# ‘til the Next Zero-Day Comes

**Ransomware, Countermeasures, and the Risks They Pose to Safety**

**Bruce Hunter**

Safety and Security Consultant, Sydney, Australia

## Abstract

*Cyber-attacks on critical infrastructure are not new, but their recent intensity has increased the risk of intended or unintended consequences to safety systems to become a real and present danger. Ransom use of malware attacks have mainly concentrated on business systems, by denying access to essential data, but recent attacks have affected critical infrastructure with consequential shutdown of operation-al technology including safety-related functions. Although ransomware may intentionally cause dangerous failures in the system, pervasive connectivity raises the risks of this happening. This article discusses the precursors to this danger as part of Information Technology and Operational Technology convergence, integration of business and control systems, conflicts arising out of this integration and monetarisation of vulnerability exploitation. Although using Industrial Control System examples are used, safety practitioners may use these to mitigate cybersecurity threats and minimise the impact of attacks on all safety-related systems and their recovery.*

## 1 Out of Gas!

Usually, cyber-attacks on critical infrastructure that includes safety-related systems go relatively unnoticed, unless they have a significant impact on the public. Partly this is due to the sensitivity of companies to bad press and cautiousness in trying to prevent copy-cat attacks. An understanding of the magnitude and nature of attacks, however, can be gained from published, but anonymized, surveys of the industries concerned.

Ransomware attacks in general have become a major threat. Industry surveys have also shown that ransomware is the cyber-threat most likely to affect their organization in the next 12 months (ISACA 2021):

- 21% of businesses in general said that their organizations have experienced ransomware attacks
- 67% said that their organizations will take new precautions in light of the attack on Colonial Pipeline, an American oil distribution system from Houston, Texas
- 78% said critical infrastructure organizations should *not* pay ransom if attacked
- 84% said ransomware attacks would become more prevalent in the second half of 2021

A 2020 survey (Bakuei et al. 2021) shows, for the US alone, that 19 organisations found ransomware in their Industrial Control Systems (ICS).

© Bruce Hunter 2022.

Ransomware risk to Operational Technology (OT) including ICS differs from other forms of attack in the following ways:

- The primary objective of ransomware is monetary gain by locking up assets and information needed by the target organisation
- Impact on critical functions including safety is generally unintended and consequential when resources needed by these functions become unavailable
- Ransomware is only designed to interrupt and may contain untested side effects, which can have reliability and safety implications. In the Colonial Pipeline case, the de-encryption tool did not work properly, and recovery required other methods.

The ransomware attack on the US Colonial Pipeline company in 2021 certainly did get noticed and led to the shutdown of the gas distribution operation for a week affecting the supply of over 40% of the US East Coast supply of automotive and aviation fuel. Like most complex failures, this resulted from a series of events and decisions that made the company's systems more vulnerable, and the response to the attack less optimal.


**Figure 1 ~ "Colonial Pipeline", Photograph by Orbital Joe**

The key events of this attack were (Charles Carmakal, 2021):

- Hackers gained entry into the networks of Colonial Pipeline on April 29 through a forgotten virtual private network (VPN) account that had poor security (Attributed a cybercrime group using to DarkSide Ransomware-as-a-service (RAAS) toolkit)
- Just before 5am on May 7, Colonial's control room saw a ransom note on their system
- DarkSide ransomware attack locked out the business operation
- As a safety precaution, Colonial shut down its entire pipeline operation, causing critical fuel shortage to Eastern US
- After extensive checks of the OT network concluded that damage was limited to some of the Information Technology (IT) business operation, supply restarted on May 13
- Colonial did pay USD 4.4M in Bitcoin ransom, as a precaution in case recovery was not achievable, although the Federal Bureau of Investigation (FBI) was subsequently able to recover most of this ransom

The following precursors the industry faced in the last few years may have strongly influenced the reaction to this event:

- The US Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA), and the FBI, advised Pipeline Operators of a spear-phishing and intrusion campaign conducted by state-sponsored Chinese actors that occurred from

December 2011 to 2013, targeting U.S. oil and natural gas pipeline companies (CISA and FBI 2021a).

- A US Congressional report highlights pipeline cybersecurity issues, but US Transportation Security Administration (TSA) "*maintains that voluntary cybersecurity standards have been effective in protecting US pipelines from cyber-attacks*" (Parfomak, 2012)
- The United States Government Accountability Office conducted a review of "*TSA's efforts to assess and enhance pipeline security and cybersecurity*" and issued 10 improvement recommendations in its congressional report, GAO-19-48, but did not highlight industry cybersecurity regulation (GAO 2018).
- In 2019 alone, there were 614 reported pipeline incidents in the United States, resulting in the death of 10 people, injuries to another 35, and about $259 million in damages (Kelso, 2020).
- Despite warnings of pipeline specific ransomware threats (CISA 2020), the industry has been criticised for poor cybersecurity practices and lobbying against stronger regulation
- Industrial Control Systems (ICS) have become an attractive target to Ransomware attackers. The motives are strong (money), the risk is low (RAAS toolkits protect attacker), the target is soft (old ICS hidden vulnerabilities abound), and reward is fairly certain (ICS operations are critical). (Palmer, 2021)
- The Colonial Pipeline company supplies about 45% of east US coast fuel, making it a major risk to US transport operations
- Poor security practices would have meant uncertainty on the reliability of OT network segmentation.

These precursors could have influenced the company's response to the ransomware attack and its outcome, which did result in the shutting down the fuel supply.

Colonial's east coast pipeline is a multi-product, multi-offtake, multi-line, multi-section, and multi-storage operation that has high risks associated with operations outside the safe envelope. Out of an abundance of caution to ensure a dangerous situation did not arise, the company chose to shut down operations to prevent spread to the OT network until the business system was cleared of ransomware and put back into operation (Hoffman and Winston 2021).

The system failure resulted in the following timeline of events with the US fuel supply:

- Crisis caused by the loss of supply resulted in the Federal Motor Carrier Safety Administration (FMCSA) declaring a state of emergency in 18 states to help with the shortages (9 May 2021)
- Colonial Pipeline eventually re-established pipeline operation (13 May)
- FBI and CISA issue alerts on pipeline ransomware threat (11 and 19 May)
- TSA update to Pipeline Security Guidelines issued, replacing criticality guidelines - naturally (TSA 2021a)
- TSA issued Security Directive Pipeline-2021-01 (TSA 2021b) directing a whole range of mandatory report and assessments with significant penalties for non-compliance (27 May)
- United States Department of Justice (DOJ) gives critical infrastructure ransomware attacks equivalent priority to terrorism. (3 June)
- CISA, with the FBI, updated a joint advisory on DarkSide Ransomware: "Best Practices for Preventing Business Disruption from Ransomware Attacks" (CISA and FBI 2021b), originally published 11 May, to supplement previous advice (8July).

- On 28 July, the US president announced further steps to safeguard critical infrastructure (Biden 2021)

Consequences of the Colonial Pipeline attack have certainly focused the minds of the process sector (Moore 2021); but why the concern? Ransomware is a substantial risk to control systems due to:

- Difficulty to recover operations as systems locked by encrypted files
- High motivation of attackers due to monetary rewards or nation-state intent
- Possibility of accidental damage to safety systems as a by-product, due to unaccountability of cybercriminals compared to nation-state threat actors

Ransomware Lessons Learned for safety from this ransomware attack includes:

- Safety and security must be coordinated. This could have affected safety elements of the pipeline if essential operator controls, e.g. human-machine interfaces (HMIs), were affected (CISA 2020), or if the security response to ransomware had impact on safety.
- OT operational aspects may have continued if, independent of the business systems.
- Segregation between OT and IT is necessary but not always assured.

# 2 Who's in control? OT Cybersecurity

## 2.1 An Analogy

As I write this article in mid-2021, Sydney is in the middle of another lockdown, trying to control a COVID-19 Delta-strain outbreak despite months when there were effectively no cases in the country. Pandemics and the way we deal with them are very reminiscent of cybersecurity. The following issues are very much characteristic of pandemic and cybersecurity experiences:

- Failure consequences can be far-reaching and include morbidity
- Responses and their success are driven by
    - risk appetite of participants
    - motivation of the threat
- Protection involves:
    - separation of the vulnerable from the threat
    - continually increasing the resilience of the target
    - educating the user on responsibility and actions that may increase risk
- but Thwarted by:
    - constant evolution of the threat tactics and vulnerable entry points
    - detection reliant on known indications and subject to false positives and negatives
    - lack of persistence in assessing and addressing the risks
    - the risk that defence may actually harm the defended
    - unpopularity of preventive measures
    - cognitive bias and complacency about risk

## 2.2 Convergence of Technology

Control systems have evolved from mechanical, electrical, electronic, and programmable electronic systems but usually remained standalone. OT has converged with hardware and software of IT with the benefits of economies of scale, supportability of common operating systems and skillsets. A less welcome consequence of this was the inheritance of visibility and vulnerability to cyber-attack (ISACA 2016).

