Cybersecurity protection of functional safety

Bruce Hunter

Tutorial at 2018 ASCSA conference.

Overview and Objective

- Cybersecurity fundamentals
- Critical infrastructure threat landscape
- Existing standards and frameworks
- Safety AND security culture
- Cybersecurity and safety compatibility
- Safety/security risk management
- Security architectures
- Access control
- Asset/configuration management
- Vulnerability and threat management
- Release management
- Incident Management
- Security testing

- Identify specific activities to apply cybersecurity to protect functional safety systems
- Intended for system safety practitioners dealing with cybersecurity risks
- Approx. 100 Minutes

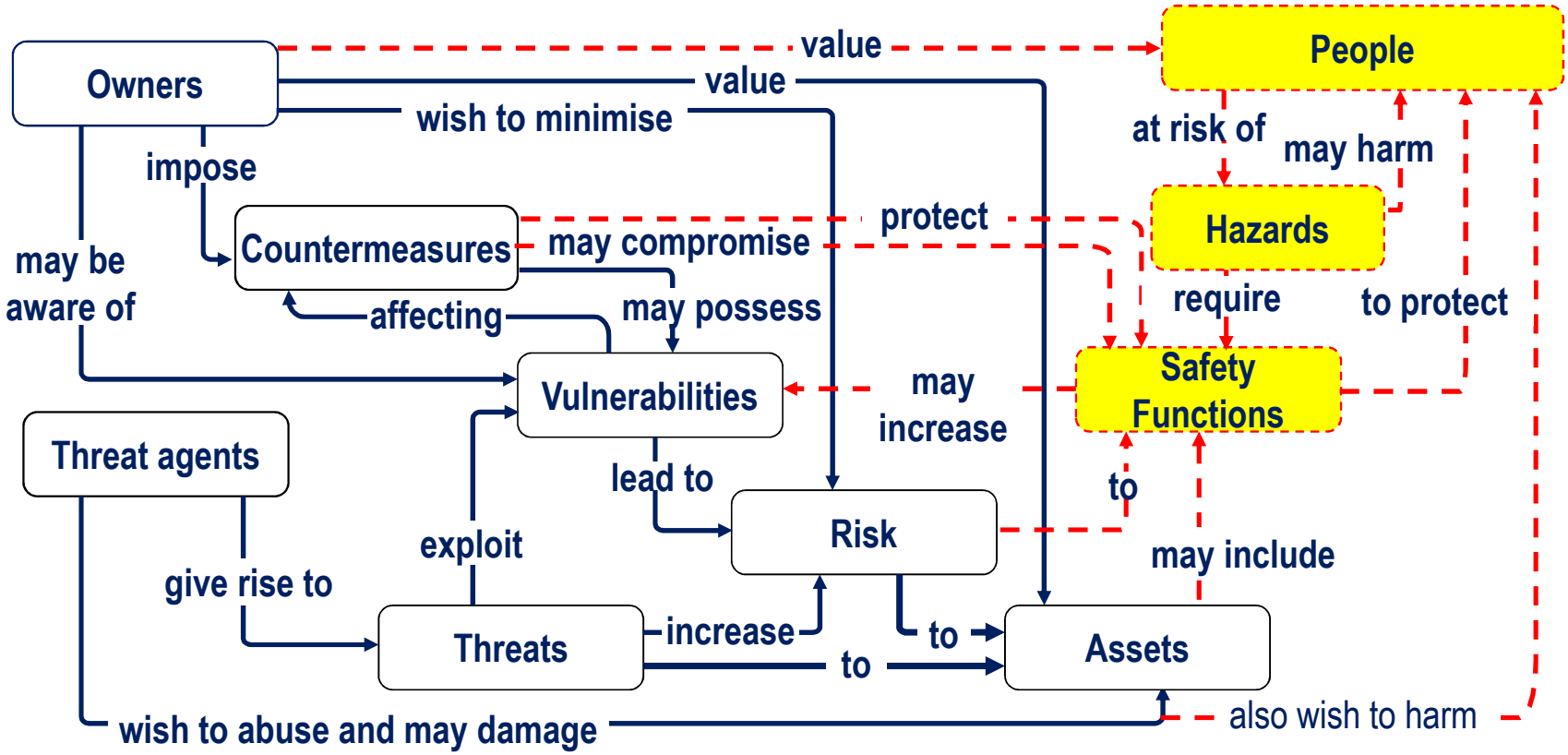
The problem

US FBI Director back in 2012 said “There are only two types of companies: Those that have been hacked, and those that will be.”

Does this now, in 2018, apply to safety systems?

Cybersecurity Fundamentals

Safety association



Adapted from IEC15408.1 (Common Criteria)

Hunter, B – Integrating safety and security in system lifecycle

The air-gap illusion

- Traditional safety systems have relied on an “air-gapped” architecture*
- IT-OT security incidents show the fallacy of isolation
  - Security by obscurity versus managed disclosure
  - Vulnerability in bypasses by people
  - Vulnerability of hidden architectures/dependencies
  - Exploitation of core technology vulnerabilities
  - Open architectures and protocols
- Technology designed on the premise of connectivity
- Walls and moats have never been a lasting defence◊

*NIST, ISACA, ICS-CERT

◊Anderson, J - *The wall is the wall: why fortresses fail*

Critical infrastructure threat landscape

INTENTIONAL

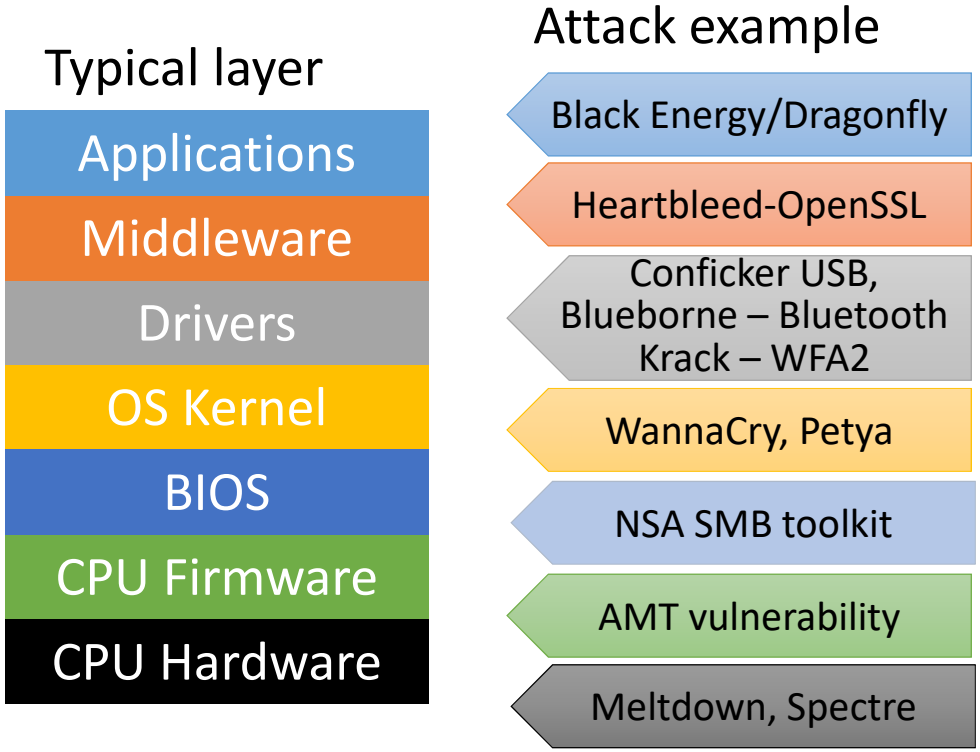
- 2000- Maroochy water treatment SCADA
- 2010 – STUXNET targeted exploitation of Siemens PLCs
- 2015..17 - Ukraine power grid, BlackEnergy, Industroyer, Dragonfly ICS specific malware (from The Register)
- 2017 - WannCry, NotPetya ransomware in OT systems
- 2017 – Intel i5 chipset vulnerability in PLCs
- Dec 2017 – Triton TRISIS – Saudi ESD compromised
- 2018 – Meltdown & Spectre speculative execution

UNINTENTIONAL

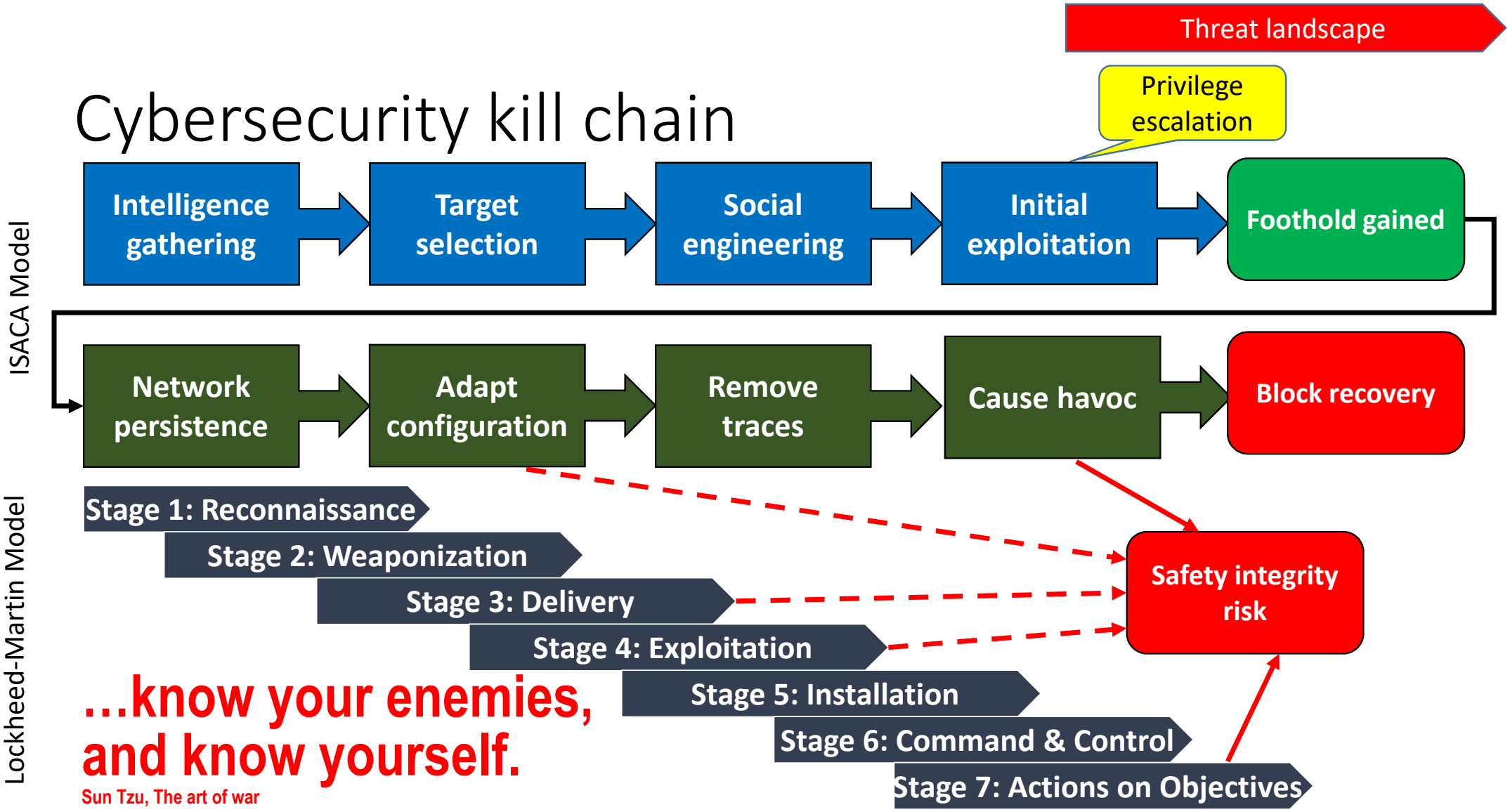
- Gas pipeline suffered shutdown on patch
- Various security software false positives
- Penetration testing crippled operational plant
- 2017 Melbourne speed cameras patch added malware

Technology Layer exploits/vulnerabilities

- Security threats look for new exploitation vectors
- Protection difficulty increases with layer depth (e.g. Meltdown and Spectre ICS-ALERT-18-011-01)
- Ingrained vulnerability zero-days (e.g. ix86 SPECint95)



