	0	0
AU-13	0	0	0	0
AU-14	50	0	0	100%

Last Updated: 1 hour ago

NIST 800-53 - Identification and Authentication

	Systems	Passed	Manual Check	Failed
IA-1	0	0	0	0
IA-2	37	40%	14%	45%
IA-3	0	0	0	0
IA-4	48	43%	14%	44%
IA-5	52	50%	10%	39%
IA-6	36	44%	14%	42%
IA-7	36	44%	14%	42%
IA-8	0	0	0	0
IA-11	0	0	0	0

Last Updated: 1 hour ago

NIST 800-53 - Access Control (3)

	Systems	Passed	Manual Check	Failed
AC-19	0	0	0	0
AC-20	39	25%	17%	58%
AC-21	39	25%	17%	58%
AC-22	50	100%	0	0

Last Updated: 8 minutes ago

NIST 800-53 - Awareness and Training

	Systems	Passed	Manual Check	Failed
AT-1	18	91%	0	9%

Last Updated: 9 minutes ago

NIST 800-53 - Configuration Management

	Systems	Passed	Manual Check	Failed
CM-1	0	0	0	0
CM-2	70	28%	9%	63%
CM-3	9	68%	22%	10%
CM-4	0	0	0	0
CM-5	18	91%	0	9%
CM-6	85	46%	8%	47%
CM-7	85	46%	13%	41%
CM-8	1	0	0	100%
CM-9	0	0	0	0
CM-11	0	0	0	0

Last Updated: 2 minutes ago

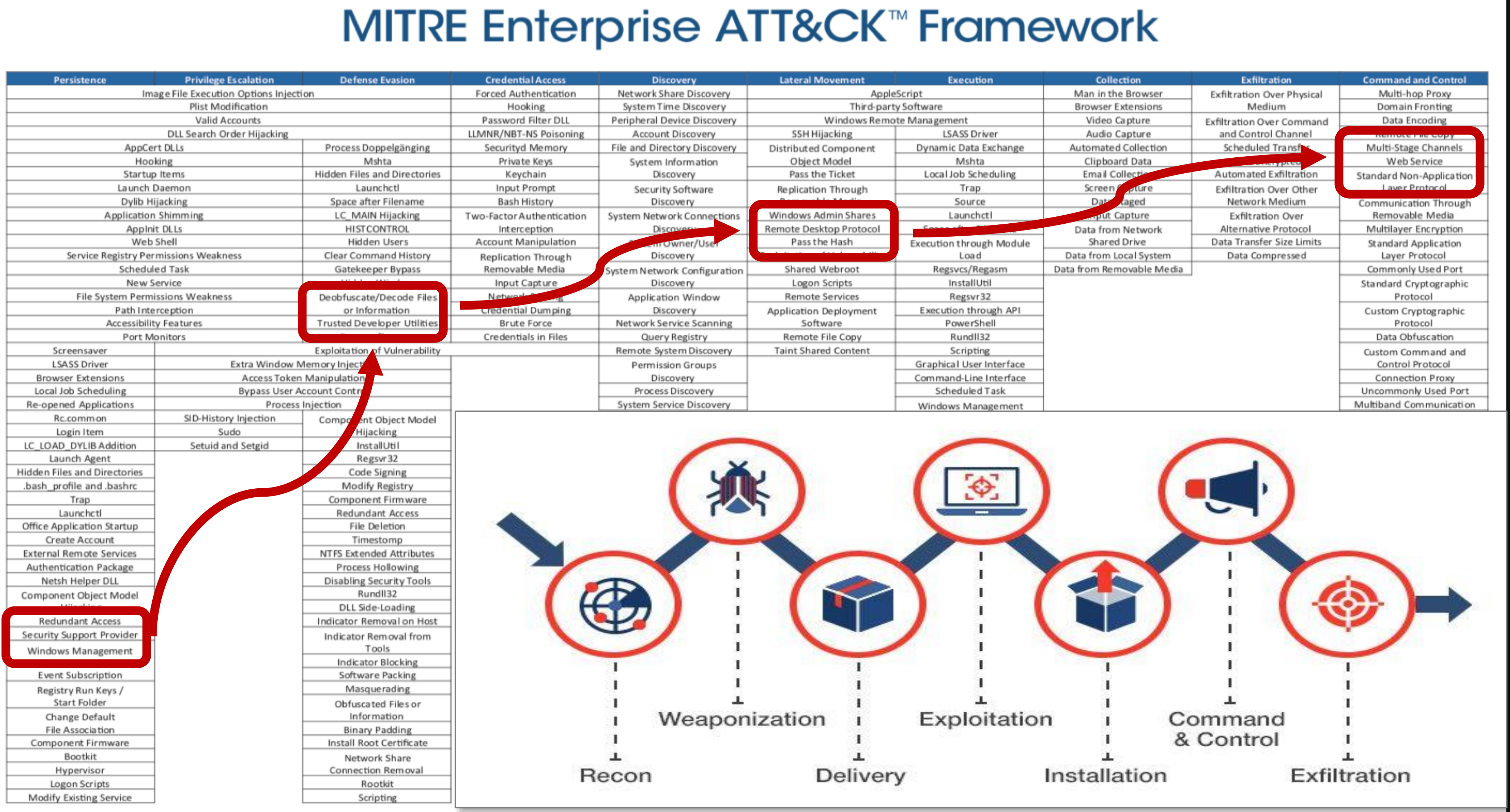
NIST 800-53 - Incident Response

	Systems	Passed	Manual Check	Failed
IR-1	0	0	0	0
IR-5	36	56%	17%	28%
IR-6	36	56%	17%	28%

Last Updated: 4 minutes ago

https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/images/sc-dashboards/NEW%20-%20NIST_80053_Dashboard_Drupal_Screenshot_revised.png

IT alert prioritization: Attacker progression



MITRE Enterprise ATT&CK™ Framework

Persistence

- Image File Execution Options Injection
- Plist Modification
- Valid Accounts
- DLL Search Order Hijacking
- AppCert DLLs
- Hooking
- Startup Items
- Launch Daemon
- Dylib Hijacking
- Application Shimming
- AppInit DLLs
- Web Shell
- Service Registry Permissions Weakness
- Scheduled Task
- New Service
- File System Permissions Weakness
- Path Interception
- Accessibility Features
- Port Monitors
- Screensaver
- LSASS Driver
- Browser Extensions
- Local Job Scheduling
- Re-opened Applications
- Rc.common
- Login Item
- LC_LOAD_DYLIB Addition
- Launch Agent
- Hidden Files and Directories
- .bash_profile and .bashrc
- Trap
- Launchctl
- Office Application Startup
- Create Account
- External Remote Services
- Authentication Package
- Netsh Helper DLL
- Component Object Model Hijacking
- Redundant Access
- Security Support Provider
- Windows Management Event Subscription
- Registry Run Keys / Start Folder
- Change Default File Association
- Component Firmware
- Bootkit
- Hypervisor
- Logon Scripts
- Modify Existing Service

Privilege Escalation

- Image File Execution Options Injection
- Plist Modification
- Valid Accounts
- DLL Search Order Hijacking
- AppCert DLLs
- Hooking
- Startup Items
- Launch Daemon
- Dylib Hijacking
- Application Shimming
- AppInit DLLs
- Web Shell
- Service Registry Permissions Weakness
- Scheduled Task
- New Service
- File System Permissions Weakness
- Path Interception
- Accessibility Features
- Port Monitors
- Exploitation of Vulnerability
- Extra Window Memory Injection
- Access Token Manipulation
- Bypass User Account Control
- Process Injection
- SID-History Injection
- Sudo
- Setuid and Setgid

Defense Evasion

- Image File Execution Options Injection
- Plist Modification
- Valid Accounts
- DLL Search Order Hijacking
- Process Doppelgänging
- Mshta
- Hidden Files and Directories
- Launchctl
- Space after Filename
- LC_MAIN Hijacking
- HISTCONTROL
- Hidden Users
- Clear Command History
- Gatekeeper Bypass
- Hidden Window
- Deobfuscate/Decode Files or Information
- Trusted Developer Utilities
- Regsvcs/Regasm
- Exploitation of Vulnerability
- Extra Window Memory Injection
- Access Token Manipulation
- Bypass User Account Control
- Process Injection
- Component Object Model Hijacking
- InstallUtil
- Regsvr32
- Code Signing
- Modify Registry
- Component Firmware
- Redundant Access
- File Deletion
- Timestomp
- NTFS Extended Attributes
- Process Hollowing
- Disabling Security Tools
- Rundll32
- DLL Side-Loading
- Indicator Removal on Host
- Indicator Removal from Tools
- Indicator Blocking
- Software Packing
- Masquerading
- Obfuscated Files or Information
- Binary Padding
- Install Root Certificate
- Network Share Connection Removal
- Rootkit
- Scripting

Credential Access

- Forced Authentication
- Hooking
- Password Filter DLL
- LLMNR/NBT-NS Poisoning
- Securityd Memory
- Private Keys
- Keychain
- Input Prompt
- Bash History
- Two-Factor Authentication Interception
- Account Manipulation
- Replication Through Removable Media
- Input Capture
- Network Sniffing
- Credential Dumping
- Brute Force
- Credentials in Files
- Exploitation of Vulnerability

Discovery

- Network Share Discovery
- System Time Discovery
- Peripheral Device Discovery
- Account Discovery
- File and Directory Discovery
- System Information Discovery
- Security Software Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Network Configuration Discovery
- Application Window Discovery
- Network Service Scanning
- Query Registry
- Remote System Discovery
- Permission Groups Discovery
- Process Discovery
- System Service Discovery

Lateral Movement

- AppleScript
- Third-party Software
- Windows Remote Management
- SSH Hijacking
- Distributed Component Object Model
- Pass the Ticket
- Replication Through Removable Media
- Windows Admin Shares
- Remote Desktop Protocol
- Pass the Hash
- Exploitation of Vulnerability
- Shared Webroot
- Logon Scripts
- Remote Services
- Application Deployment Software
- Remote File Copy
- Taint Shared Content

Execution

- AppleScript
- Third-party Software
- Windows Remote Management
- LSASS Driver
- Dynamic Data Exchange
- Mshta
- Local Job Scheduling
- Trap
- Source
- Launchctl
- Space after Filename
- Execution through Module Load
- Regsvcs/Regasm
- InstallUtil
- Regsvr32
- Execution through API
- PowerShell
- Rundll32
- Scripting
- Graphical User Interface
- Command-Line Interface
- Scheduled Task
- Windows Management

Collection

- Man in the Browser
- Browser Extensions
- Video Capture
- Audio Capture
- Automated Collection
- Clipboard Data
- Email Collection
- Screen Capture
- Data Staged
- Input Capture
- Data from Network Shared Drive
- Data from Local System
- Data from Removable Media

Exfiltration

- Exfiltration Over Physical Medium
- Exfiltration Over Command and Control Channel
- Scheduled Transfer
- Data Encrypted
- Automated Exfiltration
- Exfiltration Over Other Network Medium
- Exfiltration Over Alternative Protocol
- Data Transfer Size Limits
- Data Compressed

Command and Control

- Multi-hop Proxy
- Domain Fronting
- Data Encoding
- Remote File Copy
- Multi-Stage Channels
- Web Service
- Standard Non-Application Layer Protocol
- Communication Through Removable Media
- Multilayer Encryption
- Standard Application Layer Protocol
- Commonly Used Port
- Standard Cryptographic Protocol
- Custom Cryptographic Protocol
- Data Obfuscation
- Custom Command and Control Protocol
- Connection Proxy
- Uncommonly Used Port
- Multiband Communication