Adopting IT platforms and Operating Systems specifically provides:

- Economies of scale;
  - but increased vulnerabilities with complex designs, update frequency and obsolescence issues
- Commonality of software and hardware providing a wealth of functionality;
  - but inheritance of IT vulnerabilities and attack toolkits
  - and visibility to IT threat agents
- Increased connectivity to allow expanded operation and monitoring;
  - but expanded attack vectors or surfaces
- Increased functionality and capability;
  - but reduced reliability and predictability

These issues have made OT systems not only more vulnerable to cyber-attack, but also have impacted reliability and safety.

## 2.3 ICS Threats

Cyber-threats to systems incorporating Operational Technology (OT) have grown to a point where, in 2020, ICS Advisories were issued by US CISA at an average rate of 5 per week (https://www.cisa.gov/uscert/ics/advisories). Analysis shows that, advisories and alerts have grown to an average of 7 per week in 2021: 55% more than 2020 (Figure 2).

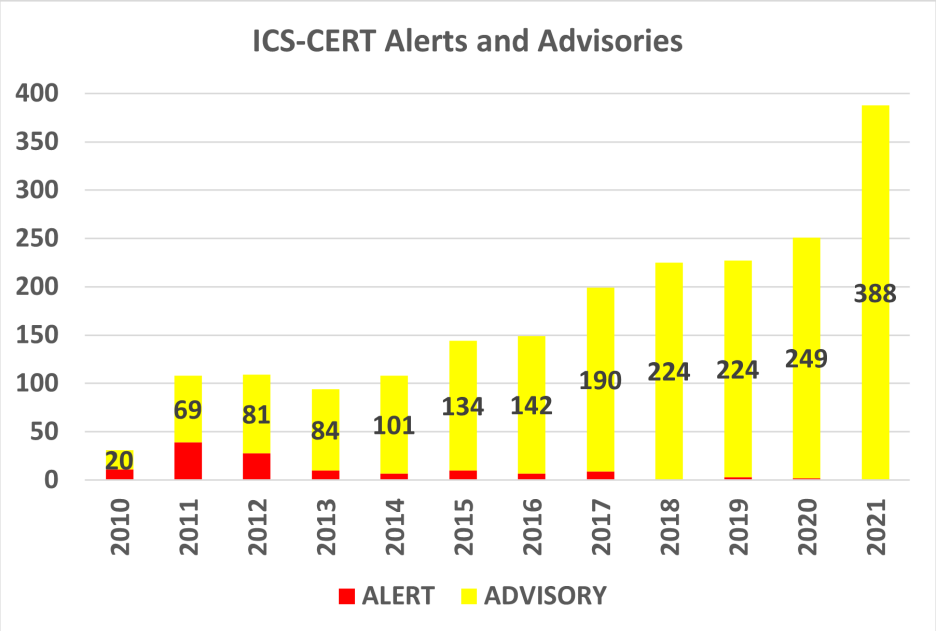


**Figure 2 ~ Analysis of CISA ICS Advisories Over Time**

Threat actors to ICS have evolved from script buddies and hacktivists to now include state-sponsored specialists and cybercrime using ransomware-as-a-service (RAAS) toolkits.

Significant past attacks noted by CISA of non-ransomware cases with ICS include:

- Joint CISA-FBI Cybersecurity Advisory (AA21-201A) (CISA and FBI 2021a): Gas Pipeline Intrusion Campaign. Attributed to China nation-state cyber actors. Of the targeted entities, 13 were confirmed compromises, 3 were near misses, and 7 had an unknown depth of intrusion. Impact is development by the attacker of capabilities against U.S. pipelines to physically damage pipelines or disrupt pipeline operations
- W32.DistTrack, also known as "Shamoon" (CISA 2021a): An information-stealing malware that also includes a destructive module. Attributed to Iranian nation-state cyber actors. Operational impacts of this attack include loss of intellectual property (IP) and disruption of critical systems.
- ICS Focused Malware Havex Trojan (CISA 2018): An information-stealing malware. Attributed to Russian nation-state cyber actors. Operational impacts may result from information gathered in this attack or malware installed.
- Malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware (CISA 2021b): Installs malware on Internet-connected HMIs. Attributed to Russian nation-state cyber actors. Impact is other actions enabled by compromised HMI.
- Cyber-Attack against Ukrainian Critical Infrastructure including electricity grid (CISA 2021c): Attributed to Russian nation-state cyber actors. Impact was the takeover of electricity grid HMI operation, shutdown communication and backup recovery with loss of large section of the grid.
- CrashOverride Malware (CISA 2021d): Attributed to Russian nation-state cyber actors. Impact is the abuse of functionality in a targeted ICS system's legitimate control system to achieve its intended effect which has included shutdown of electricity grid using standard ICS protocols but could impact all critical infrastructure organizations.
- Safety System Targeted Malware HatMan, also known as TRITON and TRISIS (CISA 2019): Attributed to Russian Government-Owned Laboratory but possibly used by Iranian nation-state cyber-actors. Disrupted the safety-related triple redundant Emergency Shutdown (ESD) of Saudi Arabian petrochemical plant. Safety protection key switch (SIS configuration mode) on one channel was left in the program state allowing the modification of the Triconex system; the other two channels detected anomaly of exploited channel and shutdown.

## 2.4 Vulnerabilities and Attack Paths

The vulnerability-patch cycle with converged IT-OT, leads threat agents to go to deeper technology layers to achieve exploitation, as examples show in Figure 3.

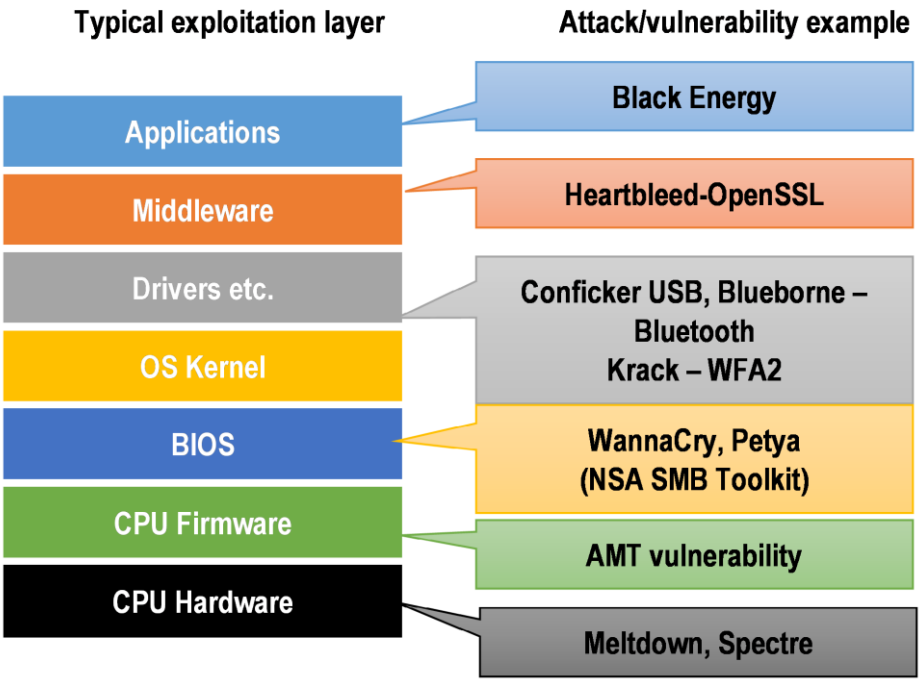


**Figure 3 ~ Increasing Depth of Exploitation in Technology Layers**

Attack paths and surfaces used by adversaries rely on accessibility to ICS OT networks. Understanding the risk of entry and protective measures is helped by a layered architecture as the example in Figure 4 modified from IEC 62443 (IEC n.d.), which is loosely based on Purdue (Purdue 1989).