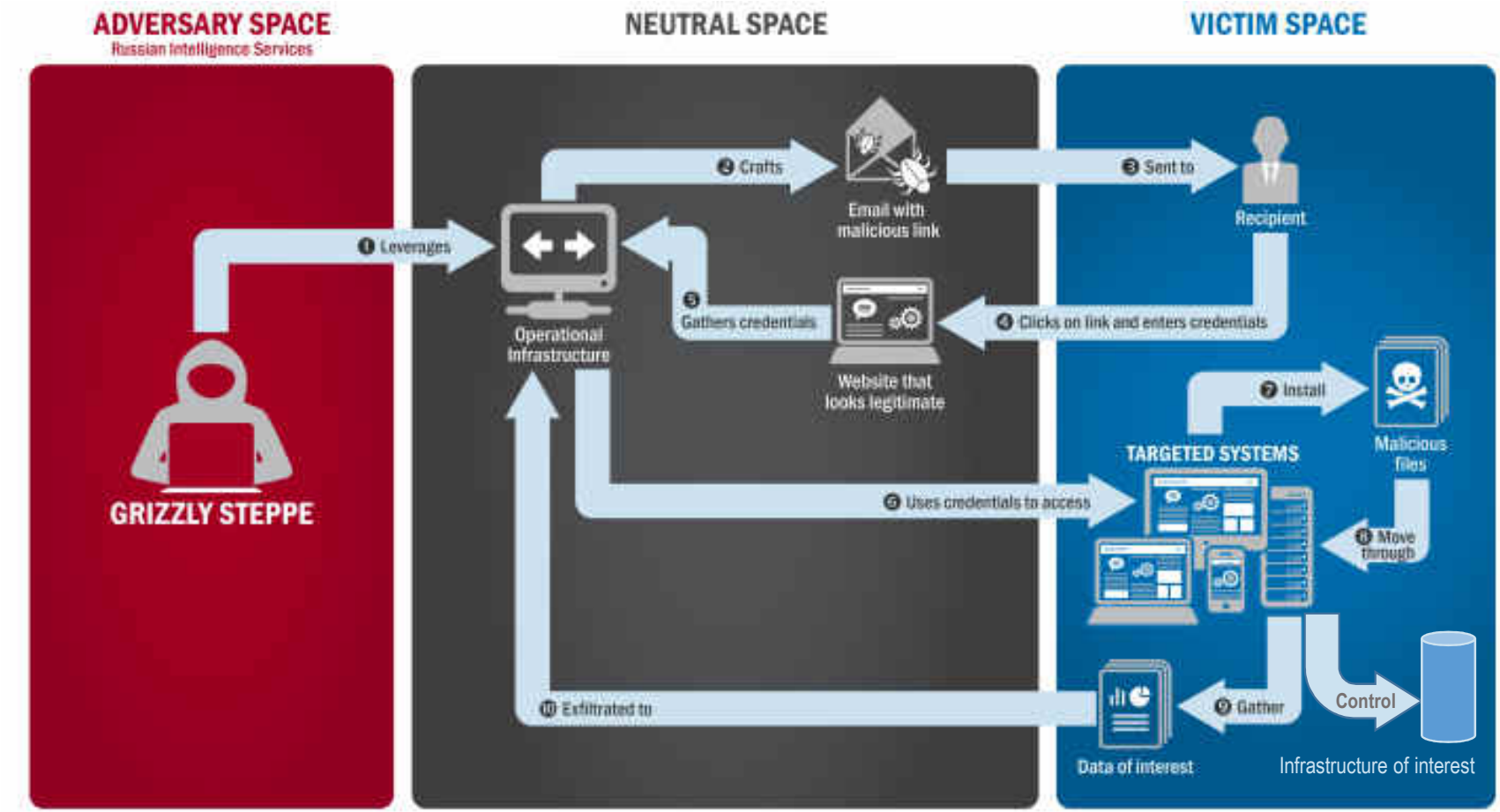
Cybersecurity kill chain



ICS Exploit case studies

Exploit	Damage	Exploitation path	Vulnerabilities	Attribution
Maroochydore 2000	Release of raw sewage	Physical exploit only Rogue wireless RTUs	Lack of asset/access control & monitoring	Disgruntled contractor (Boden,V)
Stuxnet 2010	Damage to centrifuges	Configuration exposure, ICS netwotk compromised Simatic PLCs compromised	MS08-067, MS10-061, MS10-073	Nation state(s)
BlackEnergy 2015 Aka Industroyer, Dragonfly	Ukraines energy blackout	Phishing campaign, local accounts, HMI takover	CVE-2014-4114, CVE-2014-0751	Nation state
Petya 2017 Aka-NotPetya, WannaCry(ptor)	Locking of health files and infrastructure	Lateral movement using windows PsExec, WMI, NSA derived EternalBlue/ EternalRomance	MS17-010 SMB vulnerability (NSA)	Cybercriminals & Nation state(s)
Triton 2017 HatMan, TRISIS MAR-17-352-01	Shutdown of Triconex ESD	Downloaded Python program to one ESD through compromised TriStation	Triconex firmware zero-day	Nation state

FBI analysis of APT29 attacks



US DHS-FBIJAR-16-20296A

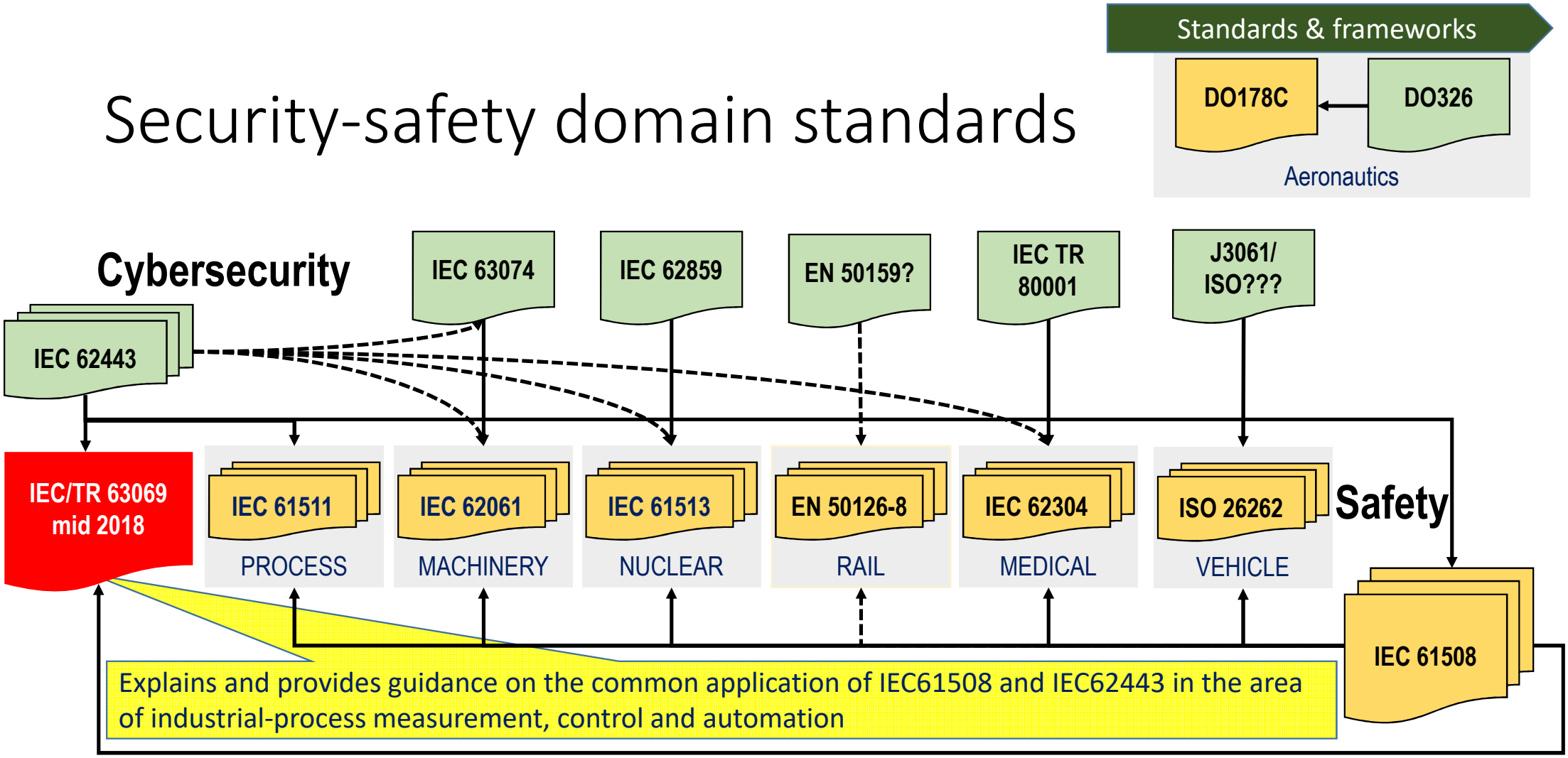
Standards and frameworks

What do standards require in protecting operational technology

Cybersecurity standards and frameworks

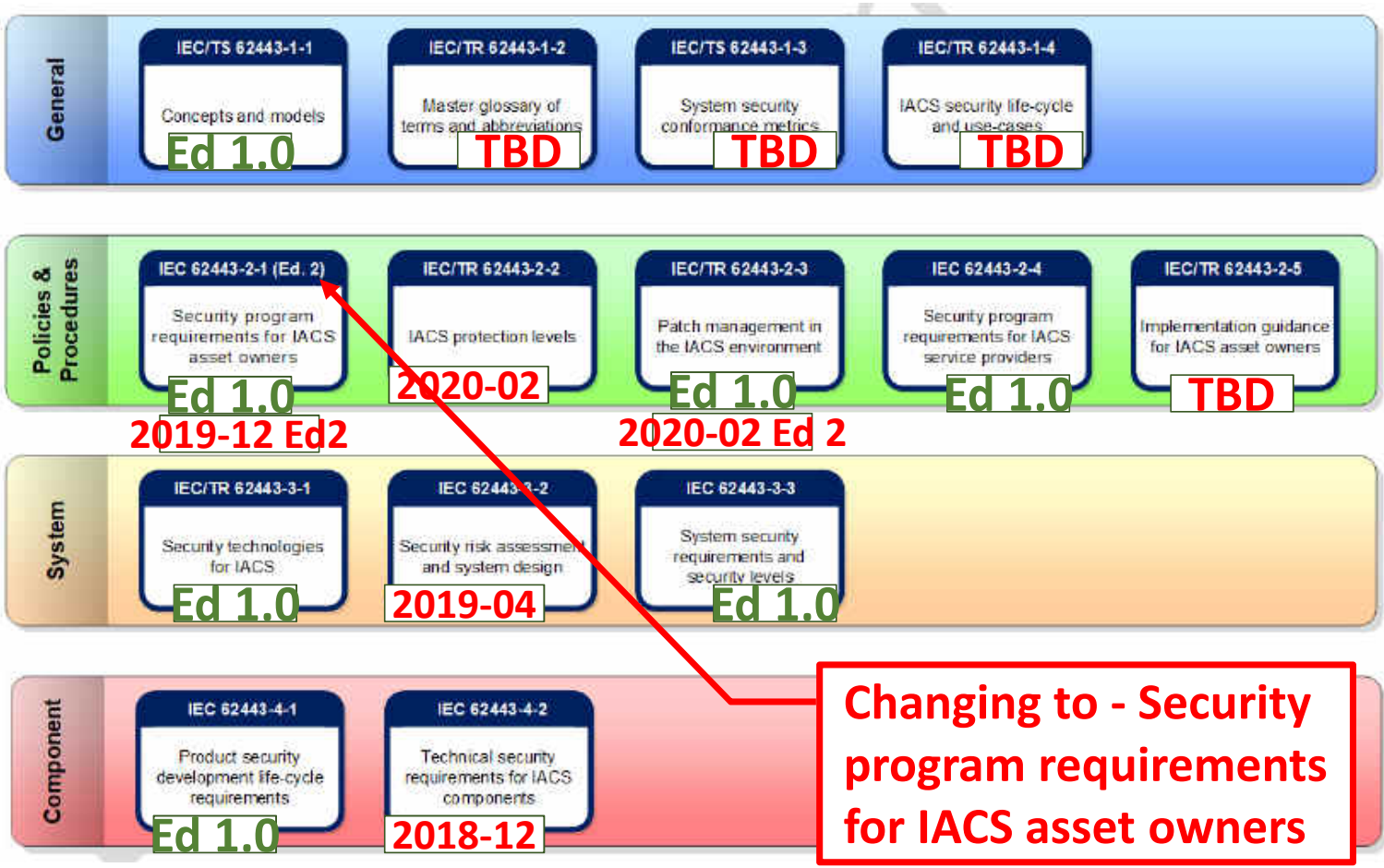
- NIST
  - NIST Framework for Improving Critical Infrastructure Cybersecurity - Cybersecurity Framework
  - SP 800-160, Systems Security Engineering
  - SP800-82 Guide to ICS security
- ISA/ISO/IEC
  - IEC 62443, Security for industrial automation and control systems
  - ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
  - ISO/IEC 27035, Information technology – Security techniques – Information security incident management
  - ISO/IEC 27036 Information technology – Security techniques Information security for supplier relationships
- Other
  - EINSA Communication network dependencies ICS/SCADA
  - ICS-CERT Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Security-safety domain standards