IT alert prioritization: Asset criticality

Critical application servers / DBs

Customer serving servers

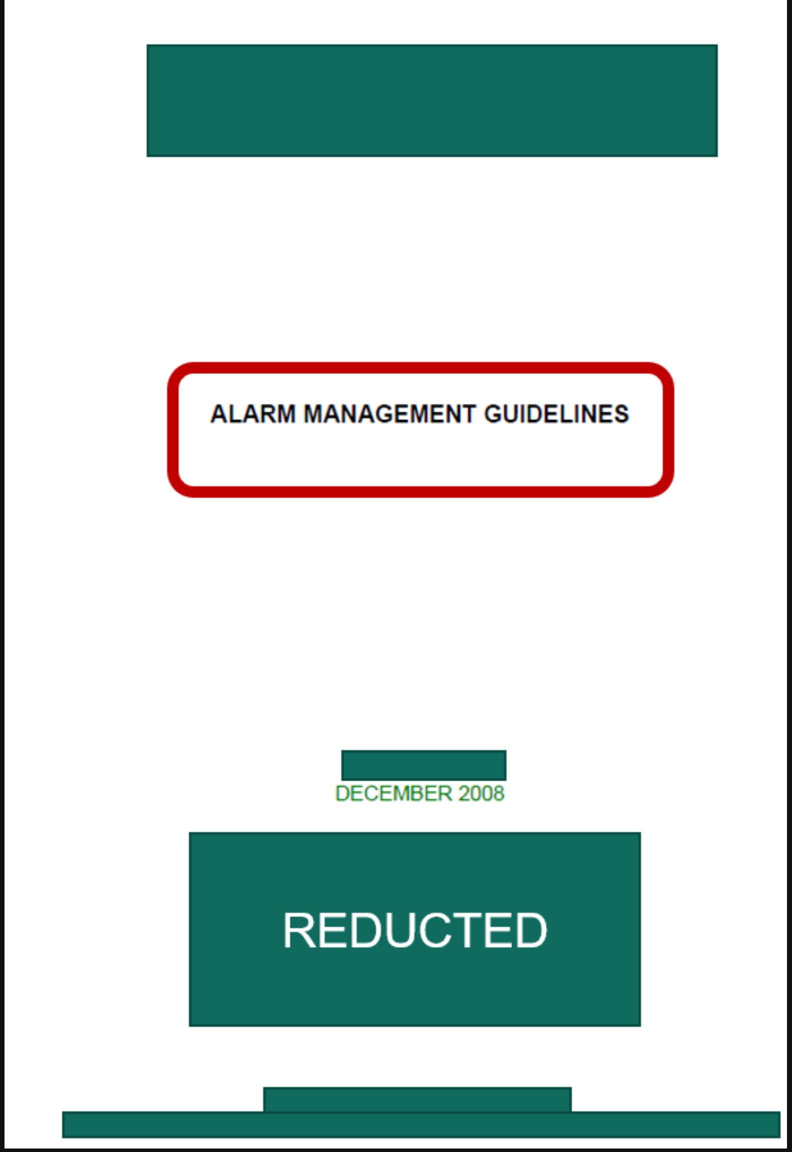
SOC: Alarm tuning

- Threat driven: Outbound traffic to known C2 server
- Policy driven: Usage of domain admin account
- Anomaly centric: High volume scanning from a single workstation

Mostly heuristic alarm threshold tuning

- Goal is to minimize false positives and noise
- Alerting on known IoC or obvious threats such as usage of privileged accounts
- Setting up a threshold for AV alerts or brute force activities
- Alerting based on behavioral patterns

OT: Alarm management guidlines



[redacted]

ALARM MANAGEMENT GUIDELINES

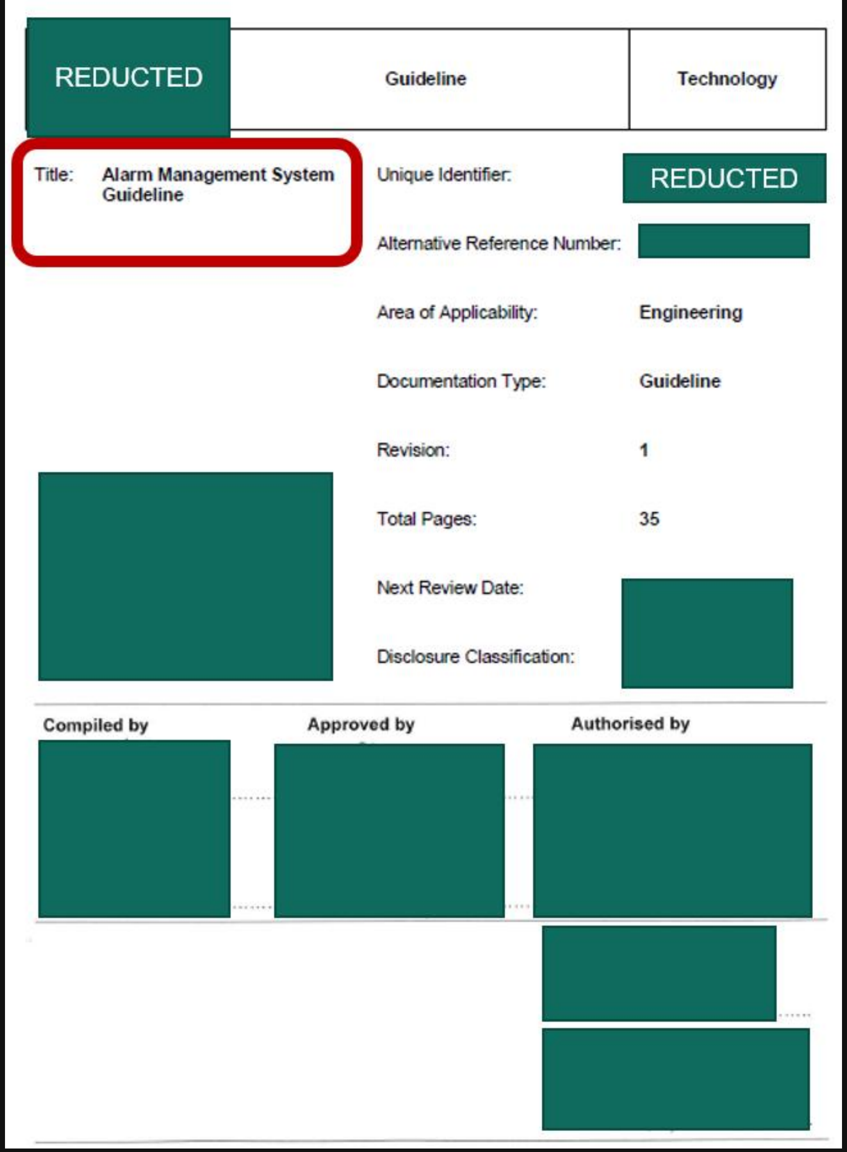
[redacted]

DECEMBER 2008

REDUCTED

[redacted]

[redacted]



REDUCTED	Guideline	Technology

Title: Alarm Management System Guideline

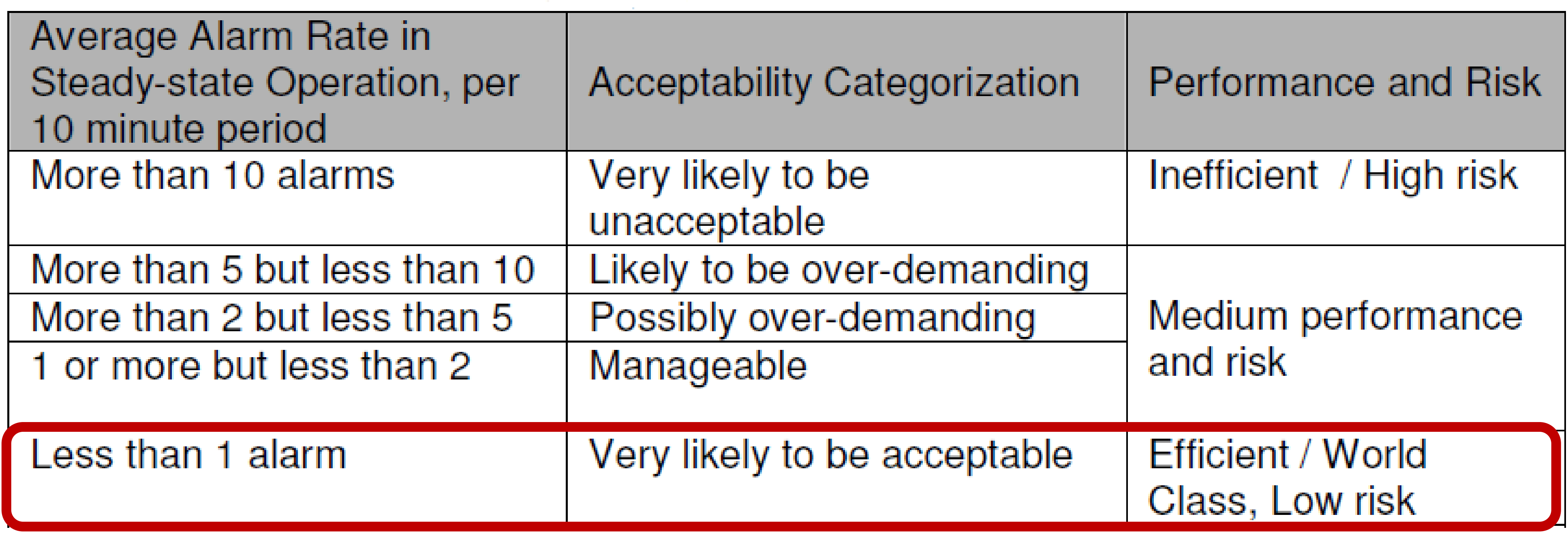
[redacted]

Unique Identifier:	REDUCTED
Alternative Reference Number:	[redacted]
Area of Applicability:	Engineering
Documentation Type:	Guideline
Revision:	1
Total Pages:	35
Next Review Date:	[redacted]
Disclosure Classification:	

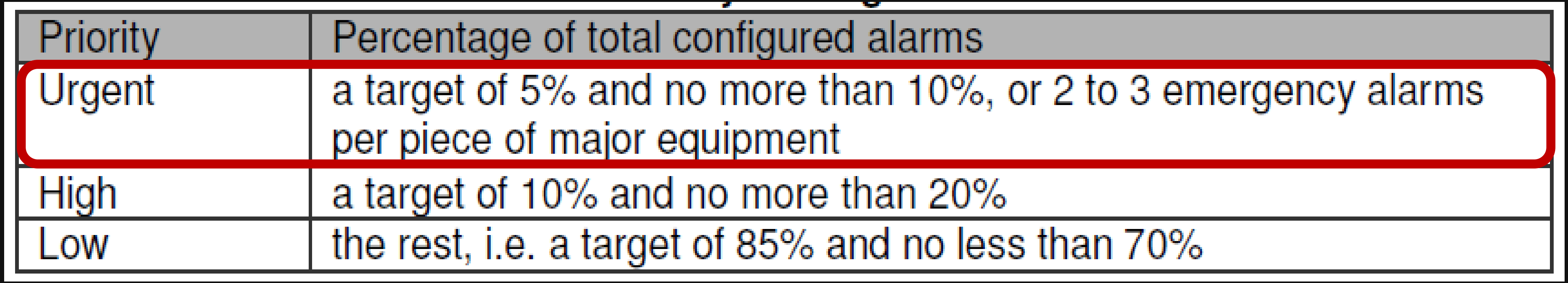
Compiled by	Approved by	Authorised by
[redacted]	[redacted]	[redacted]
		[redacted]
		[redacted]