This layered approach does provide a Defence-in-depth approach but exhibits some key vulnerable attack vectors as experience in ICS attacks:

- Entry via vulnerabilities in the web and email services of the Enterprise layer (Purdue Layer 4). Despite the use of Demilitarised Zone (DMZ) technology there are still backdoors to attacks via techniques such as email spear phishing
- Entry via Operations Control (Purdue Layer 3); DMZ again subject to backdoor entry
- Entry via Supervisory Control (Purdue Layer 2) and Controllers (Purdue Layer 1) via backdoors and malware on HMI and engineering workstation. Safety-related systems at this level have to be protected against dangerous attacks. Entry points at this level include IT technology of HMI and Engineering Workstations, again typically by malware carried on spear-phishing e-mail or remote maintenance network connection. Even if this is precluded by "air-gaps", backdoors can be gained via portable media (e.g. USB Drives) used to update system software or firmware.
- Manipulation of standard protocols in Field Device connections (Purdue Layer 1 and 0).

Network segmentation (restricting data flow) is a key technique in not only providing defence-in-depth against attack but also providing functional separation or independence for different critical elements of an ICS. Network segmentation does not necessarily mean functional separation.

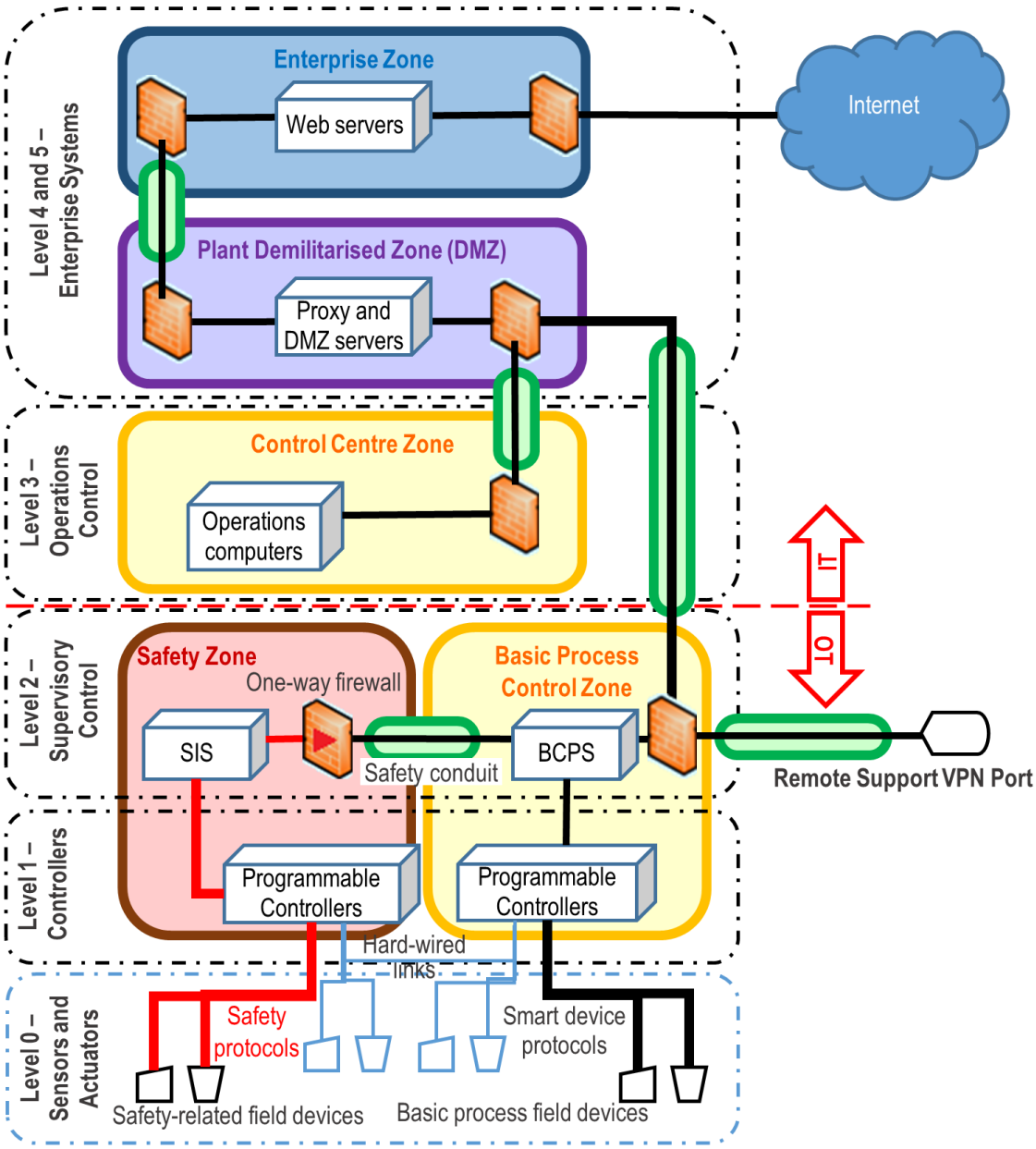


**Figure 4~ Simplified Layered ICS Security Architecture (IEC 62443)**

Evolution of OT architecture to Industrial Internet of Things (IIoT), Cloud Services and Nested Edge Technology is providing emerging challenges to true defence-in-depth, segmentation, and cybersecurity protection of safety-related systems. Protective segmentation becomes difficult in Software Defined Perimeters due to logical architecture as shown in Figure 5, which is extracted from Annex C of draft IIoT standard ISO/IEC FDIS 30162. Proof of dependable functional separation and interaction is difficult to prove in software-defined networks with non-industrial protocols. Standards are catching up on the model and requirements for IIoT, but issues remain in proving trustworthy segmentation of functional layers. IEC/ISO JTC1/SC41 has highlighted these issues for future Standardization work in a technical report (ISO/IEC 2020).

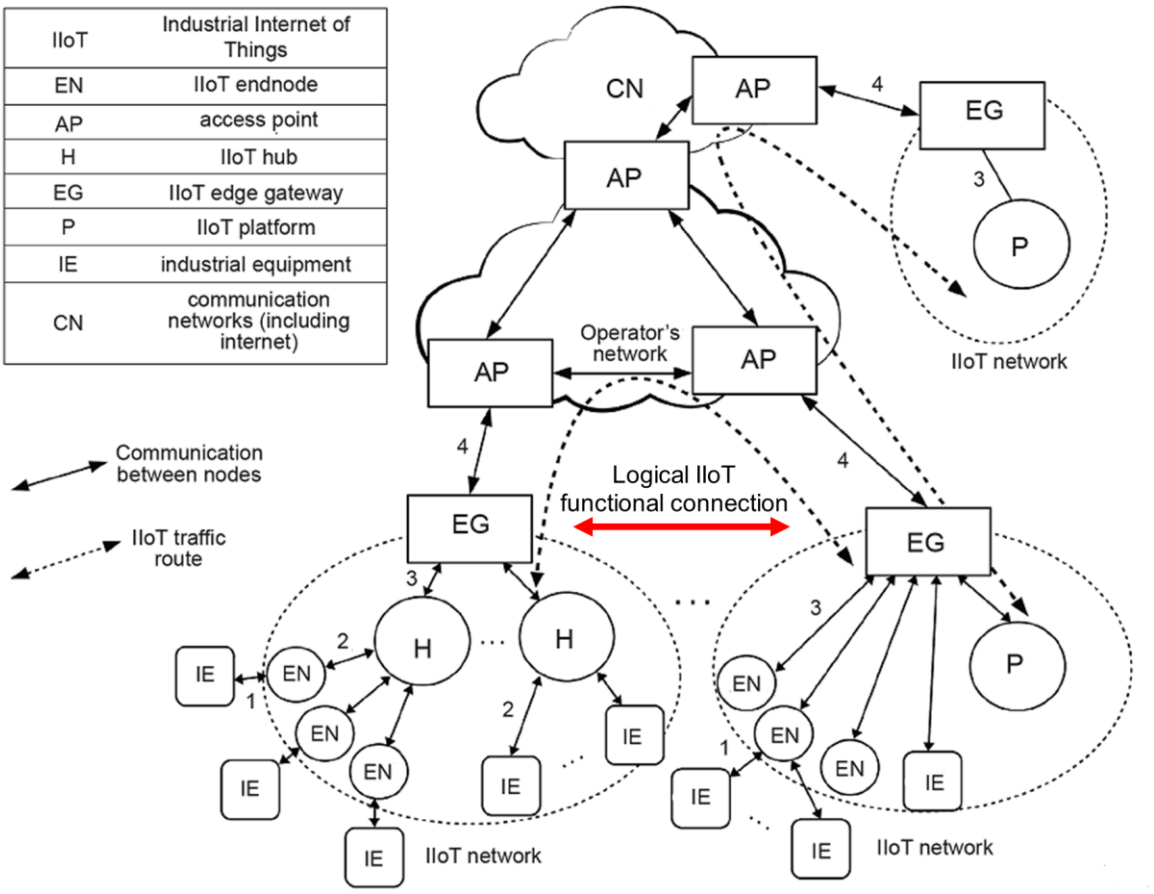


**Figure 5 ~ Logical Segmentation of Network in IIoT-Cloud Architecture**

## 2.5 Standards, Directives and Frameworks

### *2.5.1 General*

Evolving threats to and vulnerabilities of ICS have led to a variety of standards, guides, and framework to protect these systems. There is growing guidance on securing OT in ICS (Timpson and Moradian 2018) and standards to support these.