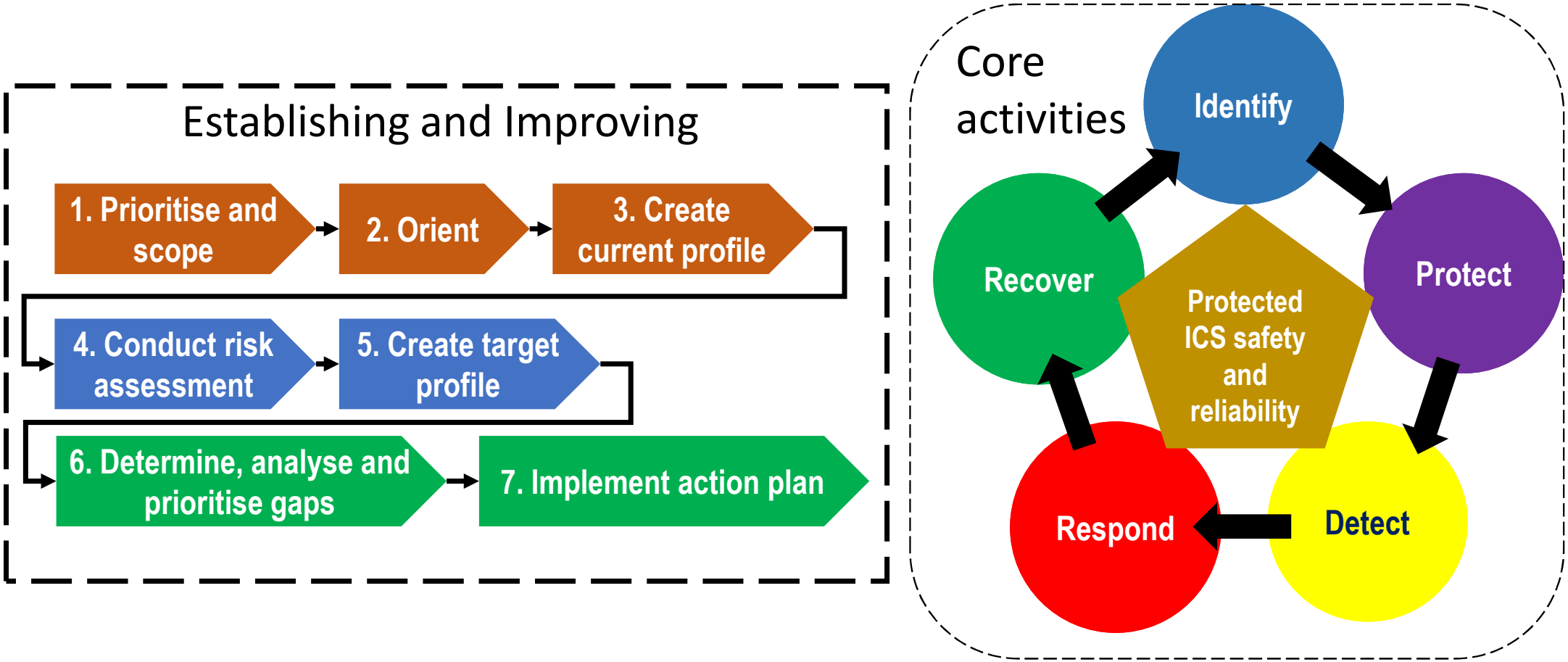


ISA/IEC 62443 series

- IEC 62443 de facto IACS security standard
- Comprehensive coverage of IACS design, operation & support
- Countermeasures must meet designated security level (SL) based on assessed risk
- 7/14 published

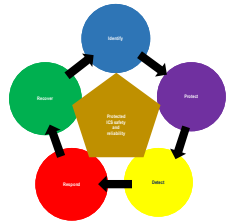


NIST Cybersecurity Framework



NIST Framework for Improving Critical Infrastructure Cybersecurity V1.0 2014

NIST Cybersecurity Self-Assessment – safety aspects



- **Identify** safety system
  - Assets, roles, dependencies, functions, regulations,
  - Related risks, communication, suppliers, impacts
- **Protect** safety system
  - Access, awareness, network
  - Configuration baseline and changes, backup systems
  - Incident response plans, fail-safe strategies
- **Detect** safety system cybersecurity events
  - Monitor for events, anomalies, vulnerabilities and threats
- **Respond** to protect system safety
  - Align security response with safety response
  - Ensure fail-safe as well as fail-secure
- **Recover** operation
  - To safe operating state
  - Joint lessons learnt and improvement

Cybersecurity documentation elements

- Required cybersecurity documentation in standards

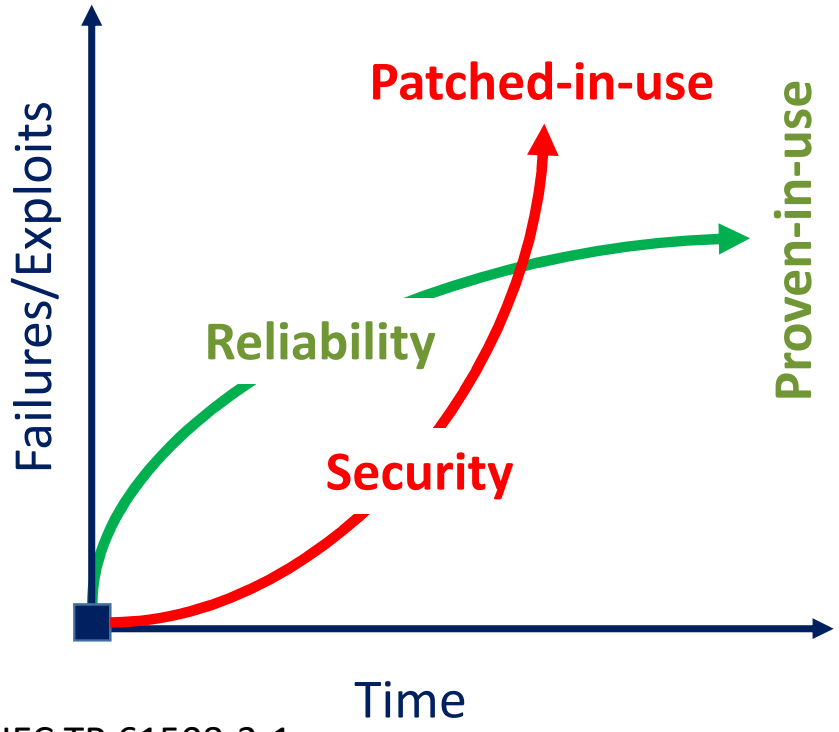
Document	Guiding standard and clause	Role
Safety Manual - cybersecurity dependencies	IEC 61508-3 Annex D	Equipment manufacturer or supplier
Security policies and procedures	IEC 62443-2-1 clause 4.3.2.6	Operator
Business continuity plan	IEC 62443-2-1 clause A.3.2.5	Operator
Patch test result	IEC 62443-2-3 clause 7.5	Supplier
Hardening guidelines	IEC 62443-2.4 clause 12.4	Equipment manufacturer of supplier
Network design document	IEC 62443-2.4 clause SP.03.03	System integrator
Cybersecurity requirement	IEC 62443-3-2 4.7	System designer
Product security requirements	IEC 62443-4-1 6.4	Product designer

Safety and security interaction

How do safety and security differ and how do we ensure they remain compatible?

The safety/security divergence

- Failure rate/integrity prediction
  - May be calculated from component or system reliability (wear-out) [1]
  - May be claimed if rigour requirements are met [2]
- Exploitation rate dependant on
  - Evolving threat actor capability
  - Evolving vulnerabilities and exposures [3]
  - Minimised by applying security requirements [3]



[1] IEC 61508-1
[2] IEC 61508-3, IEC TR 61508-3-1
[3]] IEC TR 62443-3-1 IEC 62443-3-3

Safety/Cybersecurity Review and Assessment

- Converge reviews and assessment

Review or assessment	Standard and clause	Safety and security interaction
Hazard and risk analysis	IEC 61508-3 clause 7.4	Ensure risk of malevolent and unauthorised actions are considered and assigned to security detailed threat and risk assessment.
Functional safety assessment	IEC 61508-3 clause 8	Ensure safety assessment includes the adequacy of security protection of safety functions and compatibility of security countermeasures employed.
High level security risk assessment	IEC 62443-3-2 clause 4.3	Ensure identification of cybersecurity risks in PHAR Ensure security risk context and perimeter includes safety aspects
Detailed cyber security risk assessment	IEC 62443-3-2 clause 4.6	Ensure detailed threat and risk assessment includes safety consequences of threats and incompatible countermeasures
Security implementation review	IEC 62443-4-1 clause 6.6. IEC 62443-4-1 clause 8.1	Ensure the security implementation adequately protects and is compatible with the functional safety of the system.
Security operation review	IEC 62443-2-1 4.4.3.2	Review continued protection of and compatibility with countermeasures with functional safety.
Incident response review	IEC 62443-2-1 clause 4.3.4.5	Review safety functions have been protected during the incident, safe state has been maintained during disruption and functional safety has been re-established with the system.
Operation and maintenance handover review	IEC 62443-2-1 clause 4.1.5 and 4.1.6	Review that the operator of the initial or transferred system has the necessary resources to operate and maintain the system in a safe and secure manner with all essential documentation and tools.
Overall operation and maintenance planning	IEC 61508-3 clause 7.7	Ensure operation and maintenance planning includes cybersecurity countermeasure maintenance and incident response

Cybersecurity countermeasure risks

- Include countermeasure risk in safety risks

Countermeasure/ Activity	Risk to safety function	Possible mitigations
Penetration testing	Could disrupt safety system or cause uncommanded dangerous operation	Have safe and proven penetration testing tools – isolate dangerous operation
Patching incompatibility	Could disrupt safety system or cause uncommanded dangerous operation	Verify path in pre-production platform
AV false positive	Could stop safety functions	Verify AV update in pre-production platform
PKI certificates expiry	Could stop safety functions	
Firewall policy changes	Could stop safety communications	Validate and control firewall policy especially in safety conduits
Password expiry policy	Stop operator from enacting safety-related command	Ensure effective access control management
Intrusion Protection System	Could stop safety functions	Isolate IPS from critical safety zones

Managing safety and security risk

Bridging the risk management of safety and security

IEC 61508 Hazard and Risk Analysis extras…

7.4.2.10 …shall consider the following:

- hazardous event and the components that contribute
- consequences and likelihood of the event sequences for the events
- tolerable risk for each hazardous event
- measures taken to reduce or remove hazards and risks
- assumptions made during the analysis of the risks
- rates and equipment failure rates

For cybersecurity should include

- cybersecurity events
- safety consequences from cybersecurity risks
- security/safety risk tolerability aligned
- cybersecurity countermeasures
- cybersecurity assumptions
- cybersecurity countermeasure failure/ conflict

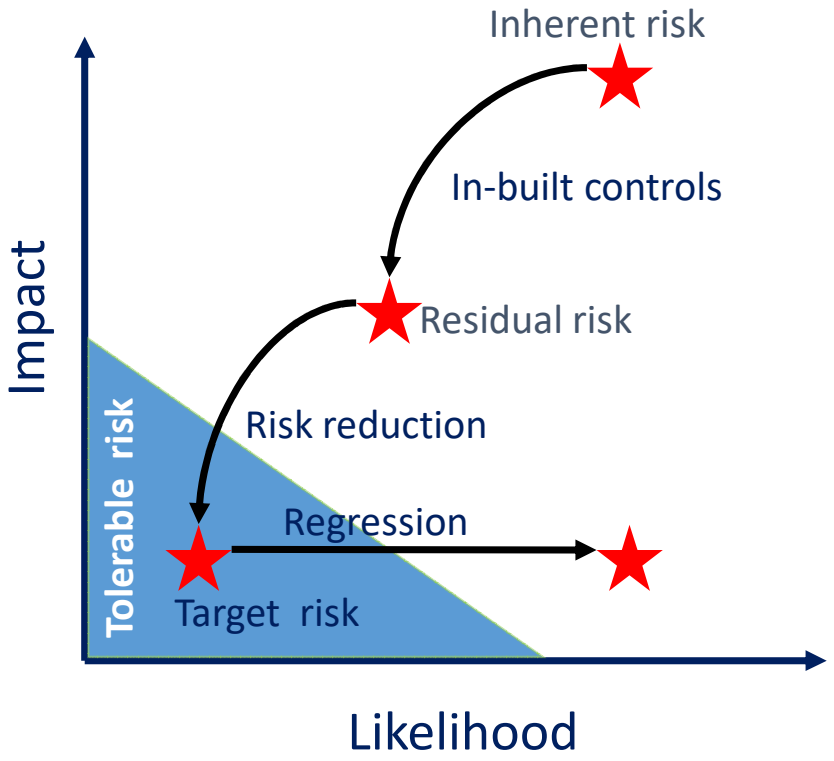
IEC 61511-1 Security risk assessment

8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);
- a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);
- a description of the potential consequences resulting from the security events and the likelihood of these events occurring;
- consideration of various phases such as design, implementation, commissioning, operation, and maintenance;
- the determination of requirements for additional risk reduction;
- description of, or references to information on, the measures taken to reduce or remove the threats.