Source: Internet

OT: Target alarm rate

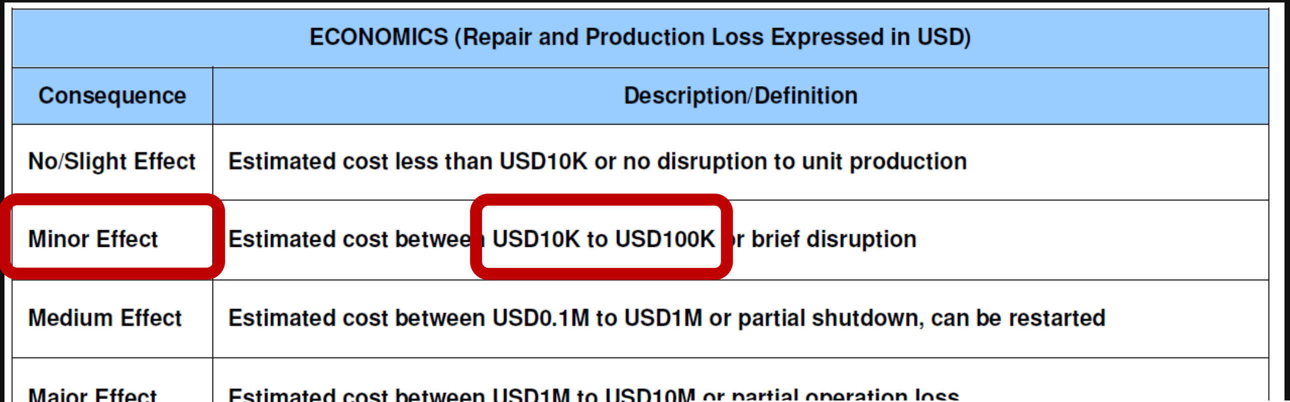


Average Alarm Rate in Steady-state Operation, per 10 minute period	Acceptability Categorization	Performance and Risk
More than 10 alarms	Very likely to be unacceptable	Inefficient / High risk
More than 5 but less than 10	Likely to be over-demanding	Medium performance and risk
More than 2 but less than 5	Possibly over-demanding	
1 or more but less than 2	Manageable	
Less than 1 alarm	Very likely to be acceptable	Efficient / World Class, Low risk

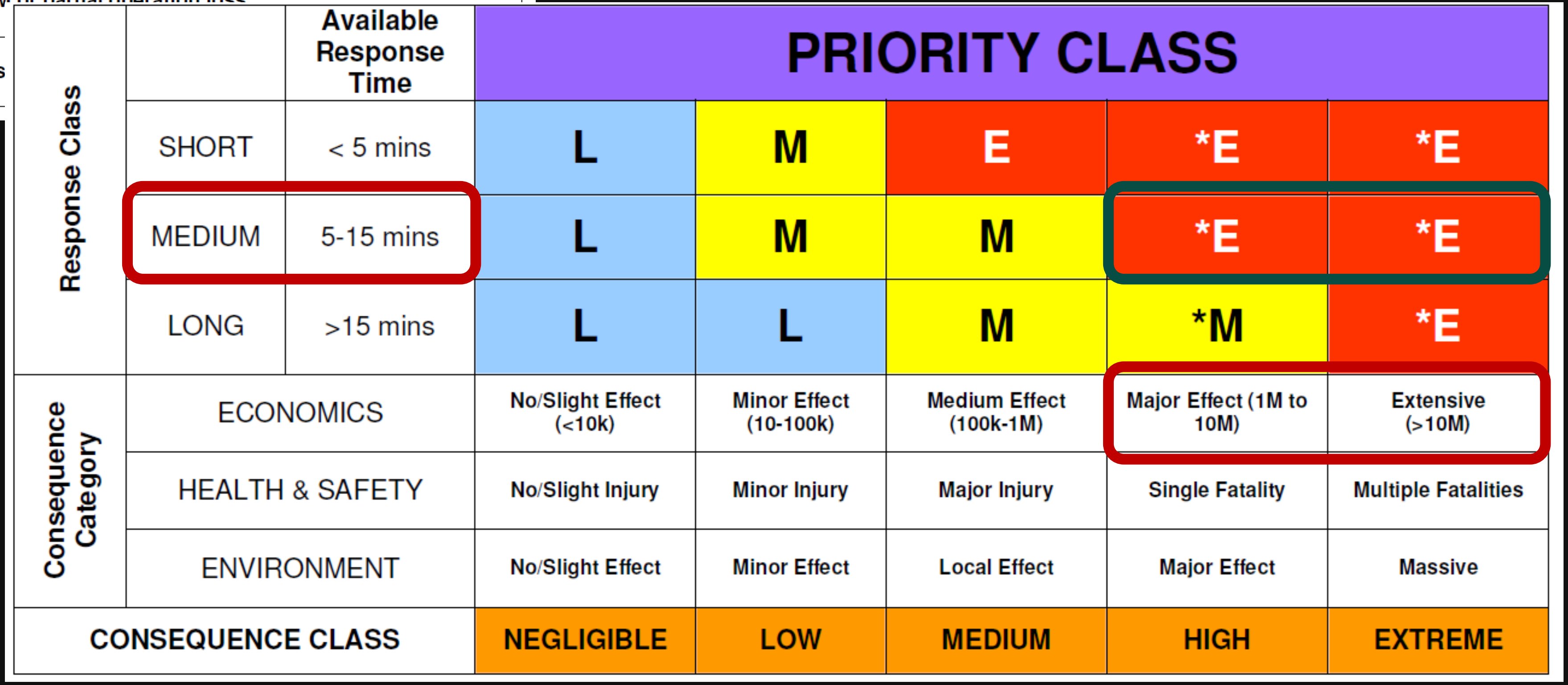


Priority	Percentage of total configured alarms
Urgent	a target of 5% and no more than 10%, or 2 to 3 emergency alarms per piece of major equipment
High	a target of 10% and no more than 20%
Low	the rest, i.e. a target of 85% and no less than 70%

OT: Alarm prioritization

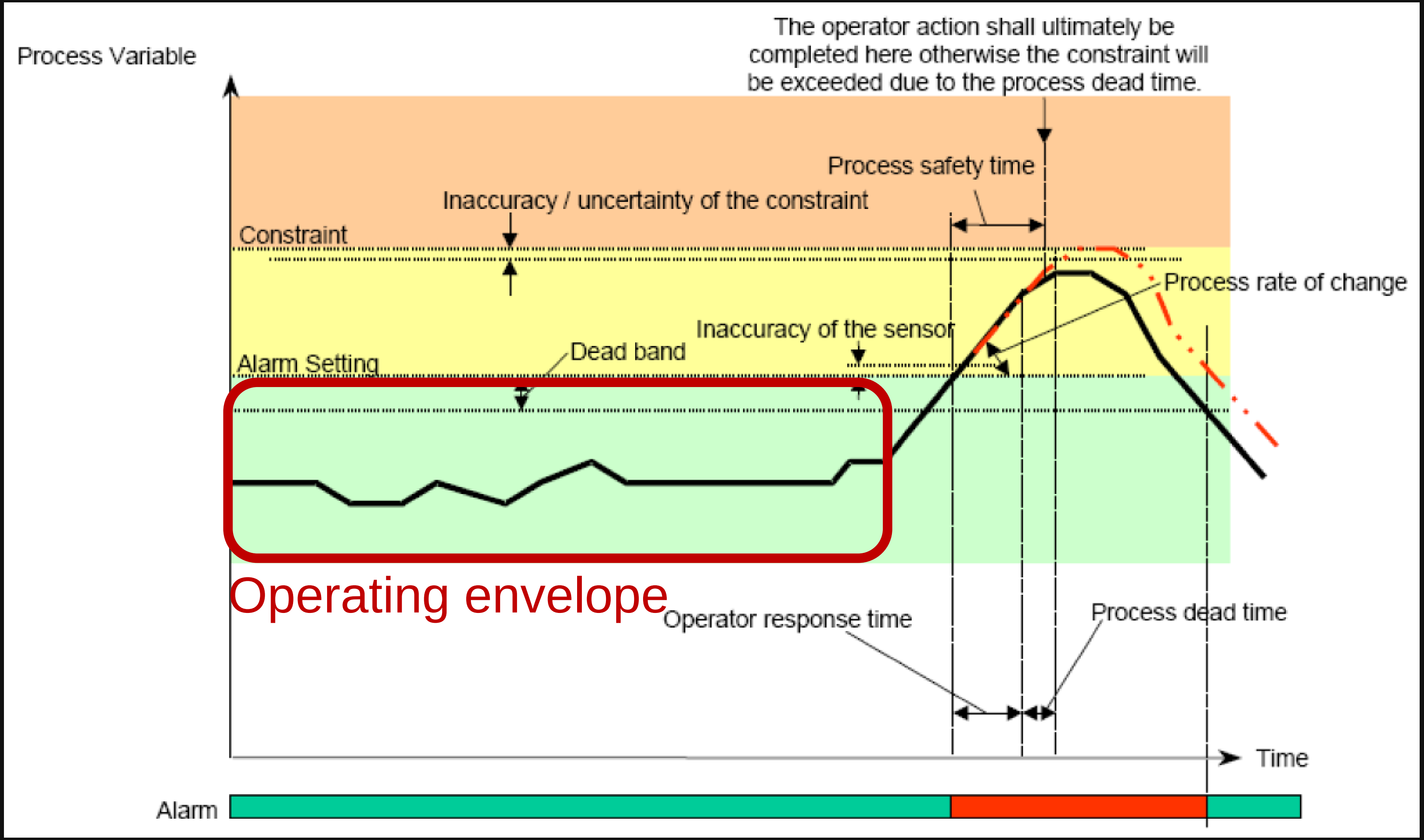


ECONOMICS (Repair and Production Loss Expressed in USD)	
Consequence	Description/Definition
No/Slight Effect	Estimated cost less than USD10K or no disruption to unit production
Minor Effect	Estimated cost between USD10K to USD100K or brief disruption
Medium Effect	Estimated cost between USD0.1M to USD1M or partial shutdown, can be restarted
Major Effect	Estimated cost between USD1M to USD10M or partial operation loss
Extensive	Estimated cost more than USD10M or subs