### *2.5.2 Ransomware Specific Frameworks*

The following specific frameworks have been established to minimise the specific risk of ransomware to ICS including pipeline systems:

- CISA FBI joint advisory on DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks (AA21-131A) (CISA and FBI 2021b)
- US TSA updated Pipeline Security Guidelines (TSA 2021a)
- NIST Framework with security lifecycle guidance on the application of the NIST CSF to ransomware mitigation (NIST 2021).

### *2.5.3 The ISO/IEC - Standard Security for Industrial Automation and Control Systems*

IEC 62443 (IEC n.d) is the "go-to" standard for OT specific cybersecurity, rather than the ISO/IEC 27000 series commonly used for IT, providing requirements to protect against various levels of cyber-attack. It also supports specific protection of safety-related aspects. The published parts include requirements for developers, asset owners, operators and assessors covering the following fundamentals, as follows:

- Security Governance (SG) – having 42 requirements
- Security Development and Integration (SDI) – having 45 requirements
- Risk Management (RM) – having 74 requirements
- Asset Management (AM) – having 128 requirements
- Identification and Authentication Control (IAC) – having 75 requirements
- Use Control (UC) – having 84 requirements
- System Integrity (SI) (includes integrity of safety functions) – having 84 requirements
- Information Confidentiality (IC) – having 47 requirements
- Restricted Data Flow (RDF) – having 30 requirements
- Incident Management (IM) – having 68 requirements
- Resource Availability (RA) – having 29 requirements

### *2.5.4 NIST Cybersecurity Framework (CSF)*

The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST 2018a), as illustrated in Figure 6, provides a model for assessing maturity of cybersecurity processes.

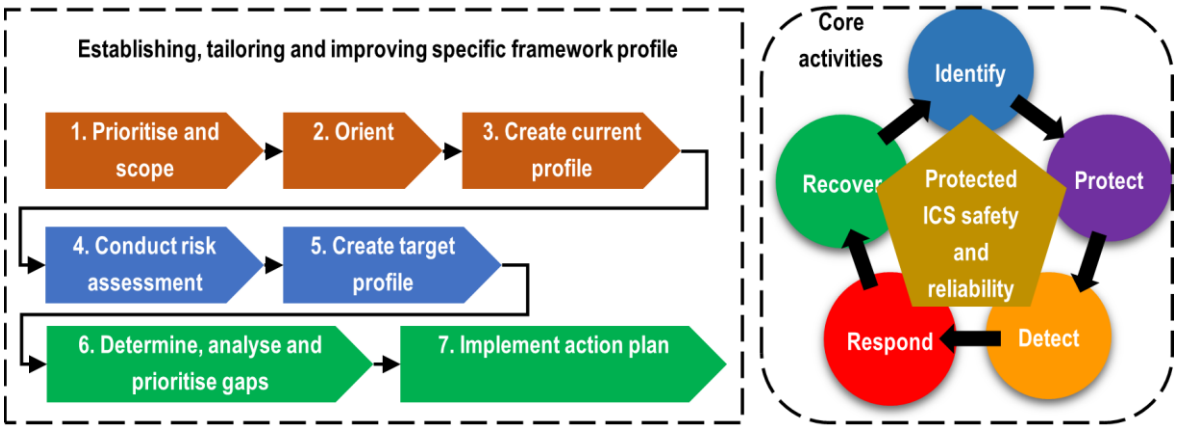


**Figure 6 ~ NIST Cybersecurity Framework Model**

Safety interaction with the NIST CSF as part of the kill chain is illustrated in Figure 10 of Sub-section 3.3.

Appendix A, Section A.2, proposes a tailoring of the framework core for safety-related systems. CSF profiles have been published for various critical infrastructure sectors.

## 2.6 Maintaining Effectiveness of ICS Cybersecurity Protection

### *2.6.1 Patching and Updates*

The effectiveness of ICS cybersecurity countermeasures is only as good as the vulnerabilities and threats address at the time of the last update ('til the next zero-day).

Effective cybersecurity protection relies on prompt patches of system vulnerabilities. This has the following challenges with OT systems:

- Reliability of the control system can be degraded by unproven updates. Reliability growth in OT is built up over time and by correction of systematic errors. Patches may cause regression in this growth.
- Security patches may cause unexpected failure due countermeasures or malware detection patterns (Goodin 2010).

Patches and updates to OT systems require validation before they are put on live ICS (Hunter 2013). Figure 7 illustrates the cycle of new vulnerabilities, patching validation and system changes.

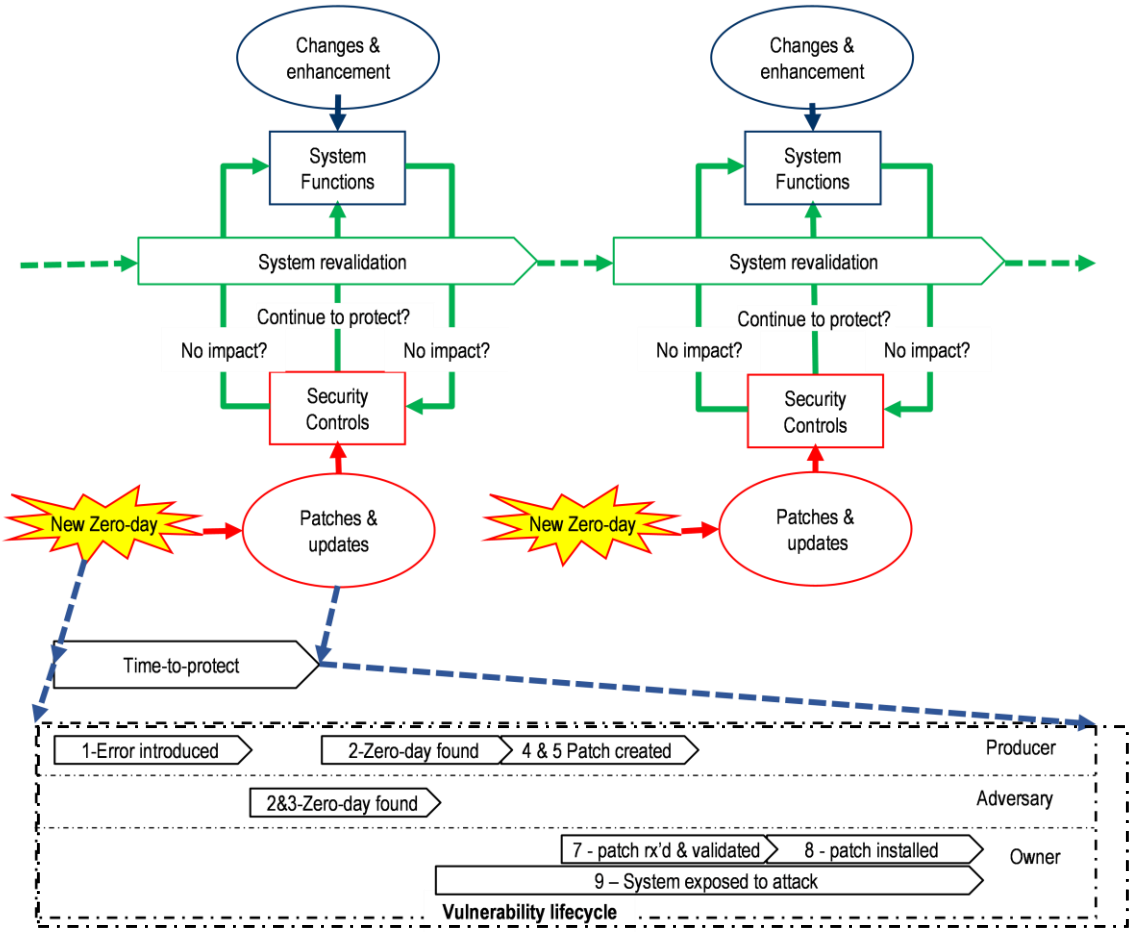


**Figure 7 ~ ICS Vulnerability, Update and Validation Cycle**

Vulnerability cycle includes:

1. point when software error results in vulnerability
2. point of discovery of new zero-day vulnerability

3. average time to exploitation in the field
4. time to develop a patch to address the vulnerability
5. time to communicate and act on vulnerability
6. time to stage patch and develop precautionary roll-back baseline
7. time to validate on test environment the reliability of the patch in the ICS and compatibility with Safety Functions
8. time to release into the production environment

The aim is to keep exposure time of the system, shown as 9 in Figure 7, as low as possible (hopefully before exploitation is initiated).