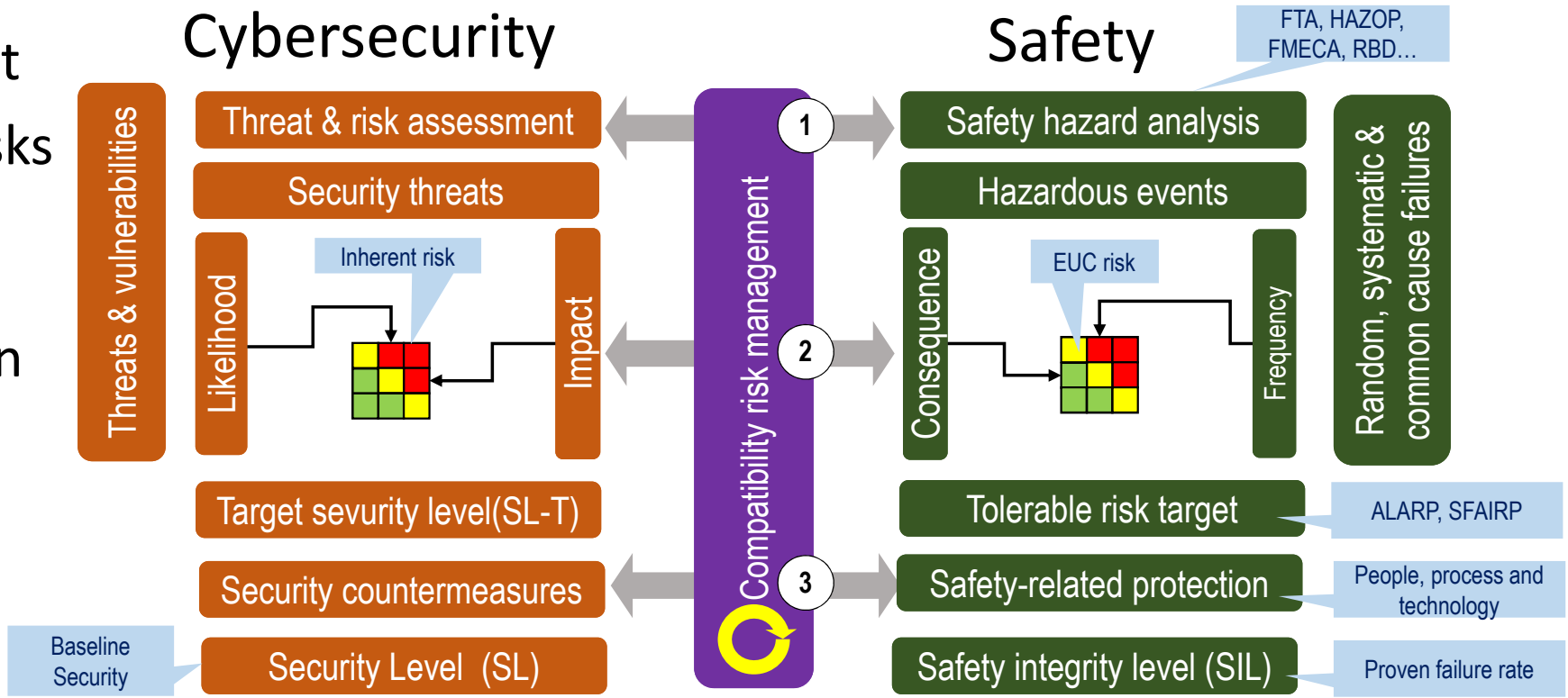
Safety/Security Risk Approach

- Improve risk coverage
  - Broad context establishment
  - Risk cooperation across domains
  - Risk communication across domains
  - Address cognitive bias
- Prevent risk regression
  - Change management review
  - Lifecycle risk review
  - Address evolving vulnerability exposures
- Allow for nondeterministic likelihood
  - Rely on multiple layers of separation

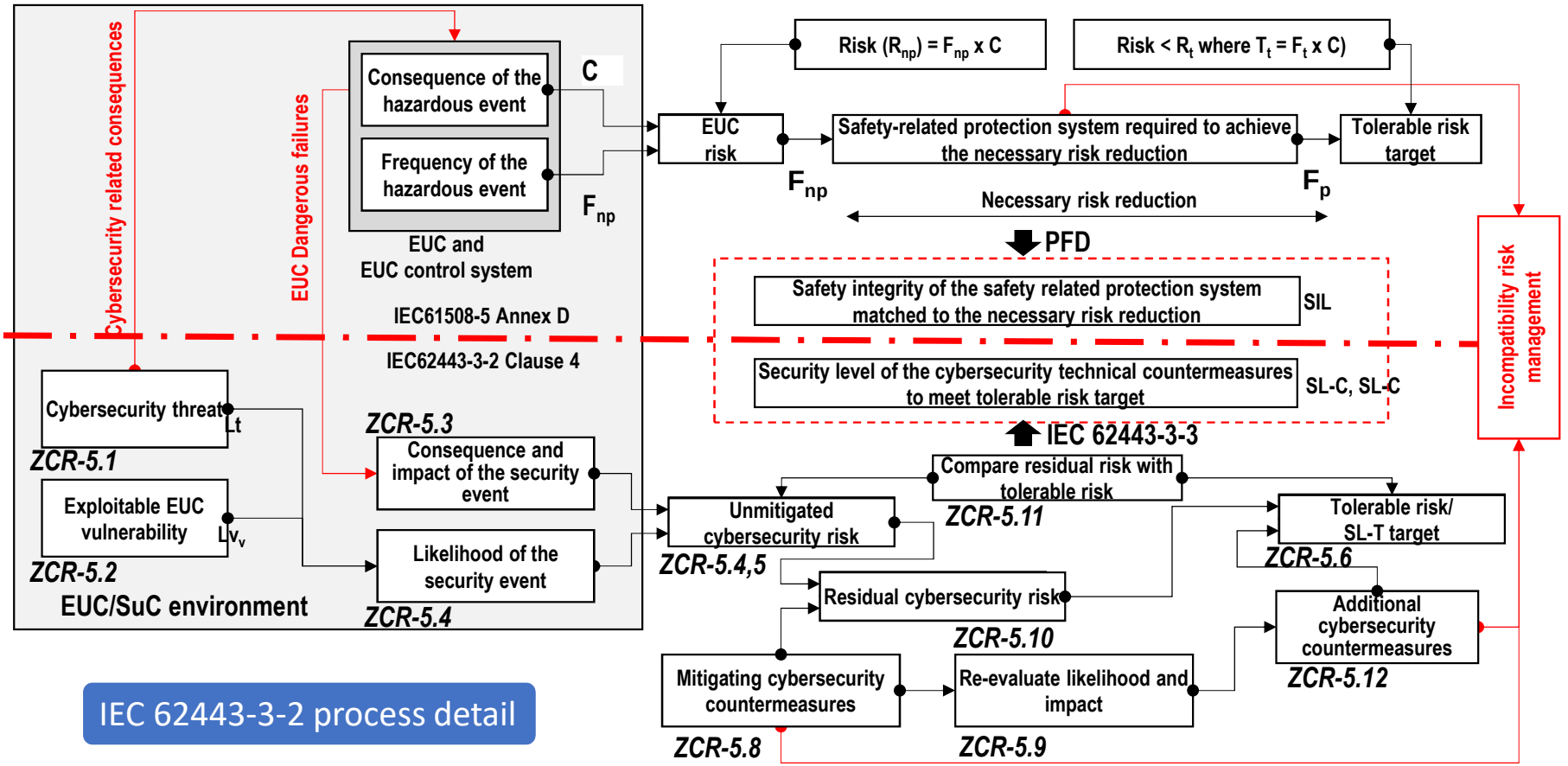


Safety/Security Risk – interaction

1. Align context
2. Associate risks and impacts
3. Harmonize and maintain controls



Example IEC 61508/IEC 62443 risk alignment



IEC 62443-3-2 process detail

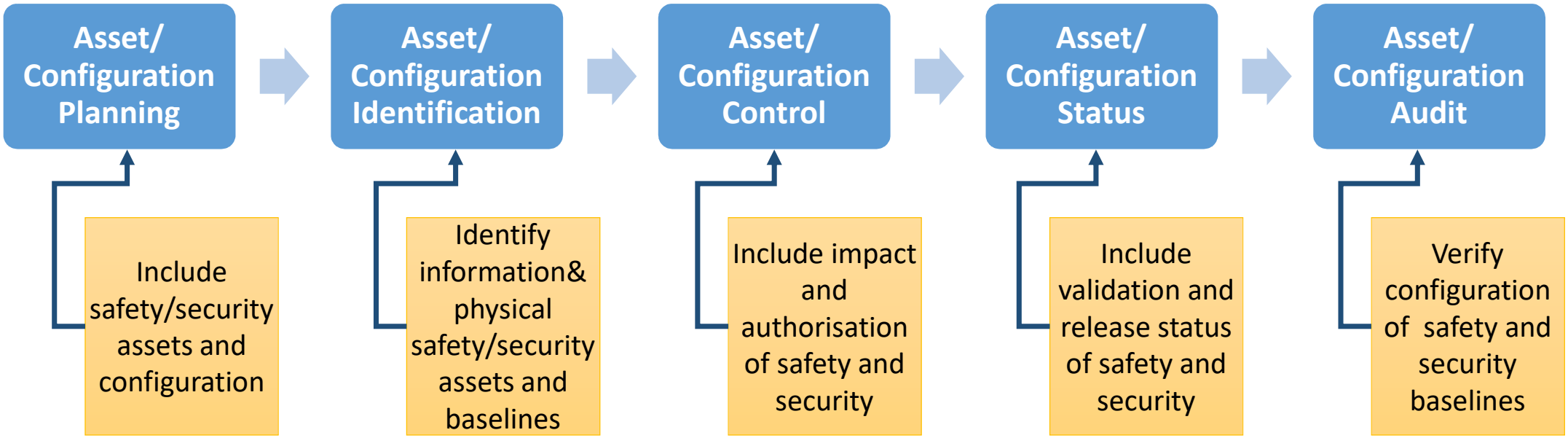
Example security addition to Hazard log

- Cross link potential cause of hazard with cybersecurity threat
- Show security countermeasure status in hazard log
- Revisit security risk and countermeasures with exploit alerts or attack surface changes
- Revisit hazard log with changes to security risk
- Include risk of security countermeasure causing safety risk

Hazard ID	System / Activity Category	Sub-system / Specific Activity	Hazard Description	Location	Potential Cause(s)	Public	Passenger	Staff	Contractor	Environment	Service Disruption	Effect(s)/ Consequence(s)	Frequency	Severity	Risk Index	Hazard Controller (Projects)	Proposed Safeguard shall be detail specified by following stage (1) Design - Design submission / specification ref. (2) Construction - Construction Plan (3) Testing & Commissioning - T&C activity / test record / check / procedure ref. (4) O&M - Operation / Maintenance procedure ref.	Frequency	Severity	Risk Index	Remarks

Asset and configuration management

- If you don't know your assets you can't control their risk!
- If you can't control them, someone else will!
- Manage all physical and information assets e.g. equipment, whitelists



NIST SP800-160 Systems Security Engineering CM1-5

Protecting safety systems

Cybersecurity culture

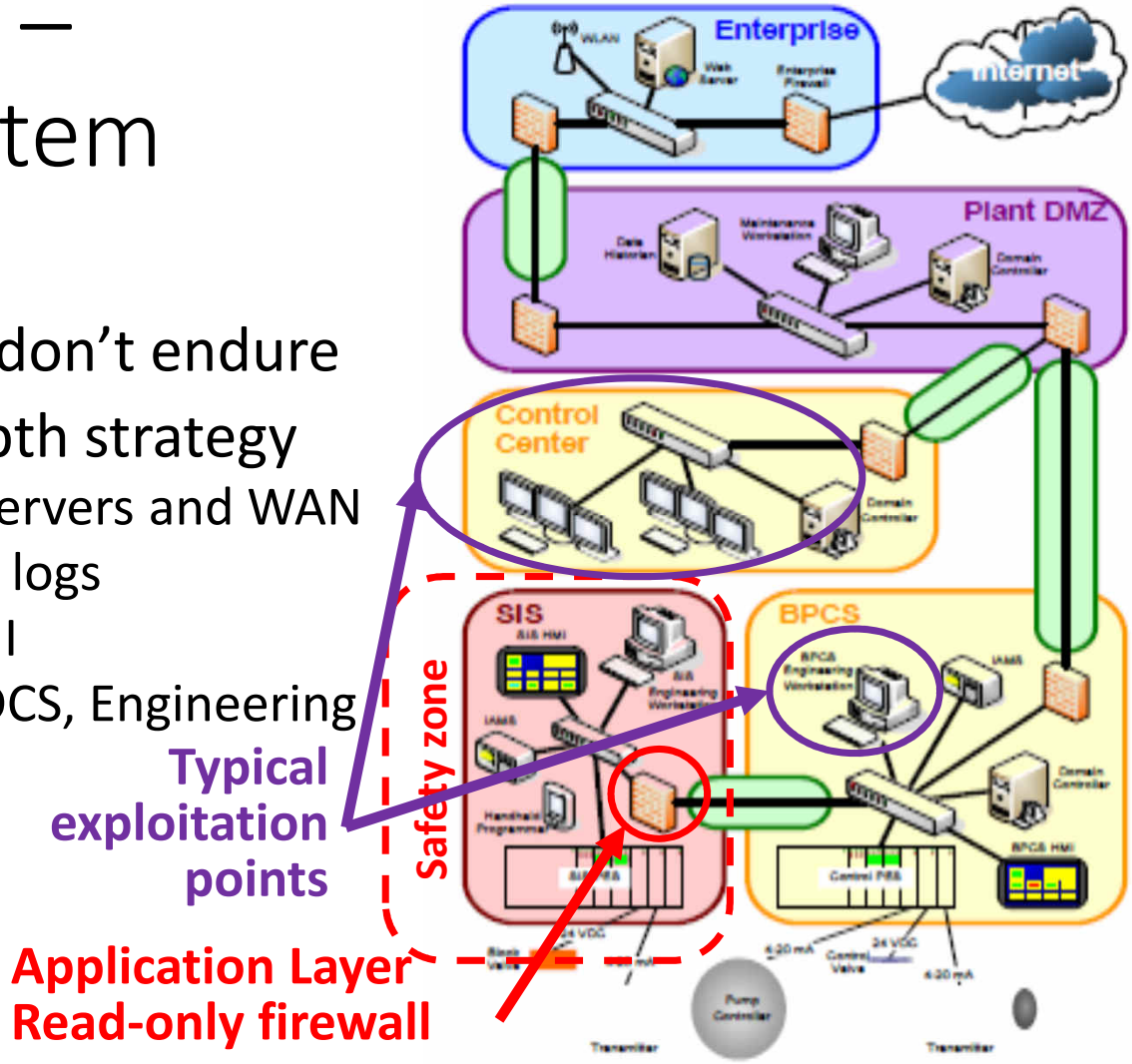
- Like safety, system insecure unless proven otherwise
- Security policies are key to protecting the system
- Human behaviour is a key vulnerability
  - Temptation is still to click on links, even when warned
  - Social engineering exploitation of choice
- Human awareness is a key security asset
  - Threat Landscape awareness
  - Kill chain awareness and indications
  - Incident response awareness and roles
- Need to have security culture as strong as safety culture