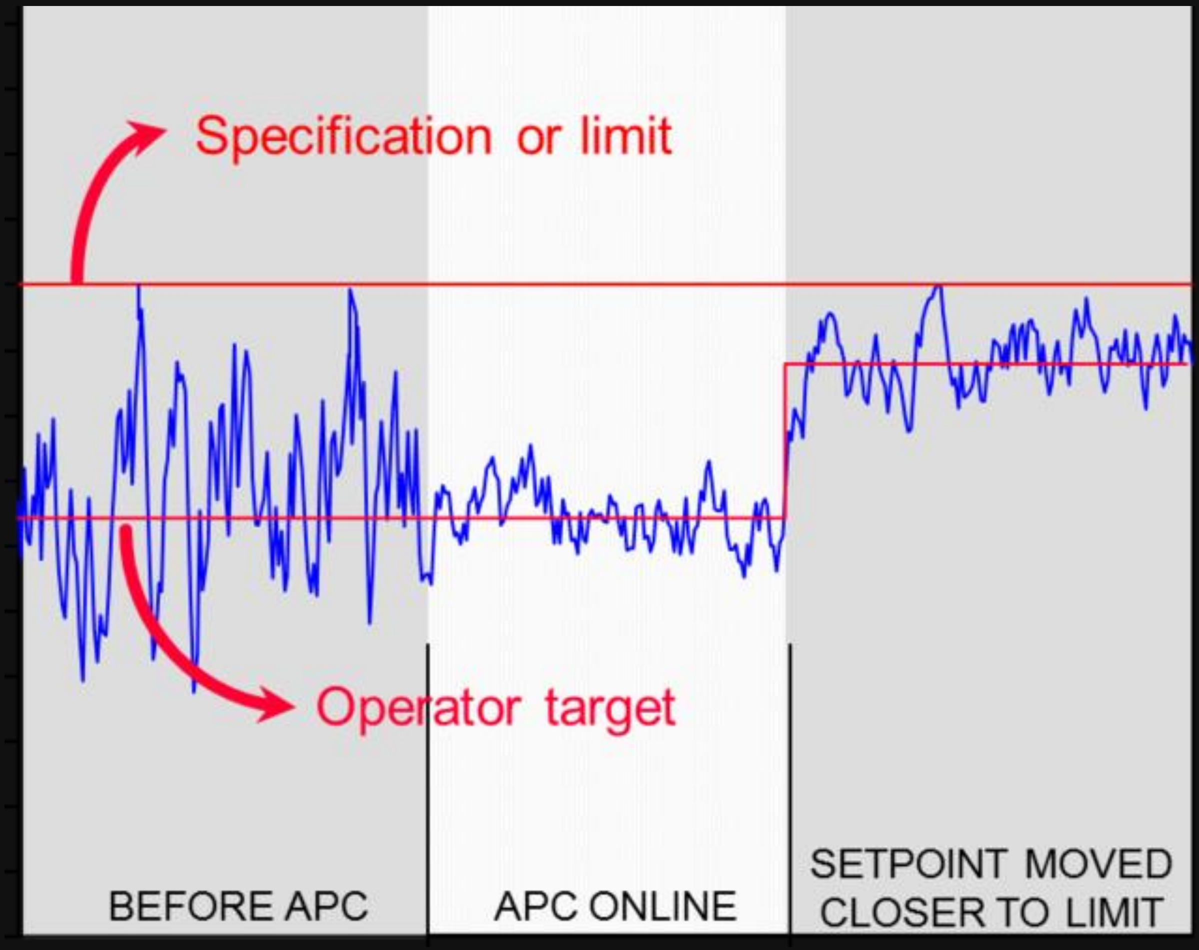


		Available Response Time	PRIORITY CLASS				
Response Class	SHORT	< 5 mins	L	M	E	*E	*E
	MEDIUM	5-15 mins	L	M	M	*E	*E
	LONG	>15 mins	L	L	M	*M	*E
Consequence Category	ECONOMICS		No/Slight Effect (<10k)	Minor Effect (10-100k)	Medium Effect (100k-1M)	Major Effect (1M to 10M)	Extensive (>10M)
	HEALTH & SAFETY		No/Slight Injury	Minor Injury	Major Injury	Single Fatality	Multiple Fatalities
	ENVIRONMENT		No/Slight Effect	Minor Effect	Local Effect	Major Effect	Massive
CONSEQUENCE CLASS			NEGLIGIBLE	LOW	MEDIUM	HIGH	EXTREME

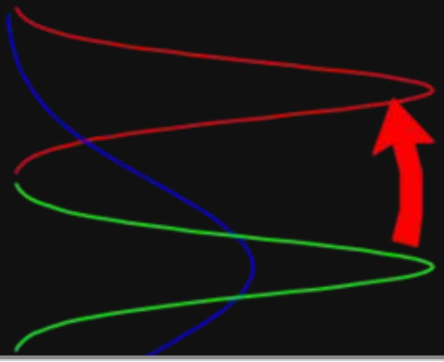
Parameters involved in establishing alarm setting

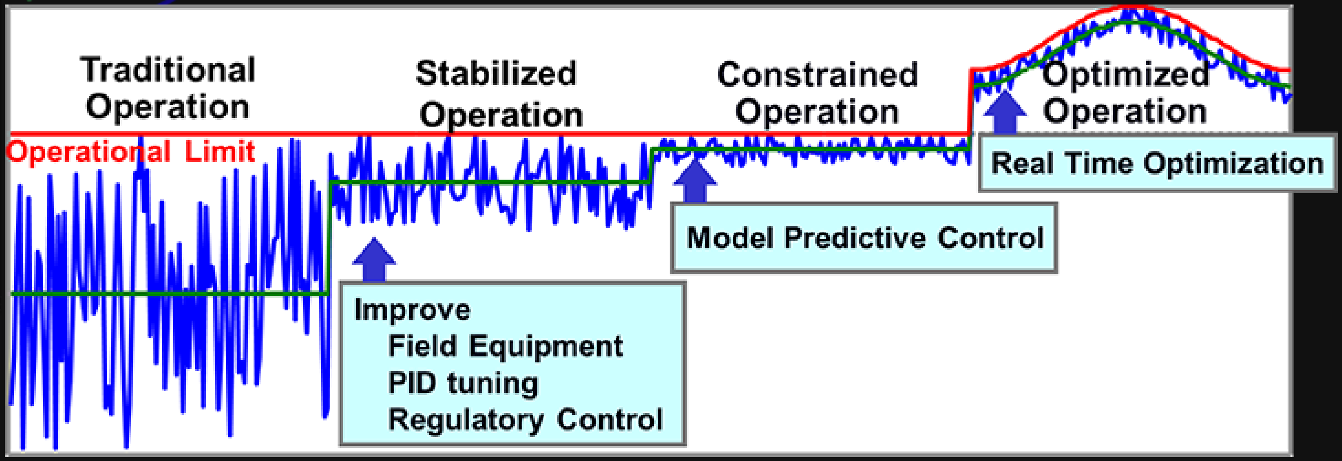


Advanced process control



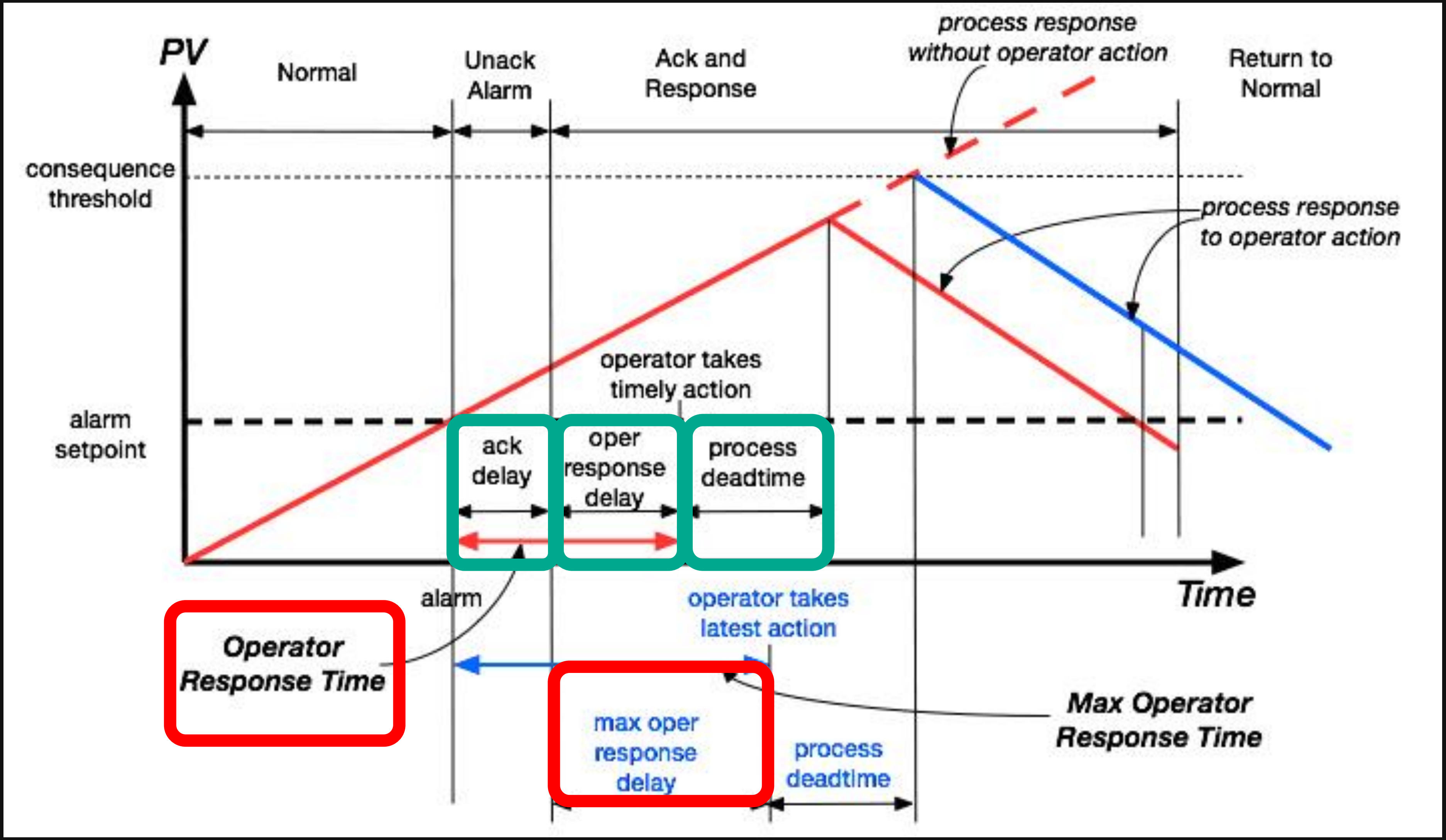
https://blog.yokogawa.com/blog/what-is-apc





https://www.mec-value.com/english/solution/system/advanced.html

Alarm response time



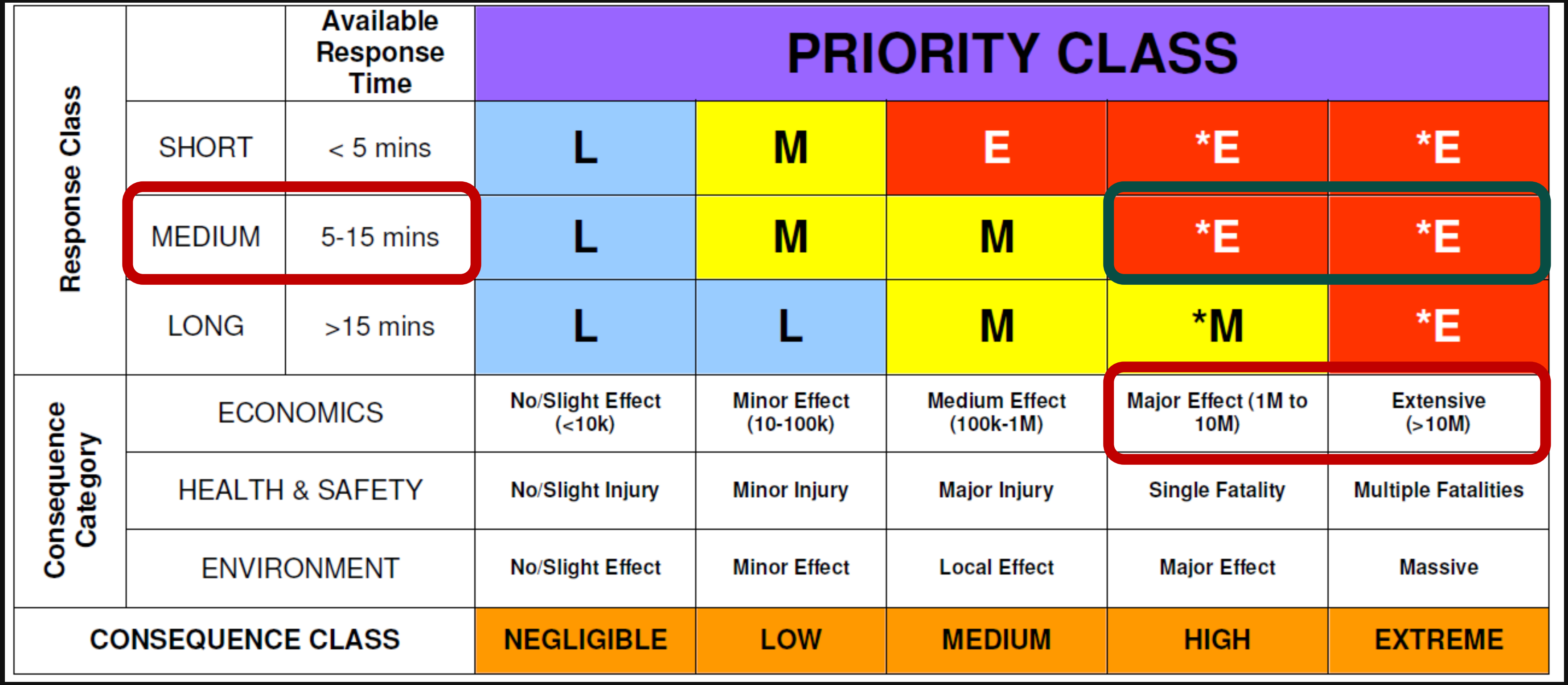
https://www.controlglobal.com/assets/00_images/2015/08/CG1508-AlarmsFeat2-Fig2-2.jpg

https://habr.com/ru/company/croc/blog/353324/

Enterprise SOC or OT SOC?