Patch Management in the Automation and Control System (IACS) environment; IEC 62443 (Parts 2-3) does specify methods and formats for patches in the development, notification, verification, and validation of security updates for OT systems (IEC n,d,).

### *2.6.2 CISA ICS Advisories and Alerts*

Awareness of emerging OT product vulnerabilities, and timely patching of these, is a key aspect of cybersecurity risk reduction. This requires a balance approach to ensure that system reliability is not compromised. US CISA provides timely advisories for ICS product vulnerabilities. Monitoring of these (https://www.cisa.gov/uscert/ics/advisories) and acting on advice should be a basis of maintain cybersecurity protection of ICS.

### *2.6.3 Physical Architecture and Network Segmentation*

Defence-in-depth, as provided by the long-accepted Purdue Enterprise Reference Architecture (Purdue 1989), is an example of a security architecture in critical industrial control system protected in “zones” and “conduits” (IEC n.d.). An example of this architecture is shown back in Figure 4 of Sub-section 2.4.

Network Segmentation has challenges in achieving separation of functions, let alone independence of these:

- We still need to communicate between IT and OT functions
  - OT functions need access to functionality in IT systems
  - IT systems need to monitor and control OT
- Network segmentation and functional separation can be bypassed by use of portable media (e.g. USB) or external maintenance links
- Firewalls separating network zones can be compromised with concerted efforts; if monitoring is only required across the gap the use of one-way firewalls or data-diodes may help in enforcing isolation.
- Security products are available that scan air-gapped systems without installing software, but these need to be set to not automatically delete files which could be critical to OT.

System Safety Standards, (IEC 2010), require that the boundary of the safety-related system be established and maintained. OT Cyber Security Standards (IEC n.d.) fulfil this by segmentation of safety related function into their own protected zones based on risk assessment, e.g. IEC 62443 Part 3.2.

Separation of functions across these safety boundaries must be maintained throughout the system lifecycle to prevent interference with process critical and safety-related functions (Hunter 2006).

### 2.7 Connectivity

Convergence of connectivity such as TCP/IP has increased the attack surface and vulnerabilities; however there have been previous attacks on systems with traditional OT architecture with safety and environmental impact, e.g. that on the Maroochy Shire Sewerage System (Smith 2001).

So, we know ICS systems cybersecurity's needs and practices; but what about protecting the safety-related elements?

## 3 Safe and Secure?

### 3.1 System Hierarchy

Safety Functions are rarely standalone, and are usually part of a larger system. In IACS, and their aligned systems, Safety Functions are considered, in the system hierarchy, as part of the control system essential functions as shown in Figure 8.

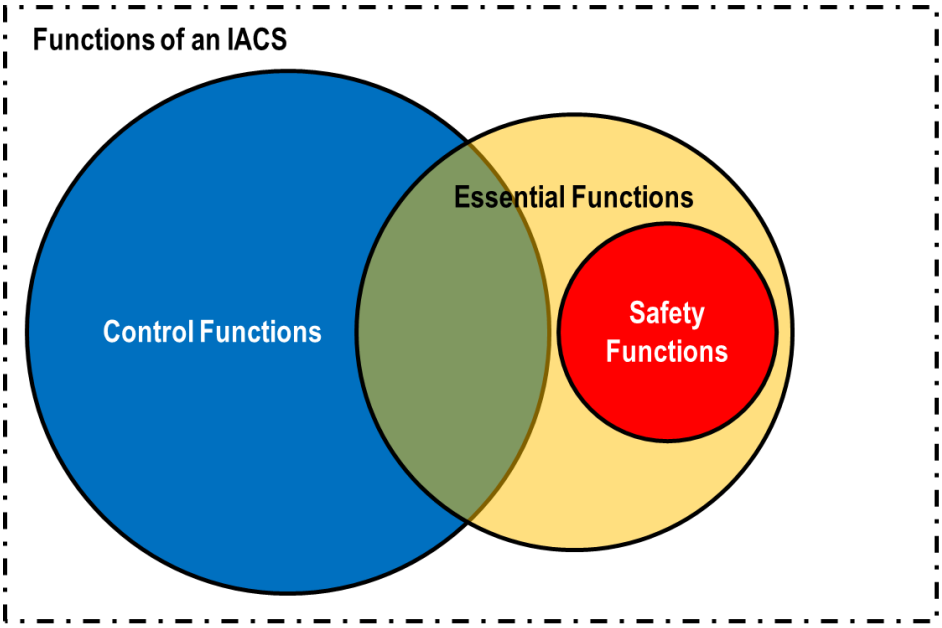


**Figure 8 ~ Hierarchy of IACS Functions (IEC 62443)**

This hierarchy helps to prioritise system dependability and protection from sources of unintended operation.

The following concepts, techniques and standards support ICS safety and security.

### 3.2 Boundaries are important after all!

As previously noted, safety standards usually call for the definition of the boundary of the safety-related elements and maintenance of and effective separation across this boundary (Hunter 2006). Setting security and safety boundaries has an impact on independence and interdependence of critical functions.

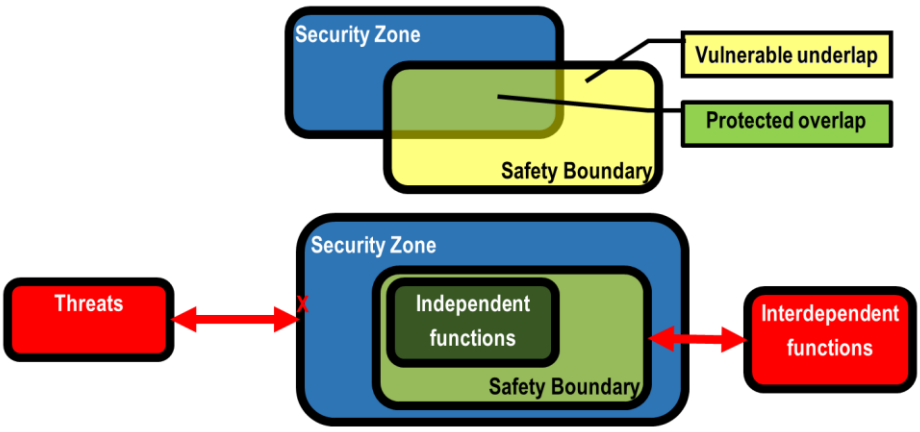


**Figure 9 ~ Safety/Security Boundary Considerations**

The placement of security perimeters and safety boundaries has a significant impact on the protection and reliability of safety functions:

- Overlap allows security countermeasures to work effectively and reduces the risk of incompatibility with safety functions;
- Underlap increases the risk of back-door attack vectors being exploited; and
- Reliability of safety functions may be affected by cybersecurity countermeasures inadvertently blocking interdependent functions outside the security perimeter.

## 3.3 Control Systems Kill Chain

Safety practitioners must face the reality that even with the best cybersecurity endeavours the possibility that Advanced Persistent Threat, "APT" will someday succeed in compromising their system. What is left is then reliance on effective safety and security response to this attack. To understand the best response to an attack, you need to know how attacks are staged.