Fostering security awareness

- Cross-train domain specialist
  - cybersecurity risks
    - Industry specific assets, threats, vulnerabilities, exploits
  - safety risks
    - Impact of cyber attacks on system safety
- Address human vulnerabilities
  - Social engineering, Accidental exposure
  - Insider attacks – suspicious behaviour, police checks
- Educate operational staff on system specific cybersecurity
  - E.g. SANS, ISACA, ACS

Security Architecture – Industrial Control System

- As in warfare, walls and moats don't endure
- Better to have a defence-in-depth strategy
  - Level 4 – Enterprise zone – webservers and WAN
  - Demilitarized Zone – proxies and logs
  - Level 3 – Plant control zone - HMI
  - Level 2 – operation zone – PLC, DCS, Engineering
  - Level 1 -
    - BPCS – HMI, Eng. Workstation
    - Isolated Safety zone – SIS
  - Layer 0 – field devices – fieldbus



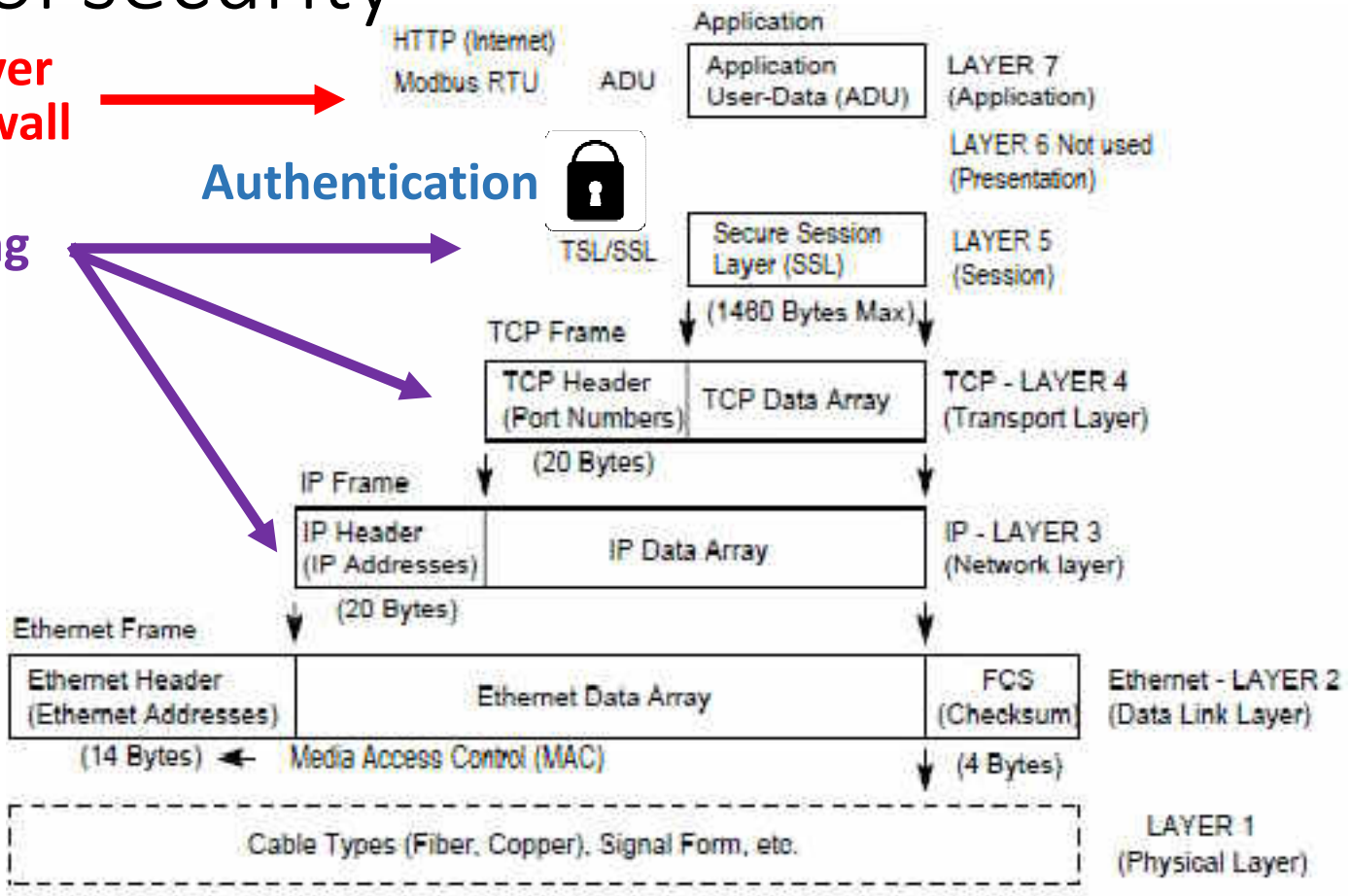
Network protocol security

Application Layer
Read-only firewall

Authentication

Firewall filtering

Strict device addressing



Security components

- **Zone** - grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access
- **Conduit** - logical grouping of communication channels that share common security requirements connecting two or more zones
- **Firewall** - inter-network gateway that restricts data communication traffic to and/or from one of the connected networks
- **Proxy server** – relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client
- **Demilitarized Zone (DMZ)** - isolation zone between a protected control network (CN) and external users, such that all production traffic "flowing" between the CN and those external users actually flows through a firewall to a proxy server and, where required by functionality, again through a second firewall

Access control

- User
  - Physical and logical access security
  - Based on least privilege
  - Role/Rule-based Access Control (RBAC)
- Zone equipment
  - Servers, workstations, devices
- Conduit communications
  - VLAN, WiFi, VPN, protocols etc.
- Authentication
  - Password policy enforcement – multifactor identification
  - PKI and certificate management
- Must meet safety needs
  - IEC 61511-1 11.7.3.2 The maintenance/engineering [and operating] interface shall provide the following functions with access security protection to each…

Protect

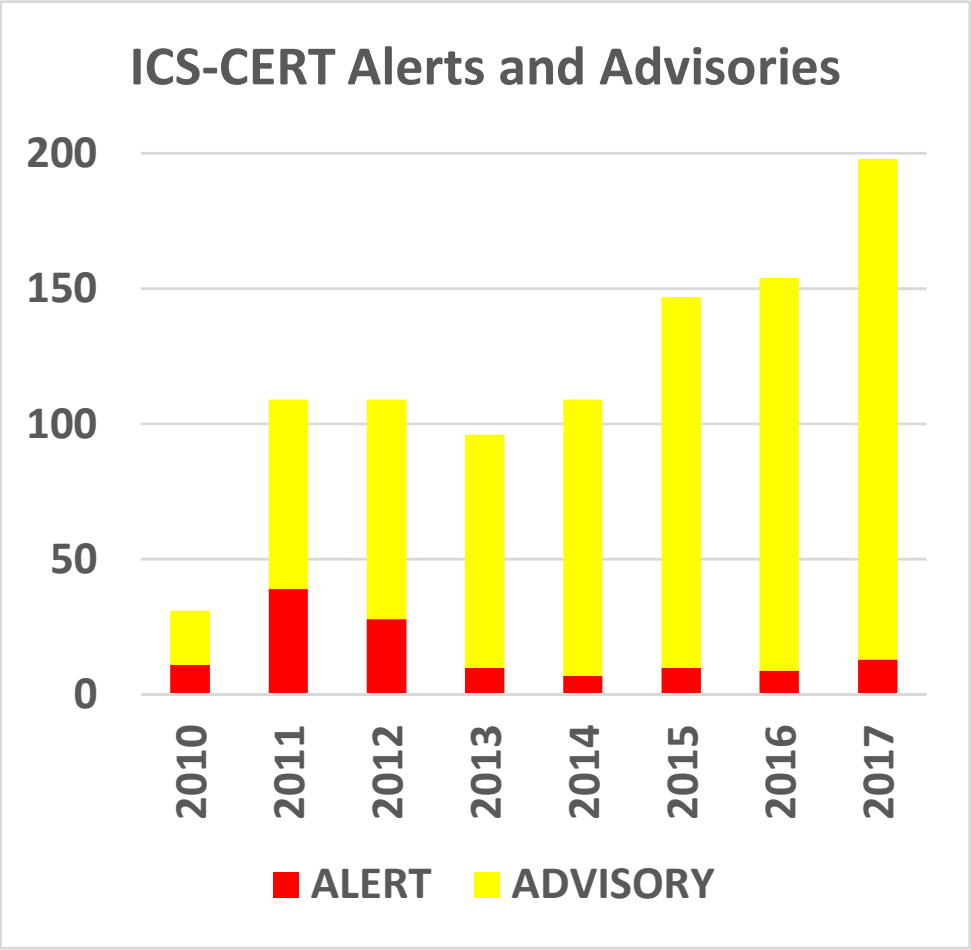
Vulnerability/threat management

Cybersecurity exploits

- Risks moving from IT to OT
- Expanding vulnerabilities and exploits
- Anticipated flood of risk to IoT

But…

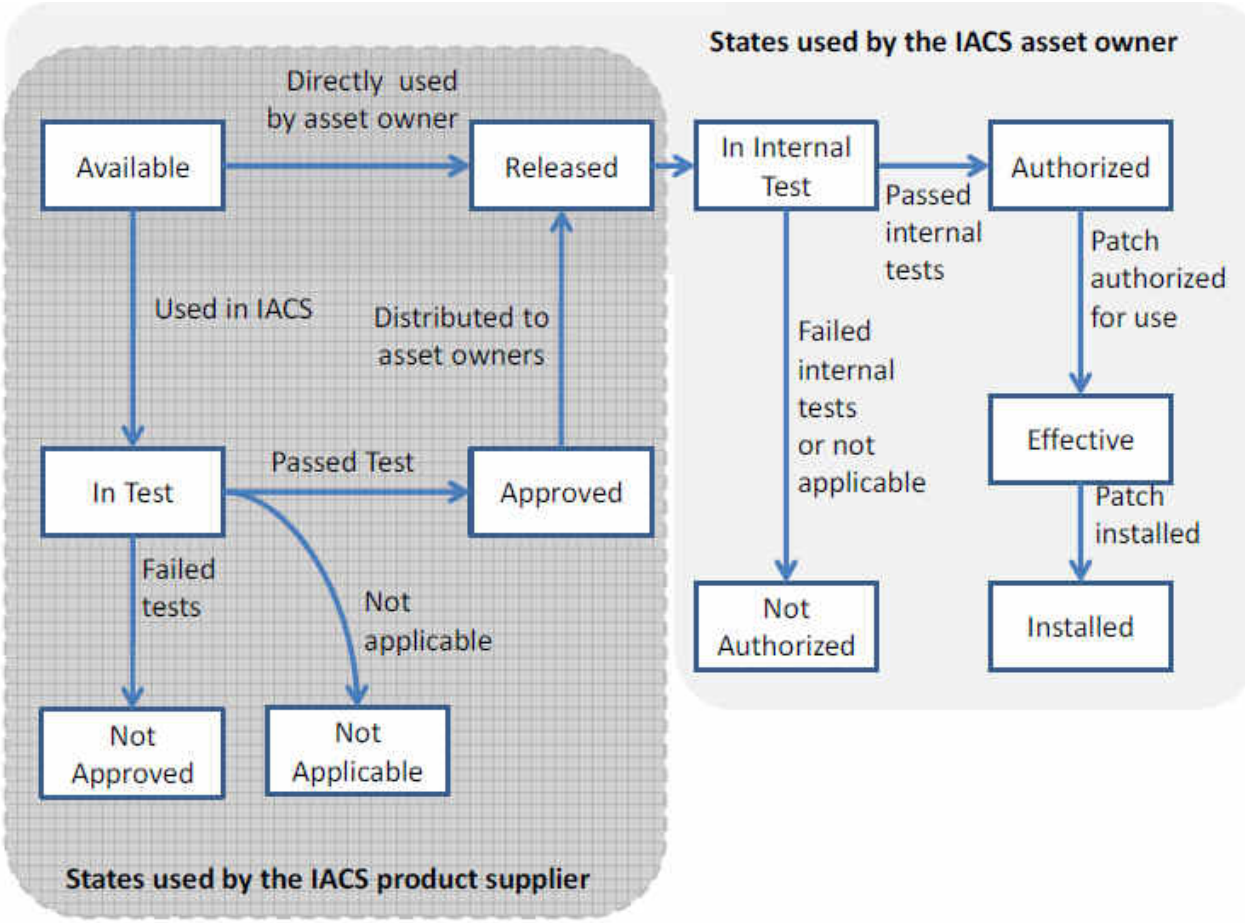
- Improved support from vendors
- Improved support from agencies
- Improved standards