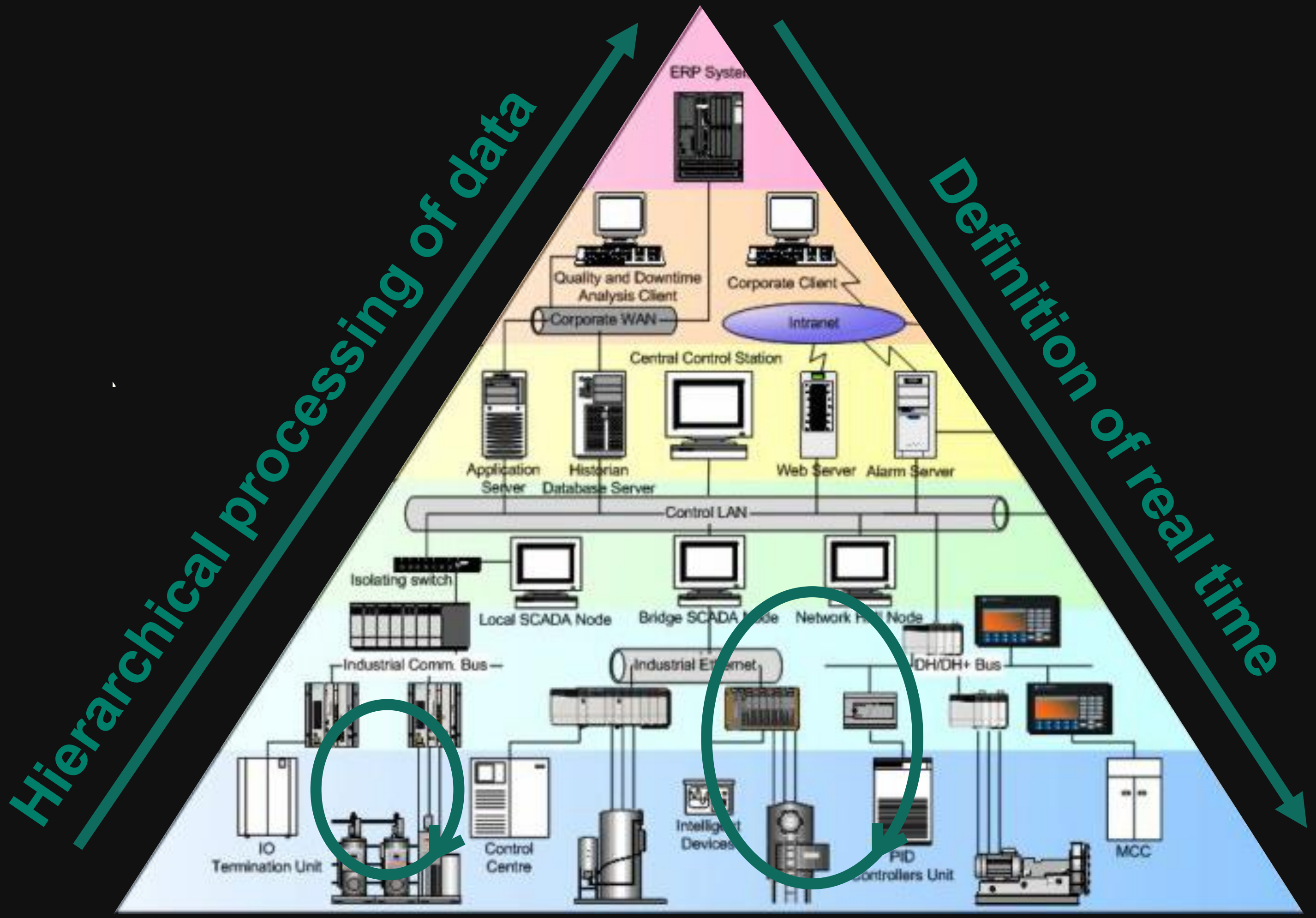
(or a little bit of both?)

OT: Understanding reaction time requirements



		Available Response Time	PRIORITY CLASS				
Response Class	SHORT	< 5 mins	L	M	E	*E	*E
	MEDIUM	5-15 mins	L	M	M	*E	*E
	LONG	>15 mins	L	L	M	*M	*E
Consequence Category	ECONOMICS		No/Slight Effect (<10k)	Minor Effect (10-100k)	Medium Effect (100k-1M)	Major Effect (1M to 10M)	Extensive (>10M)
	HEALTH & SAFETY		No/Slight Injury	Minor Injury	Major Injury	Single Fatality	Multiple Fatalities
	ENVIRONMENT		No/Slight Effect	Minor Effect	Local Effect	Major Effect	Massive
CONSEQUENCE CLASS			NEGLIGIBLE	LOW	MEDIUM	HIGH	EXTREME

Automation Pyramid



Hierarchical processing of data

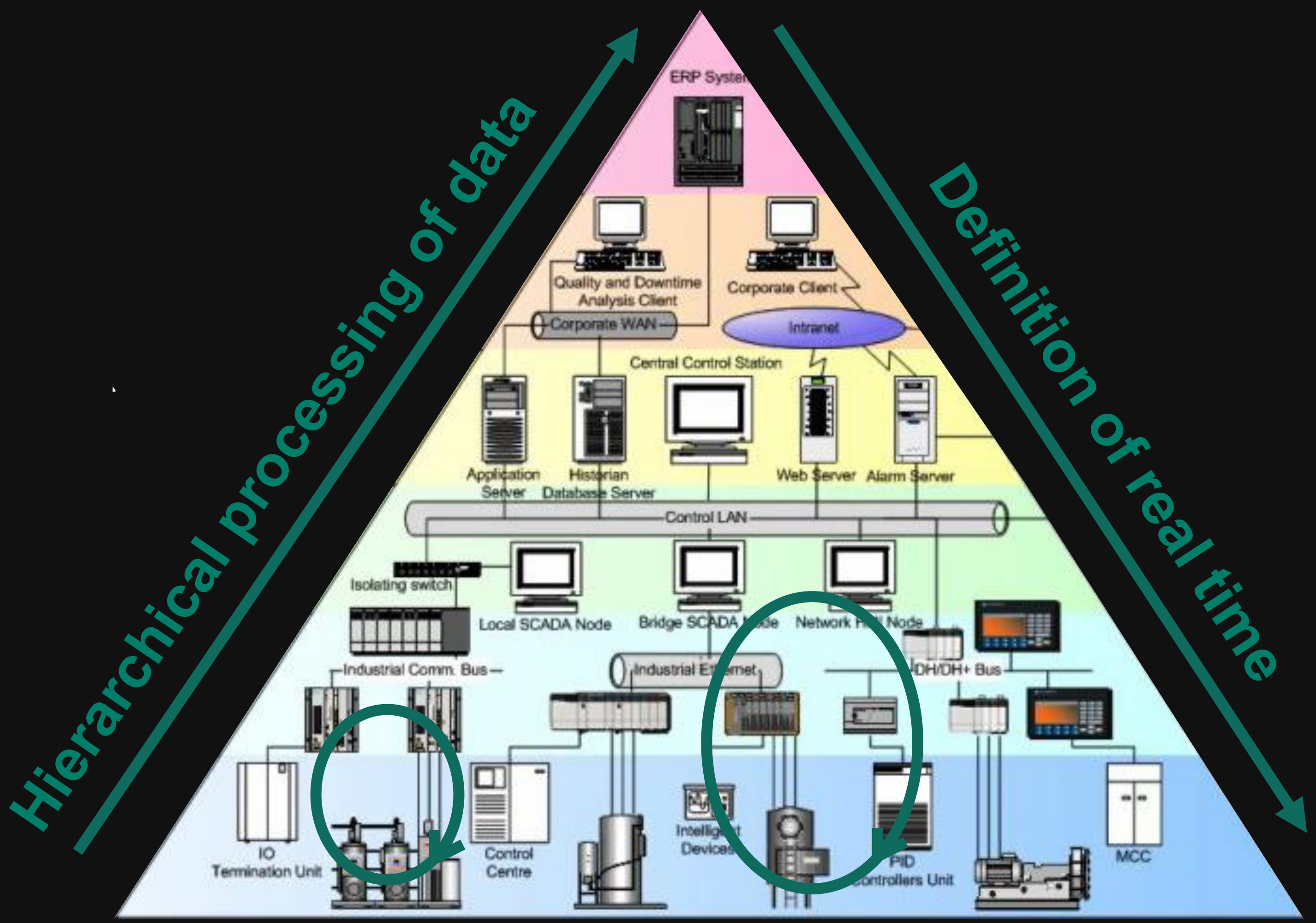
Definition of real time

Operates on raw data

Operates on information

http://krakenautomation.com/images/KrakenPyramid.jpg

Automation Pyramid



Hierarchical processing of data

Definition of real time

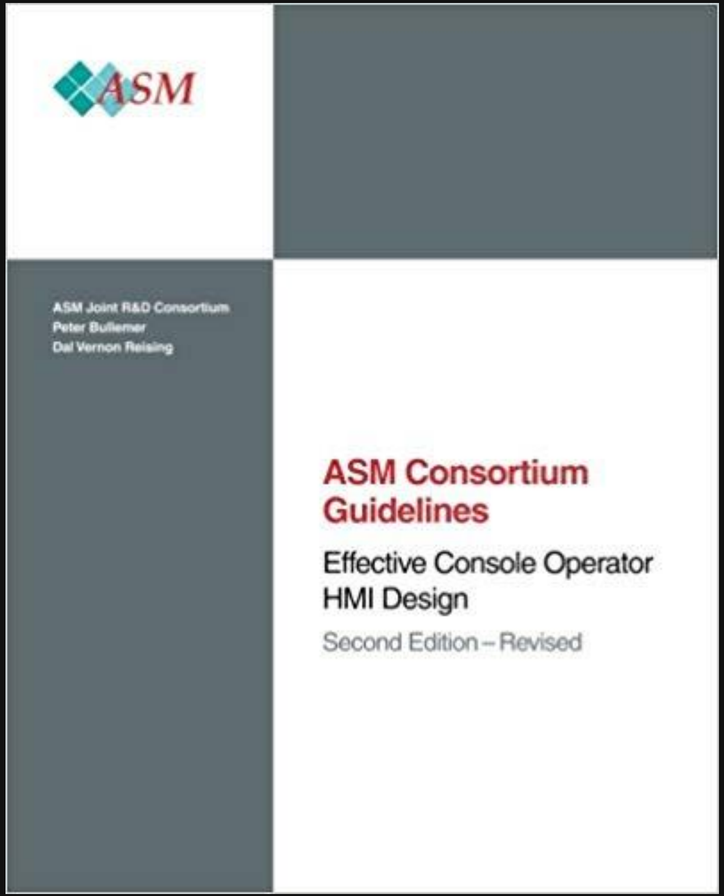
Loop in milliseconds

Loop in seconds

http://krakenautomation.com/images/KrakenPyramid.jpg

Abnormal Situation Management (ASM) Consortium

The ASM Consortium promotes their vision by conducting research, testing and evaluating which contribute to the successful reduction of abnormal situations in chemical processes.