The methods of cyber-attack have become advanced in application, and understanding the kill chain has helped to adapt mitigation to limit not only the likelihood of vulnerability exploitation but also its impact (Assante and Lee 2015). Figure 10 shows the relationship between the NIST Cybersecurity Framework (CSF) (NIST 2018a), Lockheed Martin's generic kill chain, and Safety System incident response/resiliency actions (IEC 2019a), (ISA 2017).

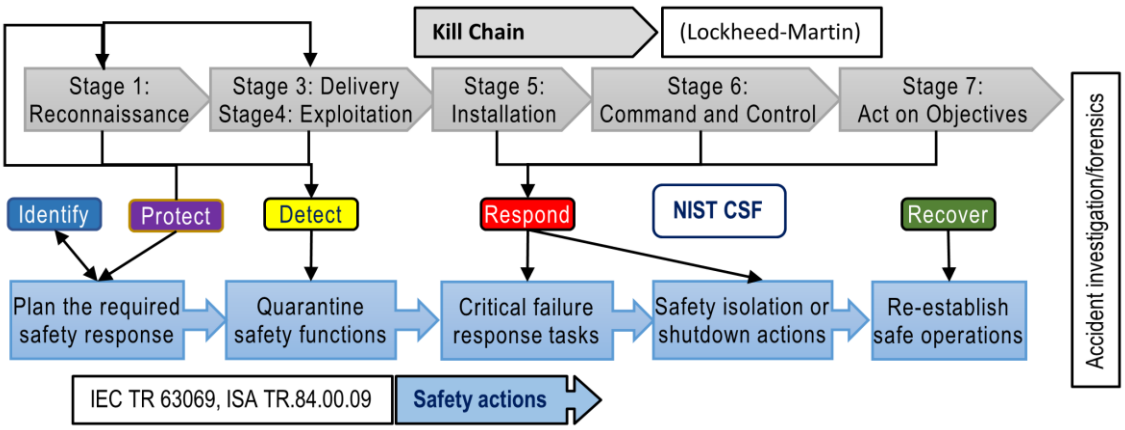


**Figure 10 ~ Interaction of Cybersecurity Kill Chain with NIST CSF and Safety**

Due to evolving nature of APT and despite best effects in cybersecurity, there is always a residual risk that safety-related components of a system will be compromised by a cyber-attack. Safety functions need to be resilient to this probability and ensure these do not lead to dangerous failures. Safety responses to a recognised attack include:

1. Plan the required safety response
2. Quarantine safety functions
3. Critical failure response tasks
4. Isolation or shutdown actions
5. Re-establish safe operations

Appendix A, Section A.1, provides a generic Framework Profile to address Ransomware risk of Safety Systems in OT.

### 3.4 Safety and Security Co-engineering Activities

Establishing safe and secure systems requires co-engineering to be undertaken across the system lifecycle (Paul et al. 2016).

IEC has published a Technical Report (IEC 2019a) to assist in protecting safety-related systems from dangerous cyber-attacks in applying safety (IEC 2010) and security (IEC n.d.) standards. It promotes the following guiding principles:

1. protection of safety implementations – to paraphrase, if it isn't secure, it isn't safe
2. protection of security implementations – to paraphrase, safety shouldn't increase security risk
3. compatibility of implementations – to paraphrase, security countermeasures shouldn't be unsafe

A fourth principle is being considered for a new edition with normative clauses:

- Guiding Principle 4: compatibility related to the higher-level system objectives
  - This could satisfy operational objectives, such as availability; and
  - Preclude down-time due to inadvertent shutdowns and fail-safe actions triggered by cyber-attacks.

Currently IEC 61508 is in development to be Edition 3. This includes more detail on handling cybersecurity risk to functional safety. This adds to clauses concerning Hazard and Risk Analysis in Edition 2 (IEC 2010).

ISA also has published a guide (ISA 2017) for the process sector to "address and provide guidance on the safety lifecycle and the cybersecurity lifecycle as they relate to the security of Safety Controls". It covers safety and security activities across the lifecycle from assessment, design, installation, operation, maintenance, modification, and decommissioning.

### 3.5 Unintended Countermeasure Consequences

Not all threats are external or adversarial. It is possible for inappropriate security countermeasures to impair the very functions they are protecting. This control conflict conundrum, as illustrated in Figure 11, has its counterparts in physical security such as fail-safe and fail-secure conflict of emergency exit doors (Hunter 2009) or physical security of aircraft cockpits (BEA 2016).

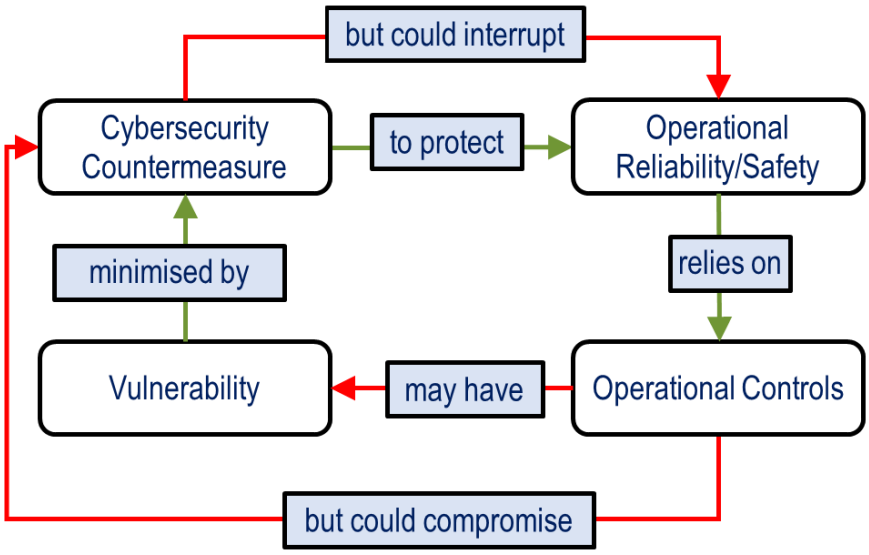


**Figure 11 ~ Control Conflict Conundrum**

The following safety and security standards do highlight this issue:

- NIST Cybersecurity Publications (NIST 2015), (NIST 2018b) classes these as "accidental or non-adversarial threats"
- Safety of Machinery IEC TR 63074 (IEC 2019b)
  - "*…shall not adversely affect safety integrity (e.g. increase in response time, etc.)*"
  - "*Any security countermeasure shall not adversely affect safety integrity (e.g. increase in response time, etc.)*"
- IEC TR 63069 (IEC 2019a) has a guiding principle: "*compatibility of implementations - Security implementations and safety implementations should not have adverse contradictions*"
- The ISA technical report on Cybersecurity Related to the Functional Safety Lifecycle (ISA 2017) classes these as "*security compromises* [which may] *occur during normal maintenance or other field activities where the cybersecurity compromise is unintentional or accidental*"

Appendix A, Section A.1, proposes common conflicts between cybersecurity and safety.

# 4 Mind the gap! - Maintaining Safety Independence

## 4.1 Risks to Functional Separation

Much reliance is placed on air-gaps, but even with no network connection between safety and non-safety related systems these can be bypassed. Loss of functional separation is almost entropic. The risk to this separation includes:

- Bypasses by human action including use of removable media, e.g. USB, that allow malware to infiltrate across the gap by breaking network segmentation and functional separation controls
- Unapproved or forgotten network connections including remote maintenance ports

- Untested changes to network configuration including:
  - message filtering;
  - port assignments;
  - access rules; and
  - authentication.

### 4.2 Establishing Effective Functional Safety Separation

Effective separation of safety systems is not as easy as it sounds. Strictly, the integrity of the separation mechanisms should have the same integrity as the safety system itself (Hunter 2006). This would mean:

- Network segmentation would require firewalls with a "SIL", i.e. Safety Integrity Level (IEC 2010)
- Human introduced bypasses, such as USB drives across air-gaps, would entail Human Reliability Analysis
- Hard-wired links across safety boundary may provide a level of isolation but require substantiation of meeting requirements for independence of safety, e.g. IEC 61508 Part 3, 7.4.2.9 (IEC 2010).

Pragmatically, separation will not be perfect or lasting; the fall-back position is to safely handle cybersecurity intrusions by a safety-driven incident response.

From a safety perspective, there are key points in the lifecycle to establish and maintain separation from non-safety parts of the system, as proposed in Table 1.