Vulnerability and threat management

- A system is as insecure as the vulnerabilities not addressed
- Monitoring for new common vulnerabilities and exposures (CVE)
  - Monitor vulnerabilities and exploit authorities (CERT, ICS-CERT, MITRE)
  - Ensure awareness and actioning equipment manufacture security alerts
  - Assess applicability, risk and urgency of security patches and updates
  - Managing OS and application updates
  - Managing malware security software patches and updates
- Validating patches and updates
  - Patches not validated may impact reliability
  - Have roll-back if patches and updates have false positives
  - Baseline proven patches and updates, and roll-out to system assets
  - Update deployed system asset configuration baseline

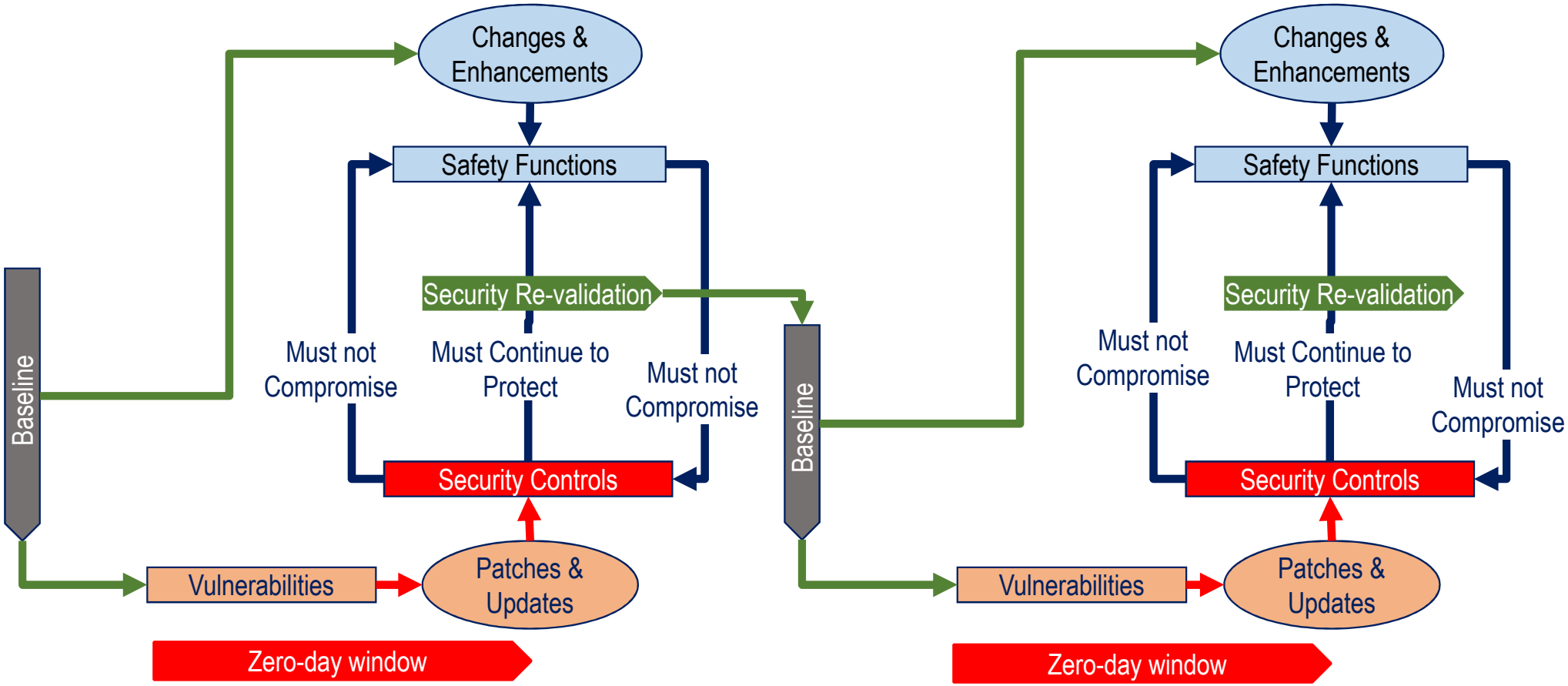
IEC TR 62443-2-3 security patch model



Typical vulnerability exposure: Profibus Telnet CVE-2014-6617

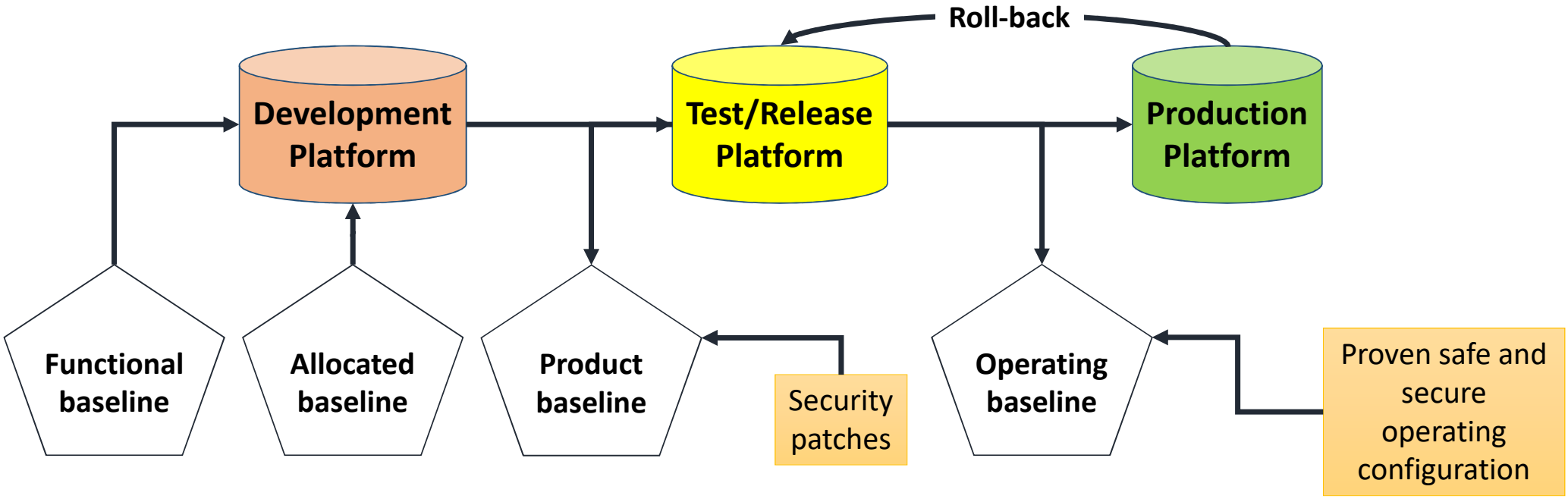
- Vulnerability Details : CVE-2014-6617
  - Softing FG-100 PB PROFIBUS firmware version FG-x00-PB_V2.02.0.00 contains a hardcoded password for the root account, which allows remote attackers to obtain administrative access via a TELNET session.
    Publish Date : 2018-03-09 Last Update Date : 2018-03-26
- CVSS Scores & Vulnerability Types
  - CVSS Score: 10.0
  - Confidentiality Impact: Complete (There is total information disclosure, resulting in all system files being revealed.)
  - Integrity Impact: Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
  - Availability Impact Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
  - Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
  - Authentication: Not required (Authentication is not required to exploit the vulnerability.)
  - Gained Access: None
  - Vulnerability Type(s): CWE ID 798
- Products Affected By CVE-2014-6617
  - # 1; Product Type – OS; Vendor - Industrial.softing; Product - Fg-100 Pb Profibus Firmware ;Version – Fg-x00-pb V2.02.0.00 ;
- Number Of Affected Versions By Product
  - Vendor Product Vulnerable Versions Industrial.softing Fg-100 Pb Profibus Firmware 1
- References For CVE-2014-6617
  - https://www.compass-security.com/fileadmin/Datein/Research/Advisories/CSNC-2014-005_softring_backdoor_account.txt
- Vulnerability Conditions
  - Vulnerability is valid if product versions listed below are used TOGETHER WITH(AND)
    - Industrial.softing Fg-100 Pb Profibus Firmware Fg-x00-pb V2.02.0.00
    - Industrial.softing Fg-100 Pb Profibus

Vulnerability Patching



Release management

- Control release process so that only safe and secure baselines are operated
  - Example platform process staging