ASM

ASM Joint R&D Consortium
Peter Bullemer
Dal Vernon Reising

ASM Consortium Guidelines

Effective Console Operator HMI Design

Second Edition – Revised

https://www.amazon.com/Effective-Console-Operator-HMI-Design/dp/1514203855

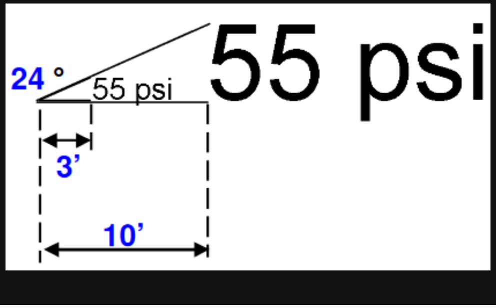
Layers of HMI views

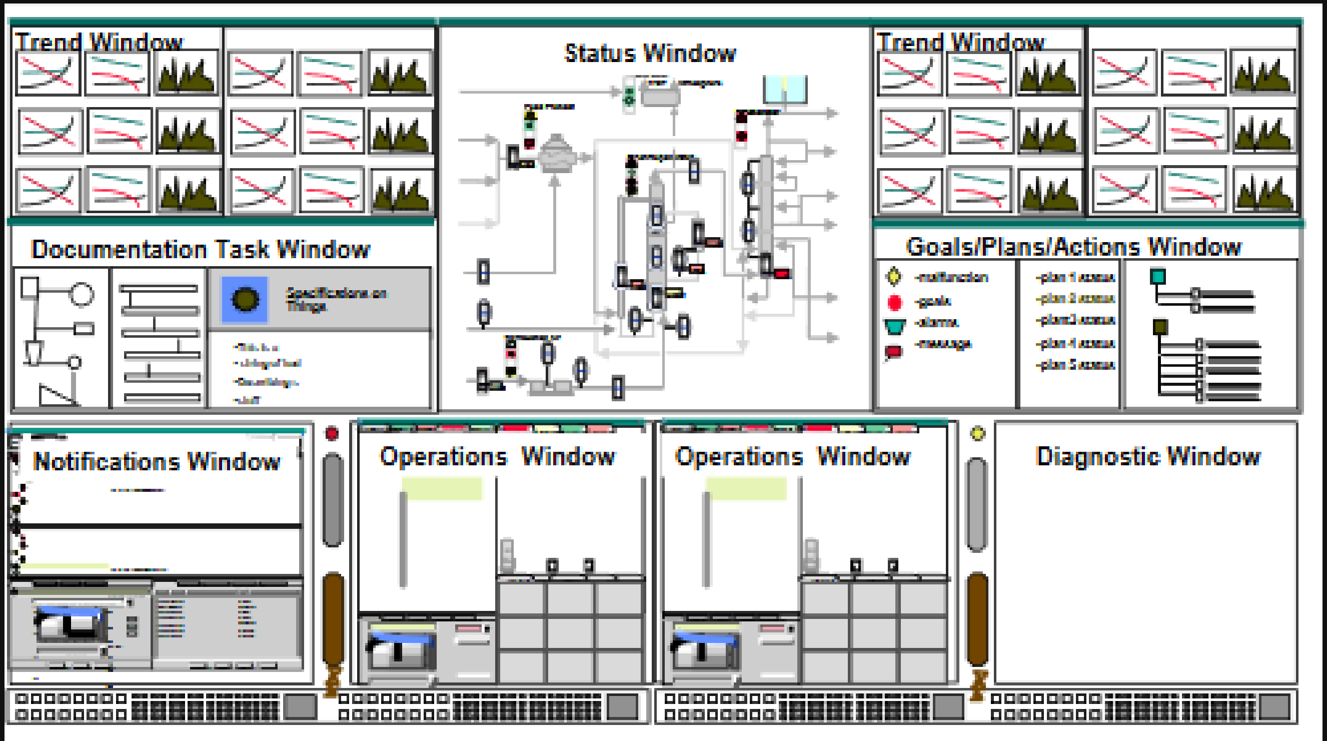
What is displayed in each level is plant (customer) specific, there is only general guidance:

- Level 1 – plant overview
- Level 2 – unit overview
- Level 3 – equipment overview
- Level 4 – trends / elements of contro logic

Trends are one of the most important displays

Effective Text/ Object Size





https://www.asmconsortium.net/Documents/2009%20ASM%20Displays%20GL%20Webinar%20v014.pdf

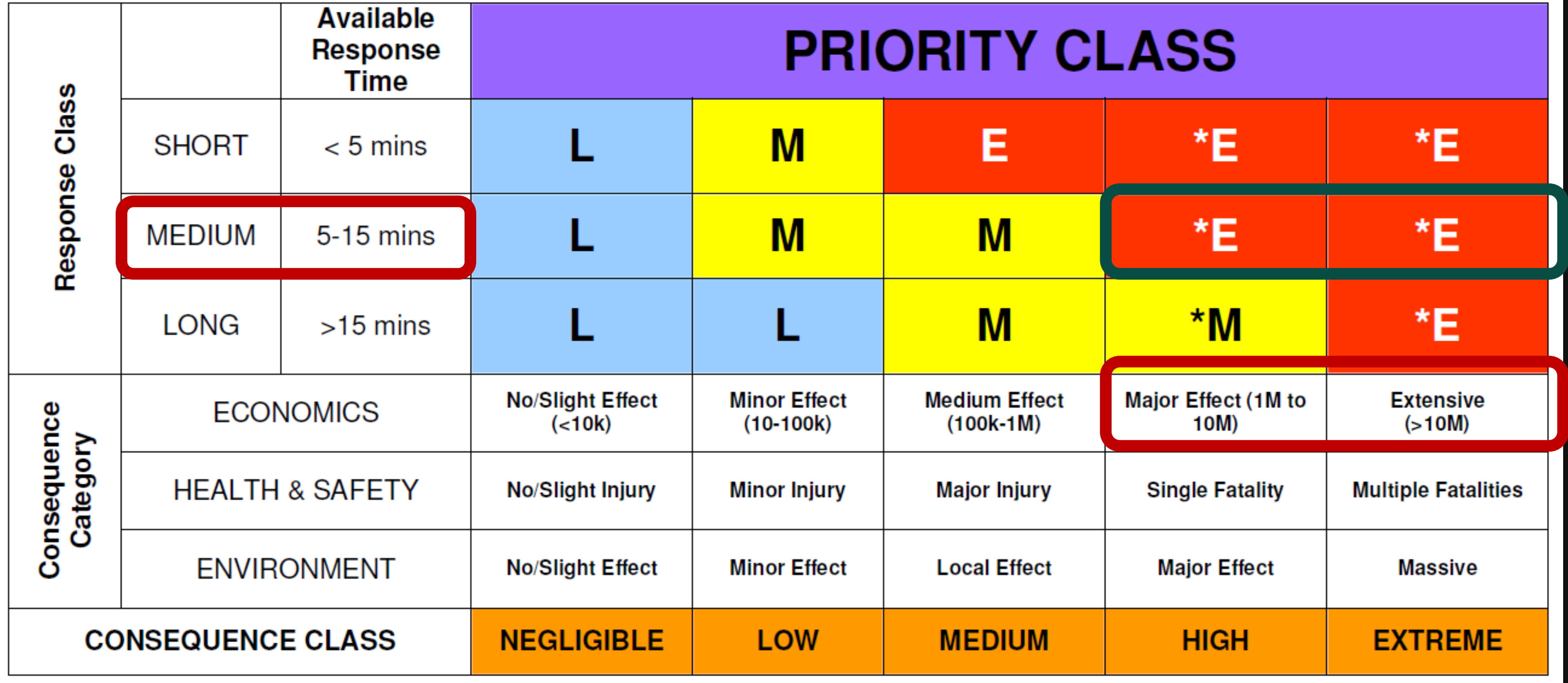
Fundamental design of HMI

The operator interface allows operators to focus their mental resources on controlling the process, not on interacting with the underlying system platform.

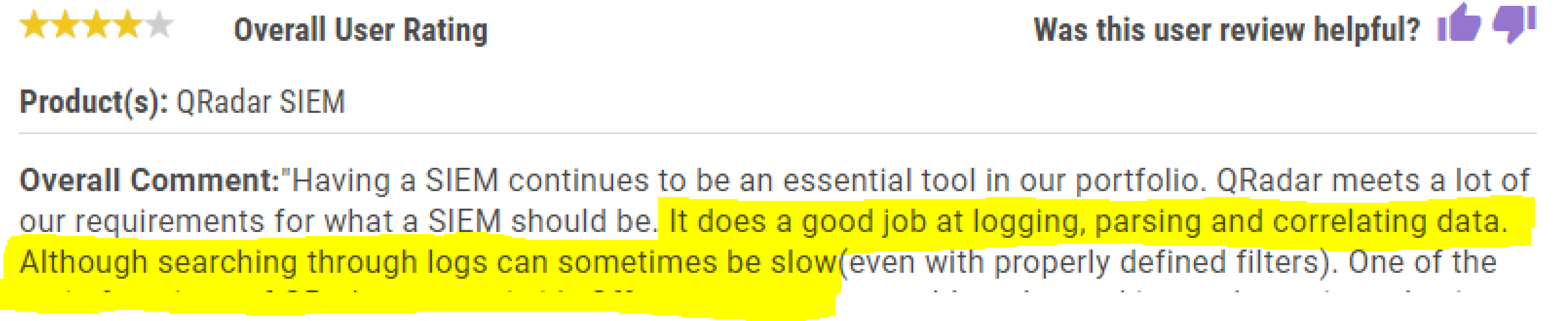
That means the HMI is consistent and easy to use in terms of making minimal demands on the console operators’ mental and physical resources to understand and interact with the process control system.

https://www.controleng.com/articles/creating-an-asm-compliant-hmi-goes-deeper-than-screen-color-selection/

OT: Understanding reaction time requirements



		Available Response Time	PRIORITY CLASS				
Response Class	SHORT	< 5 mins	L	M	E	*E	*E
	MEDIUM	5-15 mins	L	M	M	*E	*E
	LONG	>15 mins	L	L	M	*M	*E
Consequence Category	ECONOMICS		No/Slight Effect (<10k)	Minor Effect (10-100k)	Medium Effect (100k-1M)	Major Effect (1M to 10M)	Extensive (>10M)
	HEALTH & SAFETY		No/Slight Injury	Minor Injury	Major Injury	Single Fatality	Multiple Fatalities
	ENVIRONMENT		No/Slight Effect	Minor Effect	Local Effect	Major Effect	Massive
CONSEQUENCE CLASS			NEGLIGIBLE	LOW	MEDIUM	HIGH	EXTREME



★★★★☆ Overall User Rating

Was this user review helpful?