**Table 1 ~ Lifecycle Consideration of Safety Boundaries and Functional Separation**

| IEC 61508 Safety Lifecycle | Functional Safety Separation Activities | Related Cybersecurity Activities |
|---|---|---|
| Phase 4. Overall Safety Requirements | Determine safety boundaries | Determine security perimeters and zones |
| Phase 5. Overall Safety Requirement Allocation | Determine separation requirements | Cybersecurity architecture segmentation requirements |
| Phase 9. System Safety Requirements Specification | Specify trans-boundary information allowed and prohibited | Establish network firewall rules and air-gap needs |
| Phase 10. Safety-related Systems Realisation | Establishment of separation measures | Verify security requirements support safety requirements. |
| Phase 13. Overall Safety Validation | Proof of separation of non-safety systems or influences | Validate effectiveness of security architecture and separation of safety zones. |
| Phase 14. Overall Operation, Maintenance and Repair | Monitoring for compromised separation | Conduct safe ongoing dependency, visibility, and penetration testing |

| IEC 61508 Safety Lifecycle | Functional Safety Separation Activities | Related Cybersecurity Activities |
|---|---|---|
| Phase 15. Overall Modification and Retrofit | Re-evaluating safety boundaries and separation | Validate system modifications have not reduced the effectiveness of security architecture and separation of safety zones. Prevent unauthenticated SIS configuration changes. |

# 5 Summing up

Safety related systems are a growing target of cyber-attacks, including ransomware. Designers, installers, operators, and maintainers of these system should:

- Understand that safety functions in control systems are subject to increasing cyber threats;
- Ensure safety-related systems are effectively protected by well-maintained cybersecurity measures that are compatible with the system's safety functions;
- Safety and security must be coordinated and cooperative:
  - Safety practitioners, try talking with your cybersecurity counterparts
  - Cybersecurity practitioners, try talking with your system safety counterparts
  - You will be amazed how useful these conversations are…
- Segregation between OT and IT is not assured. Air-gapping is not certain (see RSA 2FA lesson (Greenberg 2021)). Functional separation must be proven and actively maintained for ongoing integrity of safety;
- The challenges of Software Defined Perimeters, such as used in IIoT and Factory 4.0, may increase cyber-attack surface for OT and safety-related systems. They may also decrease true reliability and provable safety integrity.

### Disclaimers

Opinions expressed in this paper are based purely on the public references listed. They do not infer culpability or carelessness on any party.

### Acknowledgments

The author acknowledges the dedication of safety and security professionals who protect us from dangerous outcome of failures in technology in our lives. The author appreciates the help of Gurinder Pal Singh, Ian H. Gibson, and anonymous peer-reviewers, who have offered advice on this article.

Figure 1 is a photograph taken in 2005 by Orbital Joe, from his album, "Around Baltimore and the State": https://www.flickr.com/photos/orbitaljoe/albums/154745. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 2.0 Generic (CC BY-NC-ND 2.0) International License. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/2.0/.

**References**

Assante, M. J., & Lee, R. M. (2015). *The Industrial Control System Cyber Kill Chain.* SANS White Paper, October 2015. Retrieved from SANS Institute: https://sansorg.egnyte.com/dl/HHa9fCekmc Accessed 19th January 2022

Bakuei, M., Flores, R., Remorin, L., & Yarochkin, F. (2021). *2020 Report on Threats Affecting ICS Endpoints*. Retrieved from Trend Micro Research: https://documents.trendmicro.com/assets/white_papers/wp-2020-report-on-threats-affecting-critical-industrial-endpoints.pdf Accessed 18th January 2022

BEA. (2016). *Final Report: Accident on 24 March 2015 at Prads-Haute-Bléone (Alpes-de-Haute-Provence, France) to the Airbus A320-211 registered D-AIPX operated by Germanwings.* Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, France. Final Report BEA2015-0125, March 2016. Retrieved from: https://www.bea.aero/uploads/tx_elydbrapports/BEA2015-0125.en-LR.pdf Accessed 20th January 2022

Biden, J. R. (2021). *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.* July 2021. Retrieved from The White House: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ Accessed 30th July 2021

Carmakal C. (2021). Prepared Statement to the US House Committee on Homeland Security, June 9, 2021. Retrieved from https://homeland.house.gov/imo/media/doc/2021-06-09-HRG-Testimony%20Carmakal.pdf Accessed 18th January 2022

CISA. (2018). *ICS Focused Malware.* US Cybersecurity and Infrastructure Security Agency, ICS Alert (ICS-ALERT-14-176-02A), updated August 2018. Retrieved from: https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-176-02A Accessed 19th January 2022

CISA. (2019). *HatMan—Safety System Targeted Malware.* US Cybersecurity and Infrastructure Security Agency, Malware Analysis Report MAR-17-352-01, updated February 2019. Retrieved from: https://www.cisa.gov/uscert/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf Accessed 19th January 2022

CISA. (2020). *Ransomware Impacting Pipeline Operations*. US Cybersecurity and Infrastructure Security Agency, Alert (AA20-049A), updated October 2021. Retrieved from https://www.cisa.gov/uscert/ncas/alerts/aa20-049a Accessed 18th January 2022

CISA. (2021a). *Shamoon/DistTrack Malware.* US Cybersecurity and Infrastructure Security Agency, ICS Joint Security Awareness Report (JSAR-12-241-01B), updated July 2021. Retrieved from: https://www.cisa.gov/uscert/ics/jsar/JSAR-12-241-01B Accessed 19th January 2022

CISA. (2021b). *Ongoing Sophisticated Malware Campaign Compromising ICS.* US Cybersecurity and Infrastructure Security Agency, ICS Alert (ICS-ALERT-14-281-01E), updated July 2021. Retrieved from: https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-281-01B Accessed 19th January 2022

CISA. (2021c). *Cyber-Attack Against Ukrainian Critical Infrastructure*. US Cybersecurity and Infrastructure Security Agency, ICS Alert (IR-ALERT-H-16-056-01), updated July 2021. Retrieved from: https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01 Accessed 19th January 2022

CISA. (2021d). *CrashOverride Malware.* US Cybersecurity and Infrastructure Security Agency, Alert (TA17-163A), updated July 2021. Retrieved from: https://www.cisa.gov/uscert/ncas/alerts/TA17-163A Accessed 19th January 2022

CISA & FBI. (2021a). *Joint Cybersecurity Advisory: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013.* US Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, Alert (AA21-201A), updated July 2021. Retrieved from https://www.cisa.gov/uscert/ncas/alerts/aa21-201a Accessed 18th January 2022

CISA & FBI. (2021b*). DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*. US Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, Alert (AA21-131A), updated July 2021, Retrieved from: https://us-cert.cisa.gov/ncas/alerts/aa21-131a Accessed 30th July 2021

GAO. (2018). *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*. United States Government Accountability Office. GAO-19-48, December 2018. Retrieved from https://www.gao.gov/assets/gao-19-48.pdf Accessed 18th January 2022

Goodin, D. (2010). *McAfee false positive bricks enterprise PCs worldwide.* April 2010. Retrieved from: https://www.theregister.com/2010/04/21/mcafee_false_positive/ Accessed 30th July 2021

Greenberg, A. (2021). *The Full Story of the Stunning RSA Hack Can Finally Be Told*. May 2021. Retrieved from WIRED: https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/ Accessed 30th July 2021

Hoffman, M & Winston, T. (2021). *Recommendations Following the Colonial Pipeline Cyber Attack.* Retrieved from Dragos website: https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/ Accessed18th January 2022

Hunter, B. (2006). *Assuring Separation of Safety and Non-safety Related Systems*. 11th Australian Workshop on Safety Related Programmable Systems (SCS'06), Melbourne: Conferences in Research and Practice in Information Technology, Vol. 69. Retrieved from: https://dl.acm.org/doi/pdf/10.5555/1274236.1274243 Accessed 19th January 2022

Hunter, B. (2009). *Integrating safety and security into the system lifecycle.* In Improving Systems and Software Engineering Conference (ISSEC), Canberra, Australia, p. 147. August 2009

Hunter, B. (2013). *Verifying Security-Control Requirements and Validating their Effectiveness.* INCOSE Insight, Volume 16 Issue 2, pp 45-48. June 2015

IEC (n.d). *Industrial communication networks - Network and system security*, IEC 62443, all parts separately dated. International Electrotechnical Commission, Geneva

IEC. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems.* IEC 61508. International Electrotechnical Commission, Geneva.