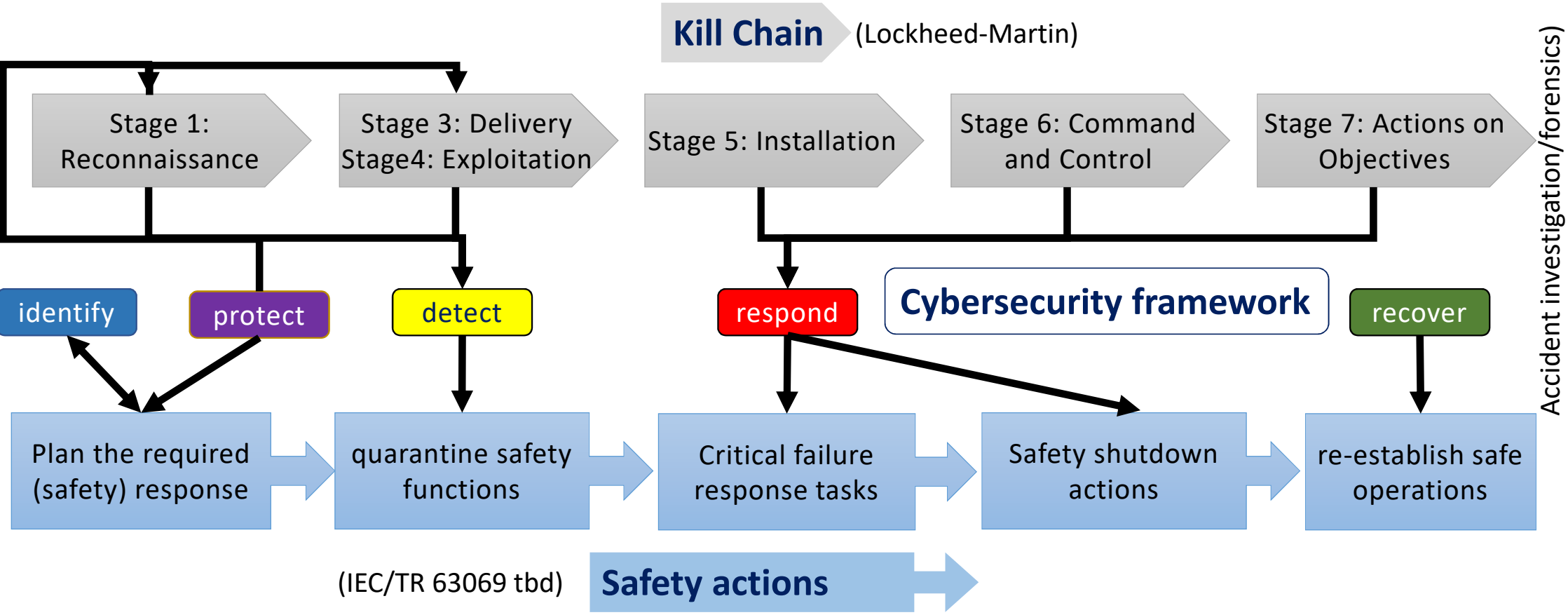
Handling safety/security incidents

How to handle cyber attacks and still keep the system safe

Detect Respond Recover

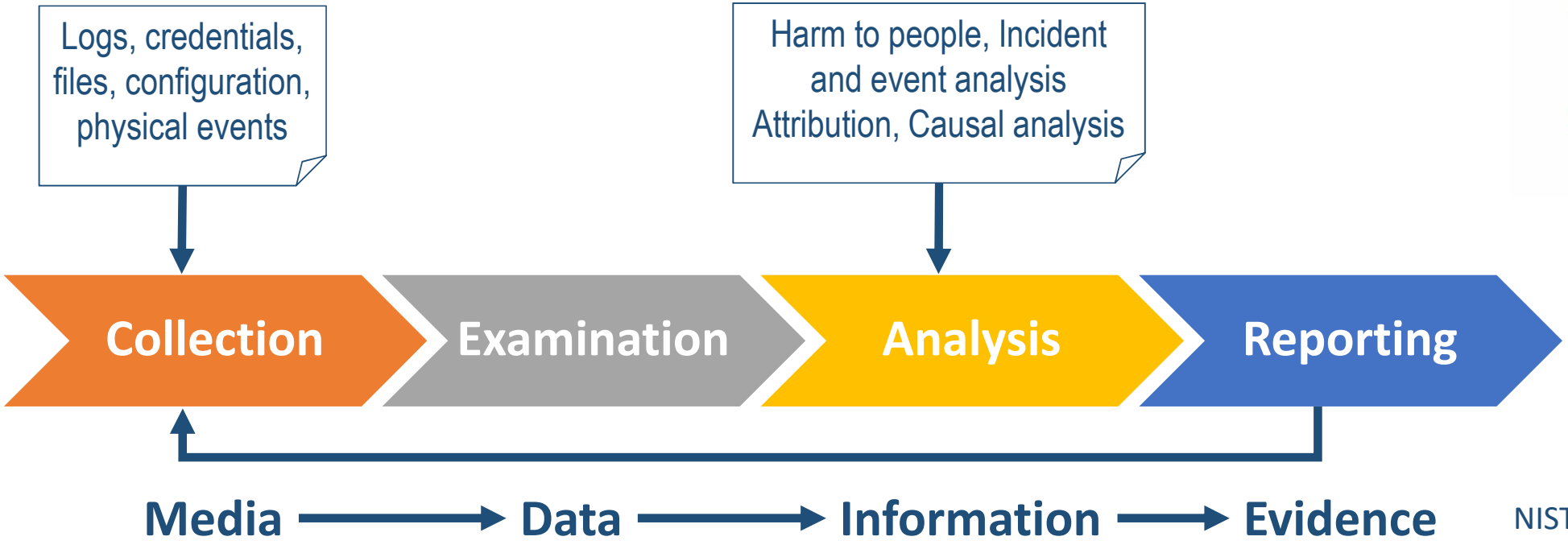
Incident and event management

Incident Management – Safety aspects



Cybersecurity and safety forensics

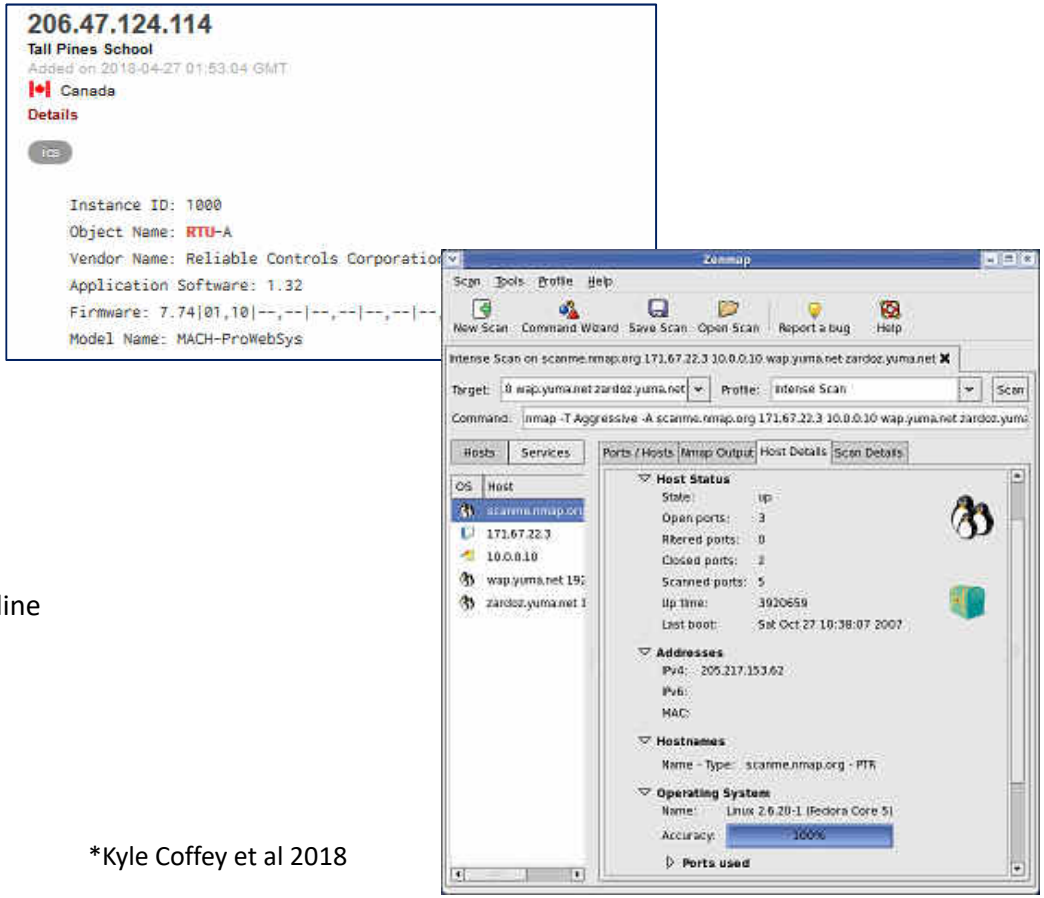
- Interacts with Accident Investigation if harm results
- Forensics rules applies to whole process – chain of custody



NIST SP800-86

Penetration testing – the safer way…

- Used to prove effective isolation of system
- Protect critical functions – misuse can be risky*
  - test off-line
  - isolate actuation
- Do not expose architecture
  - isolate from internet before testing
  - do not use cloud-based tools
  - do not use untrusted tools
  - do NOT use intense scanning
- Discovery tools
  - beware – this may expose data used in search
    - SHODAN HQ – searching for exposed equipment by name, port or function
    - Google dorks – beware – this will expose data used in search
  - NMAP-ZENMAP – mapping of network architecture – can be used off-line
- Traffic monitoring tools
  - Wireshark
  - tcpdump



Trend Micro "The SCADA That Didn't Cry Wolf" *Kyle Coffey et al 2018

Summary

- Safety systems are now a prime target for cyber attack
- Air-gapping or security-by-obscurity is no longer a certain protection
- Safety and security practitioners must cooperate to be effective
- Take a broad and coordinated approach to risk assessment
- Ensure cybersecurity countermeasures and safety are compatible
- Ensure robust safety plan for cybersecurity incident response
- Allow for cybersecurity forensics in accident investigation
- An insecure system is an unsafe system!

Questions

References - literature

- N. Mansourov, D. Campara. “System Assurance: Beyond Detecting Vulnerabilities”. ISBN: 9780123814142
- Anderson, J 2018 -The wall is the wall: why fortresses fail” warontherocks.com
- ICS-CERT Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- Trend Micro - Who’s Really Attacking Your ICS Equipment?
- ISACA 2017, “Exposing the Fallacies of Security by Obscurity - Full Disclosure”

References – Case studies

- Ralph Langner's Deep Dive on Stuxnet https://www.youtube.com/watch?v=zBjmm48zwQU
- ICS-CERT (ICS-ALERT-14-281-01E) – "Ongoing Sophisticated Malware Campaign Compromising ICS"
- Trend Micro "Who's Really Attacking Your ICS Equipment?" and "The SCADA That Didn't Cry Wolf"
- US-CERT Alert (TA17-181A) – "Petya Ransomware"
- US-CERT Alert (TA18-074A) "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors"
- Dragos Inc.,TRISIS Malware - Analysis of Safety System Targeted Malware
- T. Mahler and e. al, "Know Your Enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices," 2018
- Kyle Coffey et al., "Vulnerability Analysis of Network Scanning on SCADA Systems", 2018

References – threat/vulnerability libraries

- ICS-CERT The Industrial Control Systems Cyber Emergency Response Team - https://ics-cert.us-cert.gov/ - alerts, advisories & guidance
- Common vulnerabilities and exposures (CVE) - https://cve.mitre.org/
- CVE details - https://www.cvedetails.com/
- The register – security news and views - http://www.theregister.co.uk/security/
- The Risk Digest – forum for safety and security risks - http://catless.ncl.ac.uk/Risks/

References – useful training providers

- ISACA
  - CSX Cybersecurity Fundamentals certificate (on-line training available)
  - Certified Information Security Manager (CISM)
  - CSX Practitioner certificate (on-line training available)
  - CSX Virtual Cyber Academy including security labs
- ACS
  - Certified Professional (Cyber Security) and Certified Technologist (Cyber Security) certifications
- SANS
  - SANS Engineer Security Awareness training

References - standards

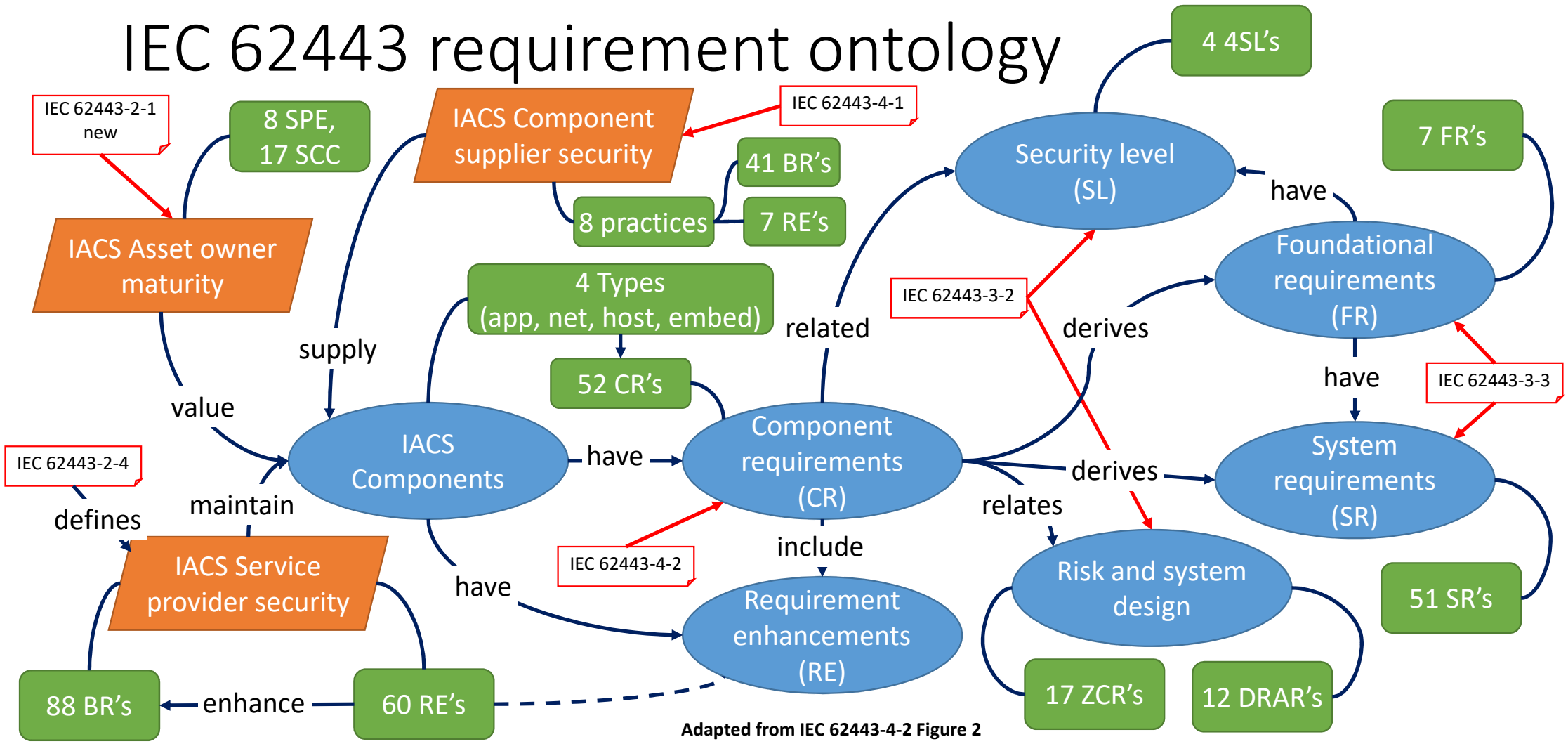
- IEC 61508: 2010, “Functional safety of electrical/ electronic/ programmable electronic safety-related”
- IEC 62443, “Security for industrial automation and control systems”
- Proposed IEC/TR 63069 Ed. 1.0 “Framework for functional safety and security”
- IEC 61511: 2016 Functional safety – Safety instrumented systems for the process industry sector
- AS 7770:2018 Draft, “Rail Cyber Security,” RISSB, 2018
- NIST, “Framework for Improving Critical Infrastructure Cybersecurity” (Cybersecurity Framework) 2014
- NIST SP 800-160, “Systems Security Engineering”
- NIST SP800-82, “Guide to ICS security”

Preview of IEC 62443 standards

The following pages summarise key safety related aspects of the IEC 62333 series. IEC 62443 is available for purchase from IEC webstore https://webstore.iec.ch/