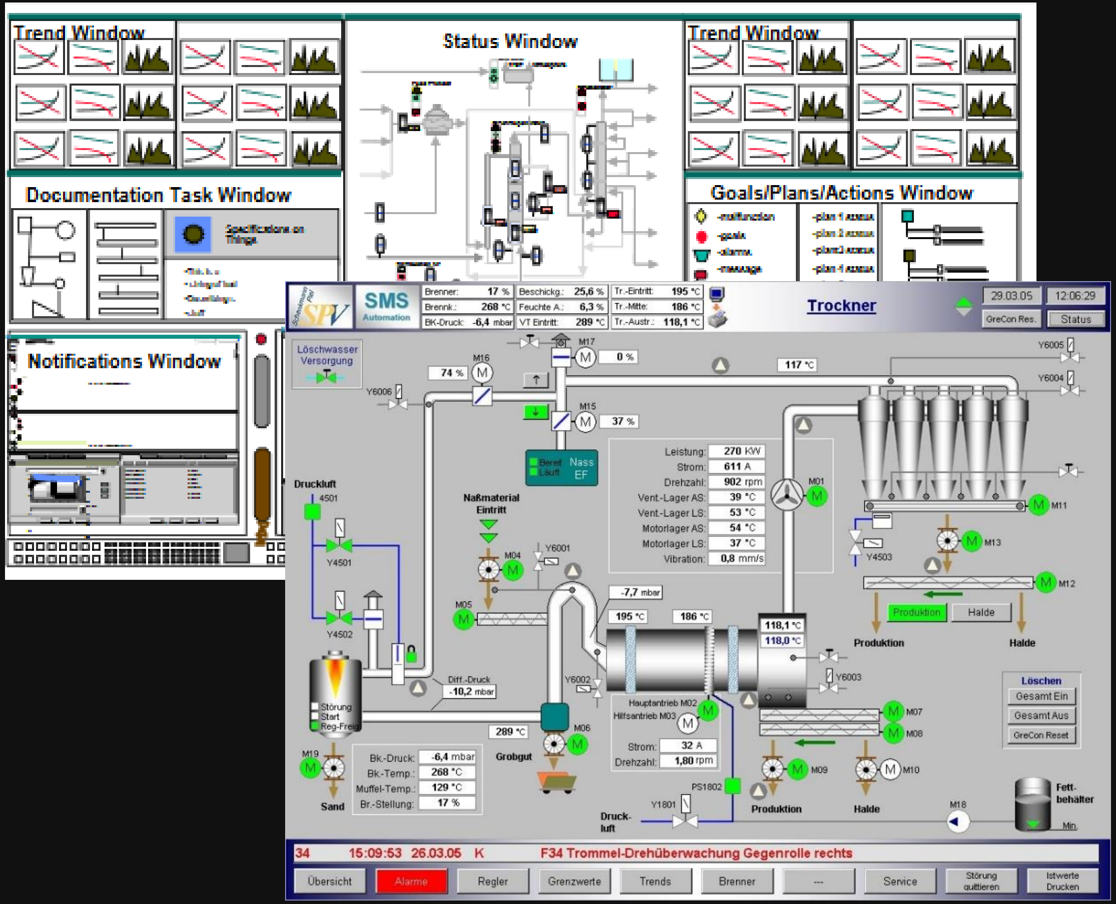
Product(s): QRadar SIEM

Overall Comment:"Having a SIEM continues to be an essential tool in our portfolio. QRadar meets a lot of our requirements for what a SIEM should be. It does a good job at logging, parsing and correlating data. Although searching through logs can sometimes be slow(even with properly defined filters). One of the

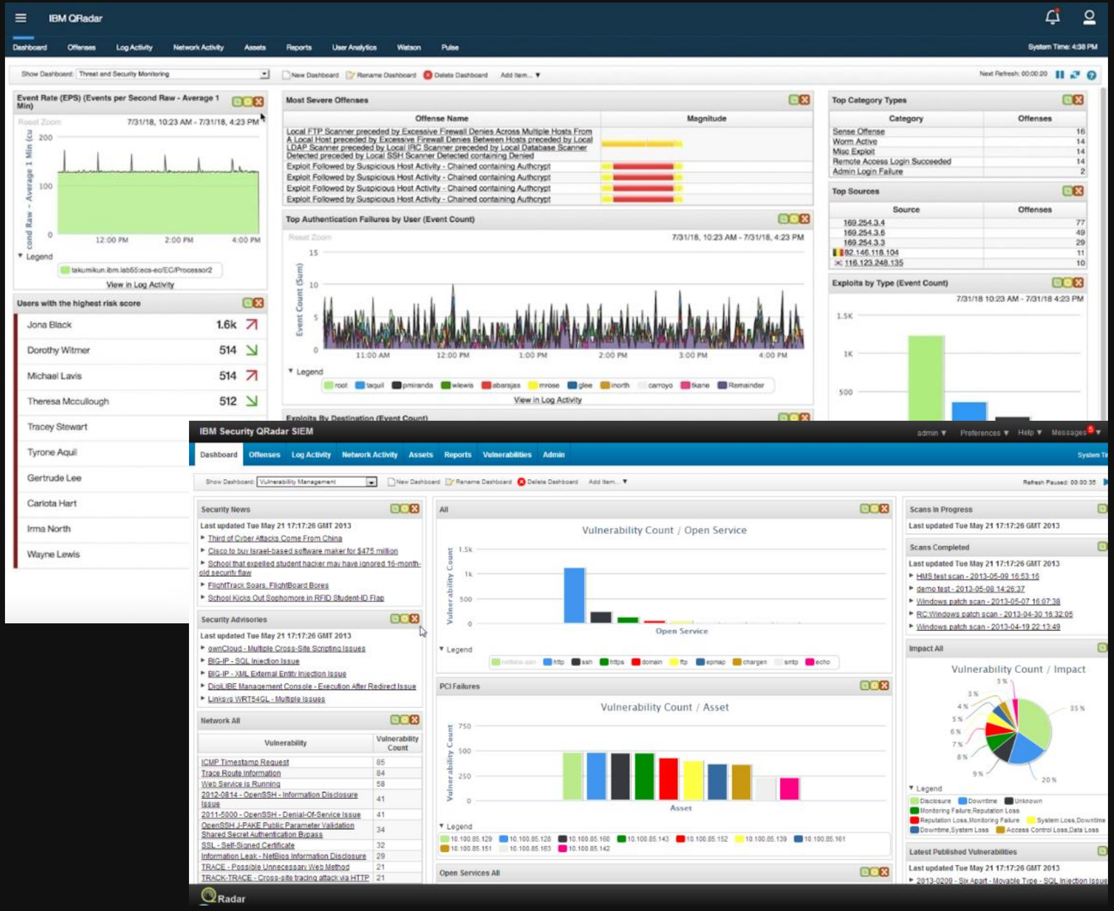
https://www.gartner.com/reviews/market/security-information-event-management/vendor/ibm/product/qradar-siem/review/view/1353353

(some) Points to consider

How can we decrease root cause analysis and mitigation decision time in SIEM tools?

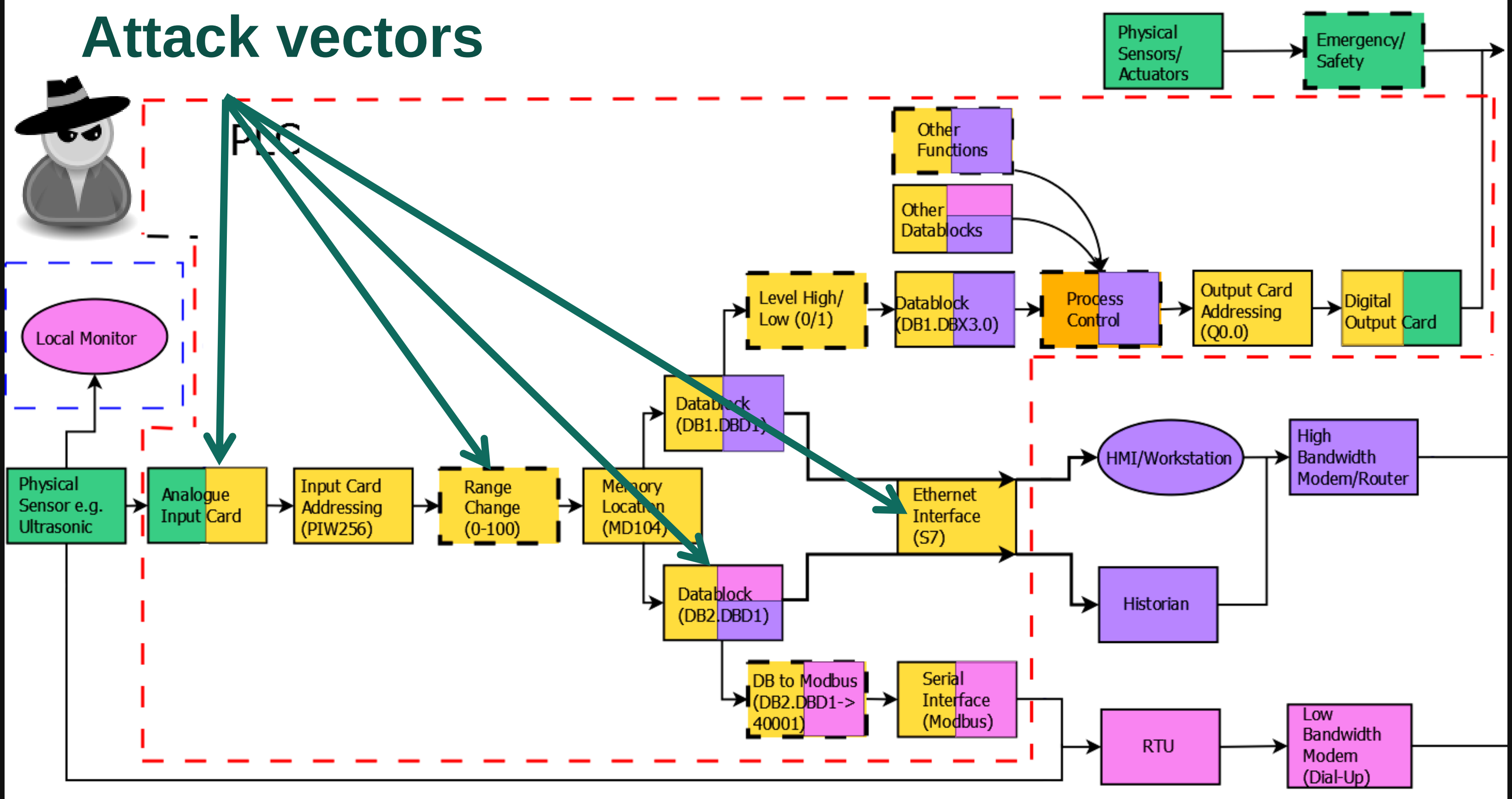


vs.