IEC. (2019a). *Technical Report: Industrial-process measurement, control and automation – Framework for functional safety and security.* IEC TR 63069:2019, International Electrotechnical Commission, Geneva

IEC. (2019b). *Technical Report: Safety of machinery - Security aspects related to functional safety of safety-related control systems.* IEC TR 63074:2019, International Electrotechnical Commission, Geneva

ISA. (2017). Cybersecurity Related to the Functional Safety Lifecycle. ISA-TR84.00.09-2017, International Society for Automation, Research Triangle

ISACA. (2016). *The Merging of Cybersecurity and Operational Technology*. Information Systems Audit and Control Association (ISACA) White Paper.

ISACA. (2021). *ISACA Survey: IT Security and Risk Experts Share Ransomware Insights in the Aftermath of the Colonial Pipeline Attack*. May 24, 2021. Retrieved from ISACA: https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/it-security-and-risk-experts-share-ransomware-insights-in-the-colonial-pipeline-attack Accessed 30th July 2021

ISO/IEC. (2020). *Technical Report: Internet of things (IoT) — Industrial IoT*. ISO/IEC TR 30166:2020, International Organization for Standardization and International Electrotechnical Commission, Geneva

Kelso, M. (2020). *Pipelines Continue to Catch Fire and Explode*. Retrieved from: https://www.fractracker.org/2020/02/pipelines-continue-to-catch-fire-and-explode/ Accessed 30th July 2021

Moore, S. (2021). *Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans.* Retrieved from: https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we Accessed 30th July 2021

NIST. (2015). Guide to Industrial Control Systems (ICS) Security. SP 800-82 Rev. 2, May 2015. Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf Accessed 19th January 2022

NIST. (2018a). *Framework for Improving Critical Infrastructure Cybersecurity.* April 2018. Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf Accessed 19th January 2022

NIST. (2018b). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* SP 800-160 Vol 1, updated March 2018. Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf Accessed 19th January 2022

NIST. (2021). *Cybersecurity Framework Profile for Ransomware Risk Management.* NISTIR 8374 (Draft, September 2021). Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8374-draft.pdf Accessed 19th January 2022

Palmer, D. (2021). *Ransomware gangs are taking aim at 'soft target' industrial control systems.* July 2021. Retrieved from ZDnet Security website: https://www.zdnet.com/article/ransomware-gangs-are-taking-aim-at-soft-target-industrial-control-systems/ Accessed 30th July 2021

Parfomak, P.W. (2012). *Pipeline Cybersecurity: Federal Policy*. Congressional Research Service Report for Congress, R42660, August 16, 2012. Retrieved from https://sgp.fas.org/crs/homesec/R42660.pdf Accessed 18th January 2022

Paul, S., Rioux, L., Gailliard, G., & Wiander, T. (2016). *Recommendations for Security and Safety Co-engineering.* The Information Technology for European Advancement (ITEA 2) project "MERgE"

Purdue Research Foundation (T. J. Williams). (1989). *A Reference Model For Computer Integrated Manufacturing (CIM).* December 1989. Instrument Society of America, Research Triangle

Smith, T. (2001). *Hacker jailed for revenge sewage attacks*. October 2001. Retrieved from: https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage/ Accessed 19th January 2022. For more detail of the referenced court case, see also https://www.queenslandjudgments.com.au/caselaw/qca/2002/164 Accessed 30th July 2021

Timpson, D., & Moradian, E. (2018). *A Methodology to Enhance Industrial Control System Security.* Proceedings of the 22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, Belgrade, Serbia (pp. 2117-2126). Elselvier & sciencedirect.com

TSA. (2021a). *Pipeline Security Guidelines*. Retrieved from US Transport Security Administration: https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf Accessed 30th July 2021

TSA. (2021b). *Enhancing Pipeline Cybersecurity.* Security Directive Pipeline-2021-01. May 2021. Retrieved from: https://www.powermag.com/wp-content/uploads/2021/05/sd-pipeline-202-1-01-tsa.pdf Accessed 18th January 2022

# Appendix A. Supplemental Material

## A.1 Countermeasure Safety Issues

Inappropriately configured or utilised cybersecurity countermeasure can have negative impacts on safety as summarised by Table 2.

**Table 2 ~ Cybersecurity and Safety Conflict Issues**

| 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 patch in pre-production platform |
| AV false positive | Could stop safety functions | Verify anti-virus update in pre-production platform |
| PKI certificates expiry | Could stop safety functions | Ensure safety functions not compromised by authentication failures |
| Firewall policy changes | Could stop safety communications or dependencies | Validate and control firewall policy especially in safety conduits |
| Password expiry policy | Enforced timeout on passwords may stop operator from enacting safety-related commands | Ensure effective access control management that maintains safety controls |
| Intrusion Protection System (IPS), Endpoint Detection and Response (EDR & XDR) | Could stop safety functions if these are visibly confused with cyber-attack | Isolate IPS, Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) systems from critical safety zones |
| Networked or portable malware scanning and removal tools | False positives could remove OT critical files and applications | Validate tool in OT sandbox or test environment. Set to delete files manually. |
| Online control system internet presence discovery tools, e.g. Shodan, Google dorks | Could expose safety-system addressing to threat actors. | Use offline tools instead, e.g. NMAP, ZENMAP |

## A.2 Generic Framework Profile for Safety Systems

The NIST Cybersecurity Framework (NIST 2018a) provides a complete security cycle perspective for aspects of identification, protection, detection, response, and recovery to maintain the cybersecurity of systems. NIST has published a draft CSF profile for ransomware of critical infrastructure (NIST 2021) which provides a tailoring to the profile application to Ransomware (along with other Malware) and System Safety mitigation in Operational Technology (OT). This can be useful to assess countermeasures applied to these systems and threats they address. This framework allows specific profiles to be tailored to a system and its cybersecurity risks. Table 3 proposes safety considerations for CSF cycles and categories.

**Table 3 ~ Framework Profile Considerations for Safety**

| NIST CSF Cycle | Category | Functional Safety Considerations |
|---|---|---|
| Identify (ID) | Asset Management (ID.AM) | Safety assets and configuration identified. |
| | Business Environment (ID.BE) | Organizational safety roles and responsibilities assigned |
| | Governance (ID.GV) | Safety regulatory requirements established. |
| | Risk Assessment (ID.RA) | Safety included in hierarchy of risk assessment. |
| | Supply Chain Risk Management (ID.SC) | Response and recovery plans are tested to include safety responses. |
| Protect (PR) | Identity Management, Authentication and Access Control (PR.AC) | Network segmentation and air-gapping of safety related systems established and maintained |
| | Awareness and Training (PR.AT) | Awareness and training include interaction between safety and security responsibilities. |
| | Data Security (PR.DS) | Penetration and visibility testing is conducted with safety in mind |
| | Information Protection Processes and Procedures (PR.IP) | Response and recovery plans regularly tested with safety and cybersecurity actions<br>Vulnerability management and patching includes impact and integrity of safety systems |
| | Maintenance (PR.MA) | Changes to safety system are approved, logged, and performed in a manner that prevents unauthorized access |
| | Protective Technology (PR.PT) | Fail-safe and fail-secure mechanisms are established to deal with dangerous cyber events. |

| NIST CSF Cycle | Category | Functional Safety Considerations |
|---|---|---|
| Detect (DE) | Anomalies and Events (DE.AE) | System safety is included in determination of event impact. |
| | Security Continuous Monitoring (DE.CM) | Isolated safety zones are monitored for evidence of intrusion. |
| | Detection Processes (DE.DP) | Cybersecurity intrusion detection and protection systems do not compromise safety functions, e.g. false positives |
| Respond (RS) | Response Planning (RS.RP) | Joint safety and security response plans are executed to protect safety during attack. |
| | Communications (RS.CO) | Information is shared between safety and security personnel and coordination is practiced to minimise dangerous failures. |
| | Analysis (RS.AN) | Safety and security personnel cooperate on forensics and accident analysis that results from event. |
| | Mitigation (RS.MI) | Safety and security personnel coordinate mitigation of the event including precautionary shutdowns |
| | Improvements (RS.IM) | Safety and security personnel cooperate on lessons learned from the event. |
| Recover (RC) | Recovery Planning (RC.RP | Restoration plans are coordinated between safety and security. |
| | Improvements (RC.IM) | Lessons learned are included into response plans and processes. Gaps in safety and security protections are acted on. |
| | Communications (RC.CO) | Restoration plans are coordinated between safety and security including return to safe-state operations. |

This collation page left blank intentionally.