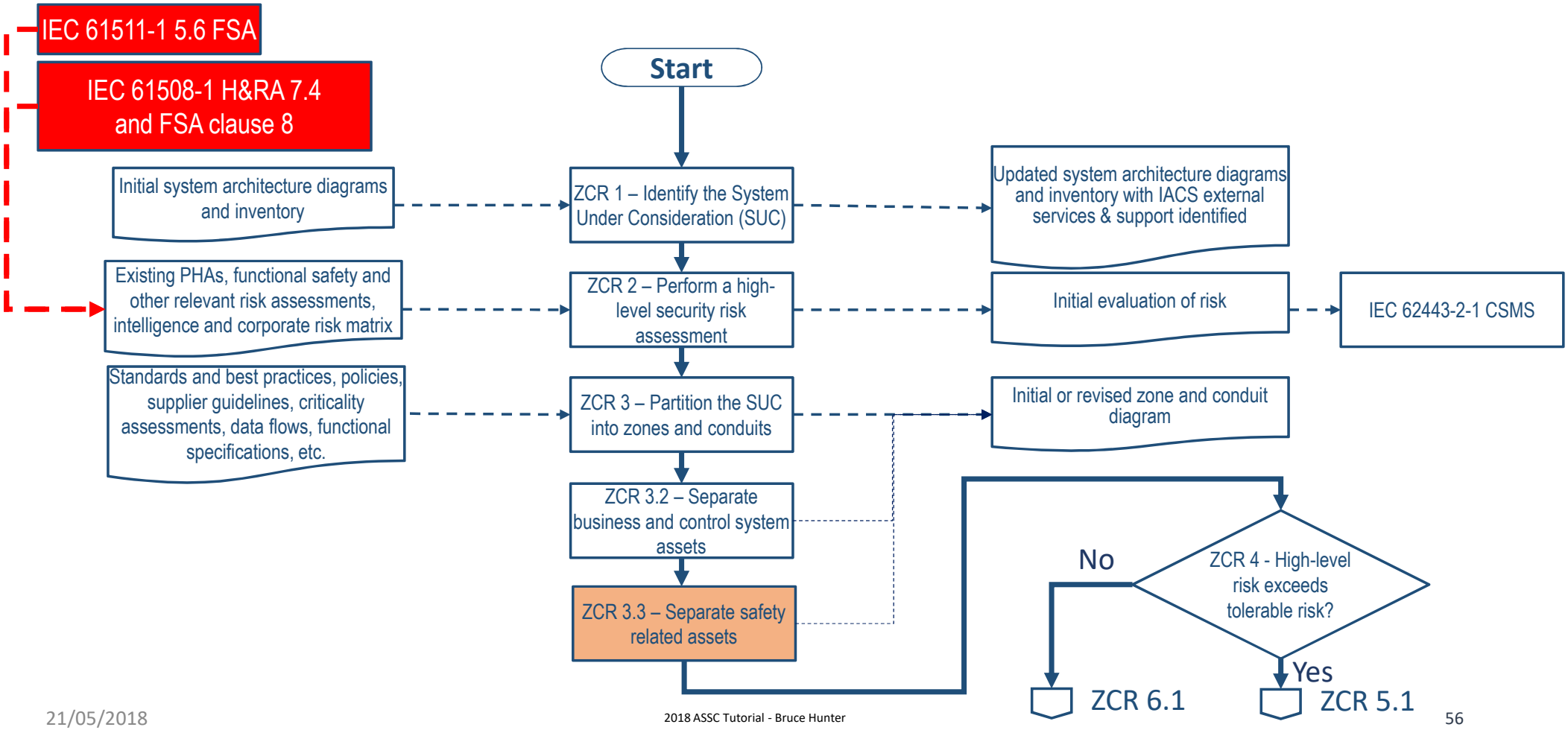
Standards & frameworks

IEC 62443 requirement ontology

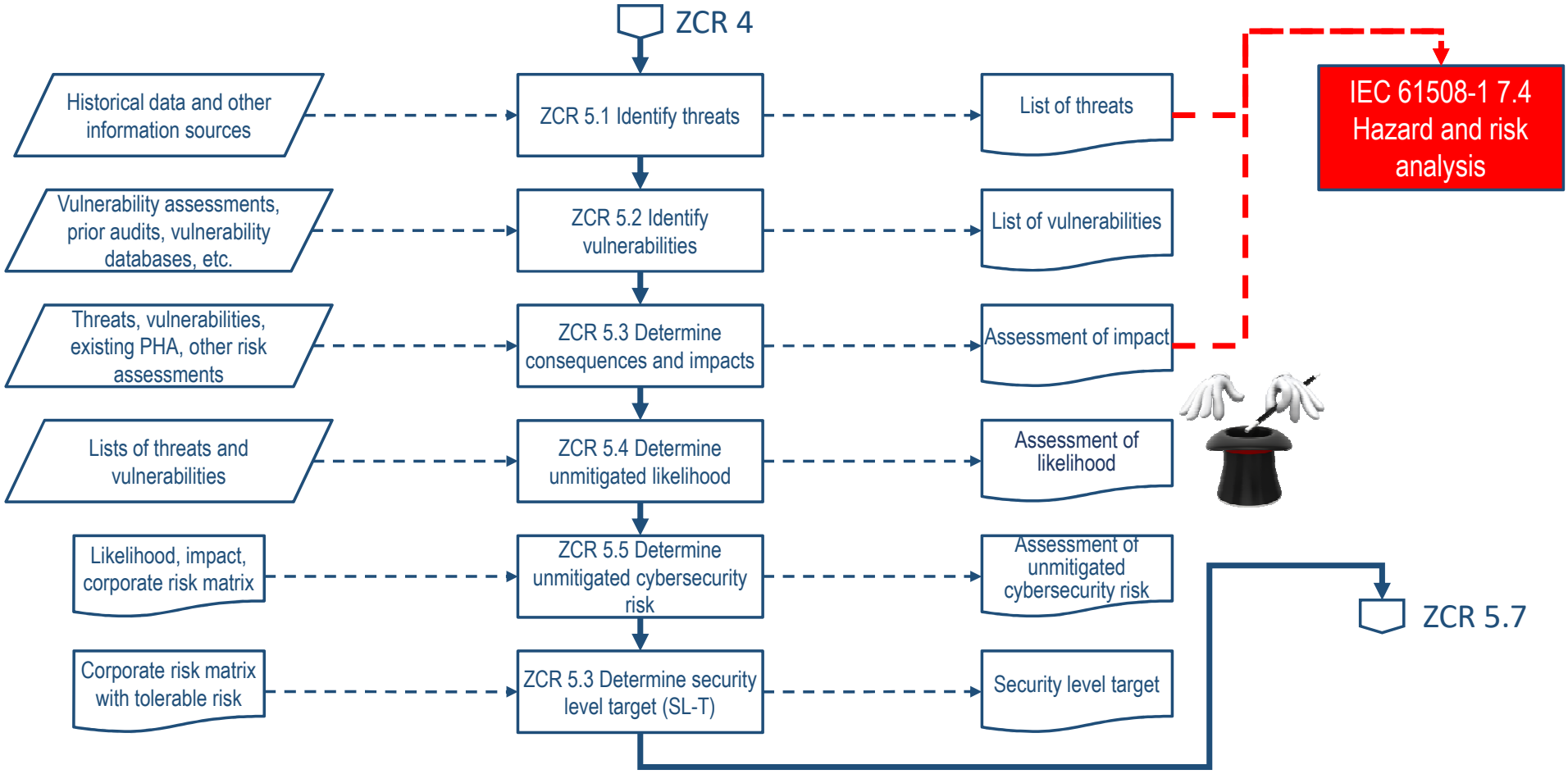


Adapted from IEC 62443-4-2 Figure 2

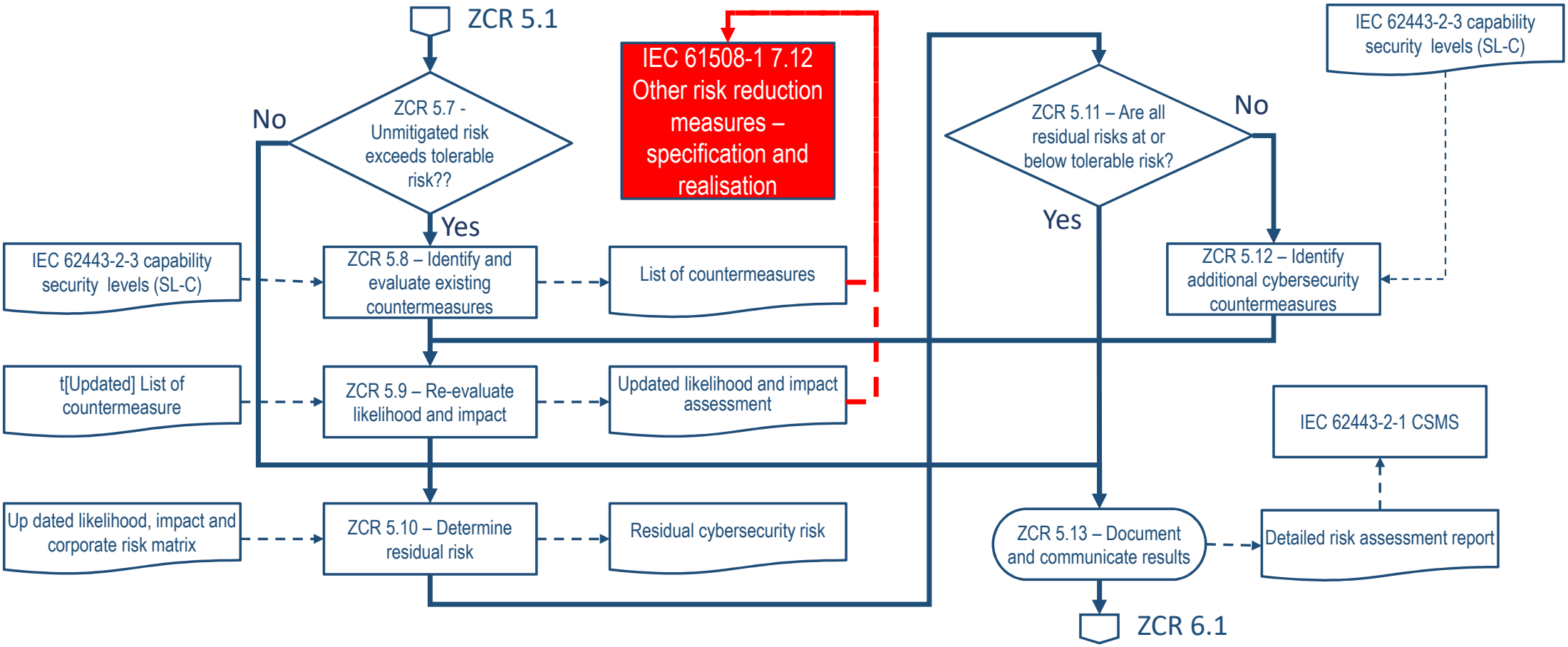
IEC 62443-3-2 Risk assessment 1



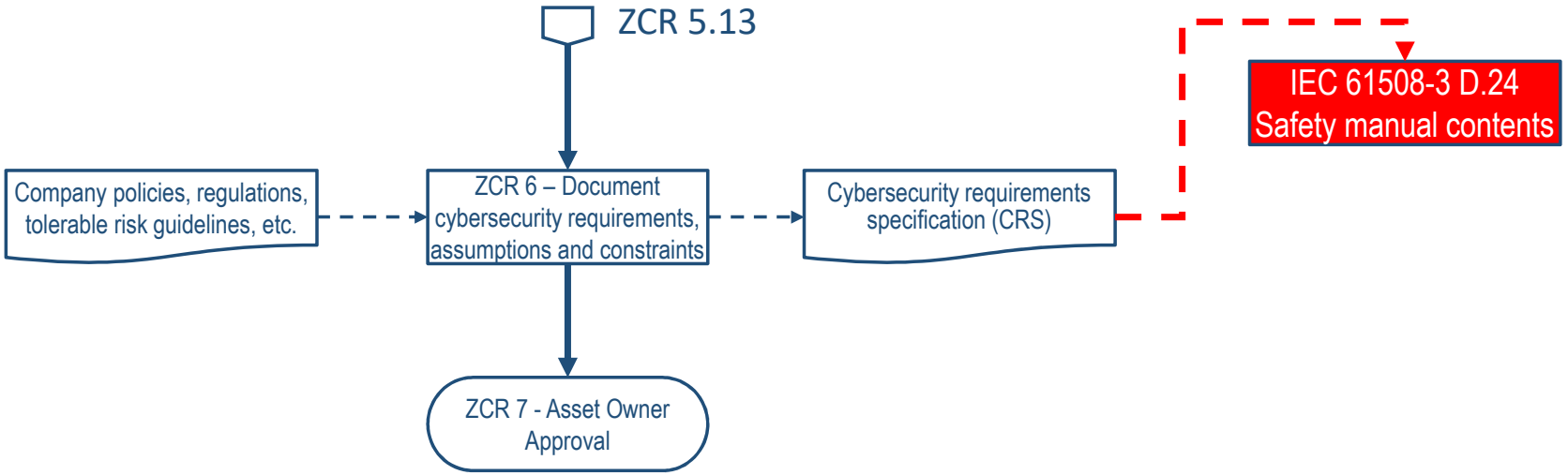
IEC 62443-3-2 Risk Assessment 2



IEC 62443-3-2 Risk assessment 3



IEC 62443-3-2 Risk assessment 4



IEC 62443-3-3 foundational requirements

Foundational requirement	Clause	Purpose and description
FR 1 – Identification and authentication control (IAC)	5	Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.
FR 2 – Use control (UC)	6	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the IACS and monitor the use of these privileges
FR 3 – System integrity (SI)	7	Ensure the integrity of the IACS to prevent unauthorized manipulation
FR 4 – Data confidentiality (DC)	8	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure
FR 5 – Restricted data flow (RDF)	9	Segment the control system via zones and conduits to limit the unnecessary flow of data
FR 6 – Timely response to events (TRE)	10	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered
FR 7 – Resource availability (RA)	11	Ensure the availability of the control system against the degradation or denial of essential services

IEC 62443-4-1 development practices

Foundational requirement	Clause	Purpose
Practice 1 – Security management	5	ensure that the security-related activities are adequately planned, documented and executed throughout the product's life-cycle
Practice 2 – Specification of security requirements)	6	document the security capabilities that are required for a product along with the expected product security context
Practice 3 – Secure by design	7	ensure that the product is secure by design including defence in depth
Practice 4 – Secure implementation	8	ensure that the product features are implemented securely
Practice 5 – Security verification and validation testing	9	ensure that all of the security requirements have been met for the product and maintained.
Practice 6 – Security defect management	10	handling security-related issues of a product that has been configured to employ its defence in depth strategy
Practice 7 – Security update management	11	ensure security updates associated with the product are tested for regressions and made available to product users in a timely manner
Practice 8 – Security guidelines	12	provide documentation that describes how to integrate, configure, and maintain the defence in depth strategy of the product