(some) Points to consider

Which logs do we need to collect? Which visibility obtain? -> Granular visualization of data flows



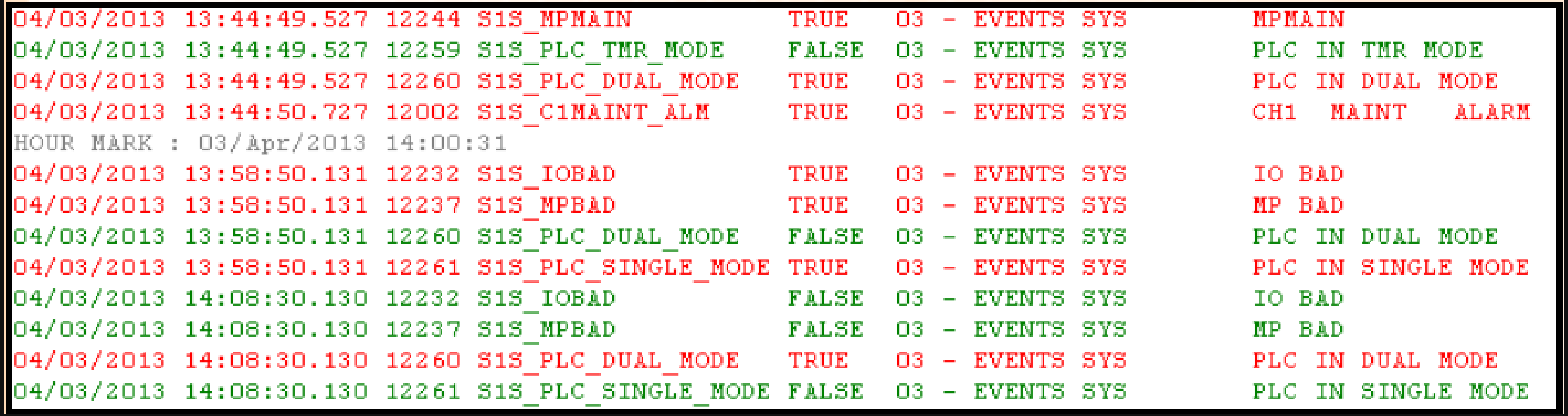
https://www.slideshare.net/MarinaKrotofil/s4x16-europe-krotofilgranulardataflowsics

(some) Points to consider

TRITON incident

- During code injection, safety PLC generated alarms
- Why was there no operators’ reaction?

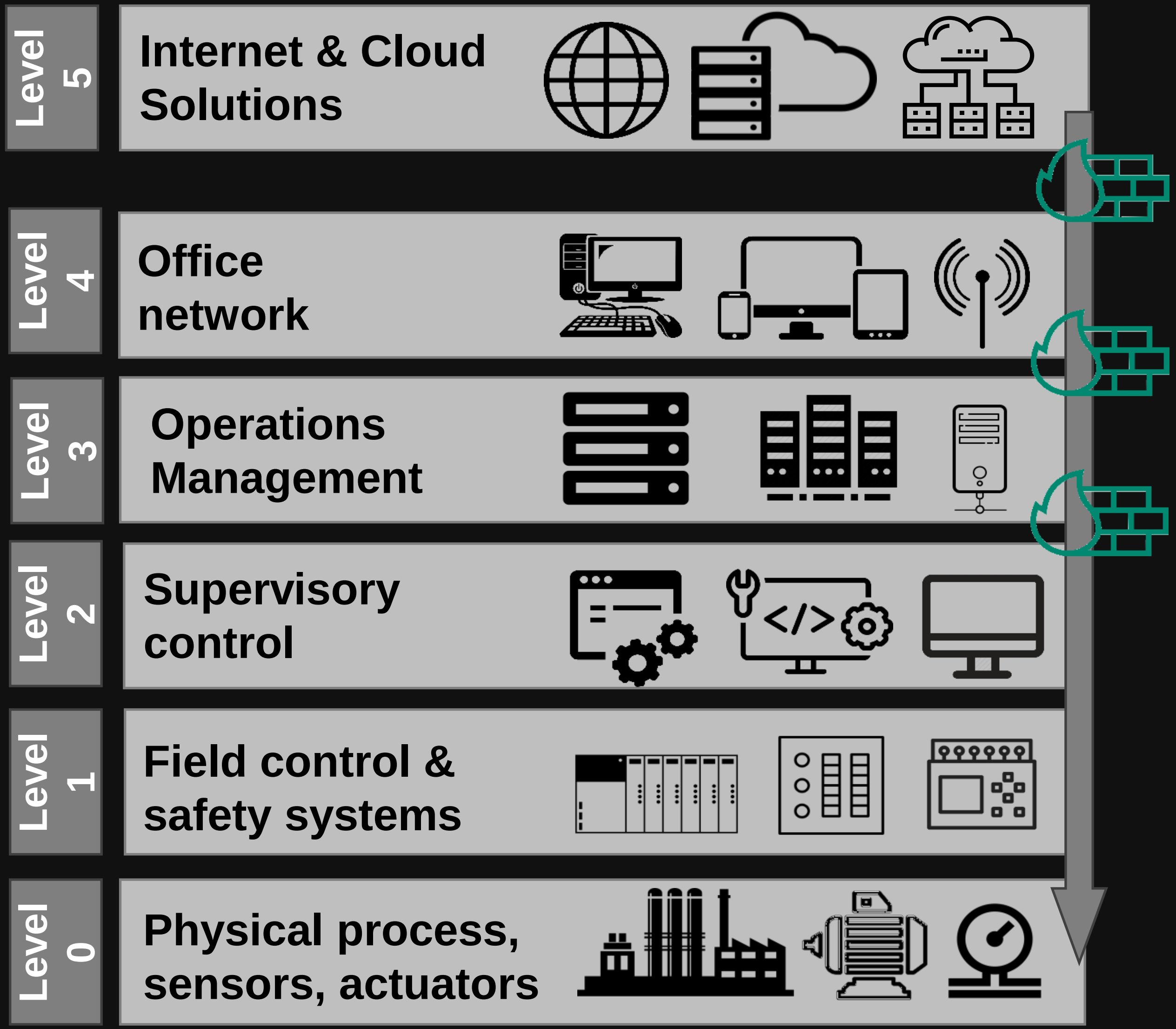
No existing procedures for collaboration between OT & IT.
Otherwise the incident could have been identiy during first plant trip



```
04/03/2013 13:44:49.527 12244 S1S_MPMAIN         TRUE   03 - EVENTS SYS        MPMAIN
04/03/2013 13:44:49.527 12259 S1S_PLC_TMR_MODE   FALSE  03 - EVENTS SYS        PLC IN TMR MODE
04/03/2013 13:44:49.527 12260 S1S_PLC_DUAL_MODE  TRUE   03 - EVENTS SYS        PLC IN DUAL MODE
04/03/2013 13:44:50.727 12002 S1S_C1MAINT_ALM    TRUE   03 - EVENTS SYS        CH1  MAINT   ALARM
HOUR MARK : 03/Apr/2013 14:00:31
04/03/2013 13:58:50.131 12232 S1S_IOBAD          TRUE   03 - EVENTS SYS        IO BAD
04/03/2013 13:58:50.131 12237 S1S_MPBAD          TRUE   03 - EVENTS SYS        MP BAD
04/03/2013 13:58:50.131 12260 S1S_PLC_DUAL_MODE  FALSE  03 - EVENTS SYS        PLC IN DUAL MODE
04/03/2013 13:58:50.131 12261 S1S_PLC_SINGLE_MODE TRUE  03 - EVENTS SYS        PLC IN SINGLE MODE
04/03/2013 14:08:30.130 12232 S1S_IOBAD          FALSE  03 - EVENTS SYS        IO BAD
04/03/2013 14:08:30.130 12237 S1S_MPBAD          FALSE  03 - EVENTS SYS        MP BAD
04/03/2013 14:08:30.130 12260 S1S_PLC_DUAL_MODE  TRUE   03 - EVENTS SYS        PLC IN DUAL MODE
04/03/2013 14:08:30.130 12261 S1S_PLC_SINGLE_MODE FALSE 03 - EVENTS SYS        PLC IN SINGLE MODE
```

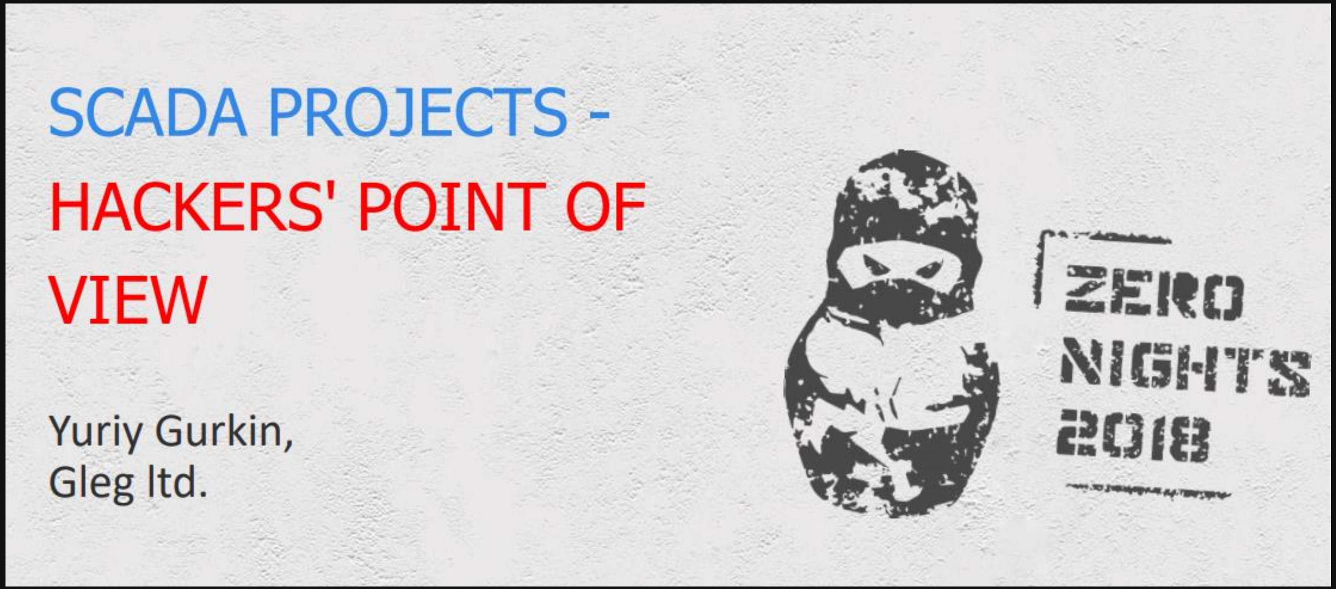
http://www.supracontrols.com/TriconexSOE%20PC_Interface.aspx

FAQ: But is not detecting at L1 too late?



- Even in corporate domain detection is done “in depth” (not only on perimeter or Internet DMZ
  - Other wise why do even bother with vulnerability and patch management at L1-L2?

FAQ: But is not detecting at L1 too late?



SCADA PROJECTS - HACKERS' POINT OF VIEW

Yuriy Gurkin,
Gleg ltd.

- Project files are trusted files and always allowed to be brought in
- Bypass all layers of protection in upper network layers
- Scanning with AV is not effective
- Immediate effect on industrial process
- Frontline vendors are also vulnerable

https://2018.zeronights.ru/wp-content/uploads/materials/21-SCADA-projects-from-the-point-of-view-of-hackers.pdf

https://habr.com/ru/company/croc/blog/353324/

Conclusions

Conclusions

- Even if the activities of the SOC and control room are in essence similar, it is important to be aware of each other differences:
    - Priorities
    - Vocabulary
    - Context
- OT domain has unique requirements in terms of responding to security events or incidents:
    - It is important to have suitable tools for incident analysis and resolution
    - It is important to collect relevant logs/have relevant visibility
    - Make Industry 4.0 great again!

Q & A

Marina Krotofil
@marmusha
marmusha@gmail.com