Australian Government

ANSTO

Nuclear Cyber Engineering

An Emergent Systems View of Computer Security

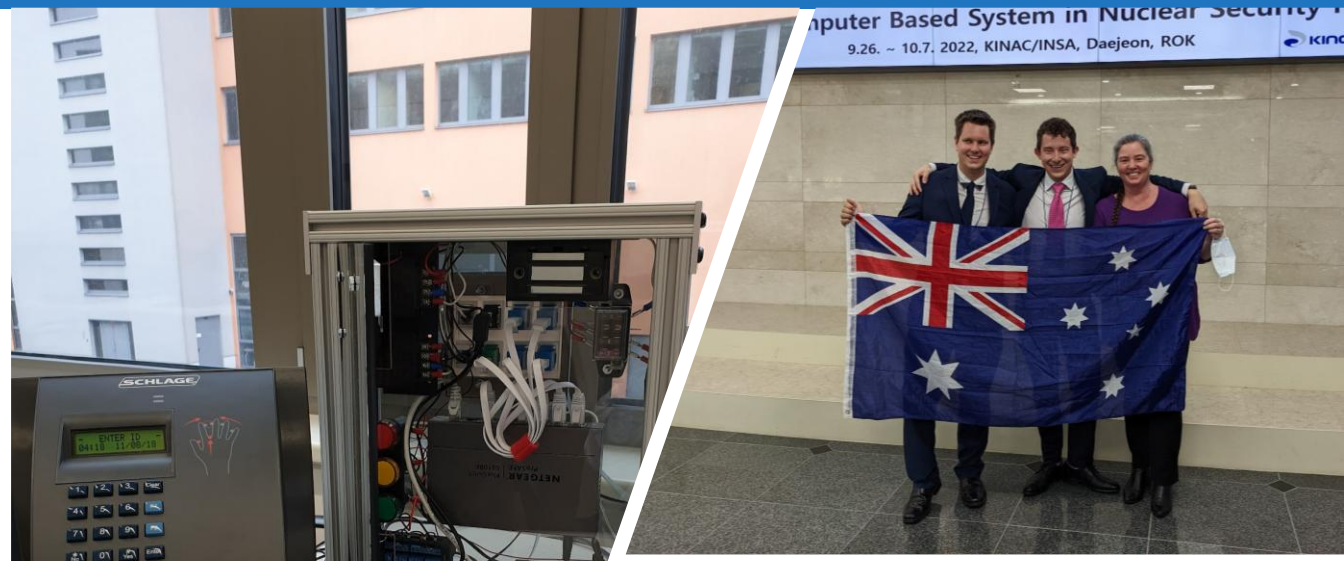
Mitchell Hewes

mitchell@ansto.gov.au

Science. Ingenuity. Sustainability.

Background

- The International Atomic Energy Agency is the global centre for nuclear cooperation, supporting Member States to ensure safe, secure and peaceful use of nuclear technologies.
- It operates through international consensus, developing guidance and standards, delivering training and exercises, and coordinating expert collaboration and research.
- Member States implement these frameworks nationally, with the IAEA providing support, peer exchange and capability uplift.
- ANSTO applies this guidance within its nuclear facilities, integrating it into cyber security, safety and risk management practices.
- ANSTO also contributes to the international system by helping develop guidance, training, research and communities of practice in nuclear cyber security.
- This creates a continuous loop:
  - international standards → national implementation → operational feedback → strengthened global practice.

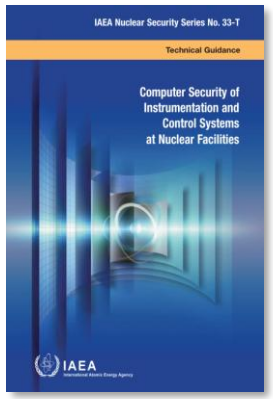


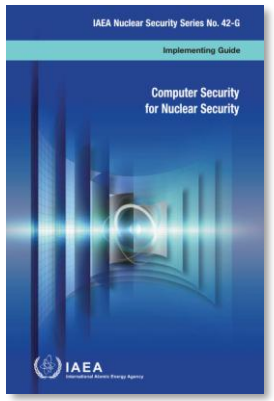
Fundamentals (PRINCIPLES)
- Objectives and principles
- Essentials from international instruments

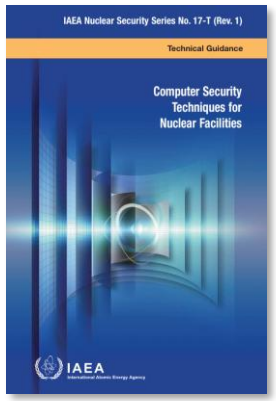
Recommendations (WHAT)
- General approaches, actions, concepts and strategies to achieve and maintain effective nuclear security

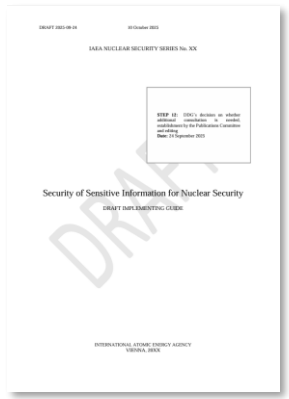
Implementing Guides (HOW)
- Broad guidance on the means by which States could meet Recommendations

Technical Guidance (DETAILS)
- Guidance on the implementation of specific technical subjects









IAEA NUCLEAR SECURITY SERIES

NSS documents assist in the implementation of obligations contained in international legal instruments relevant to nuclear security

Guidance on supply chain security already exists at the Implementing Guide (HOW) and Technical Guidance (WHAT) levels.

ANSTO

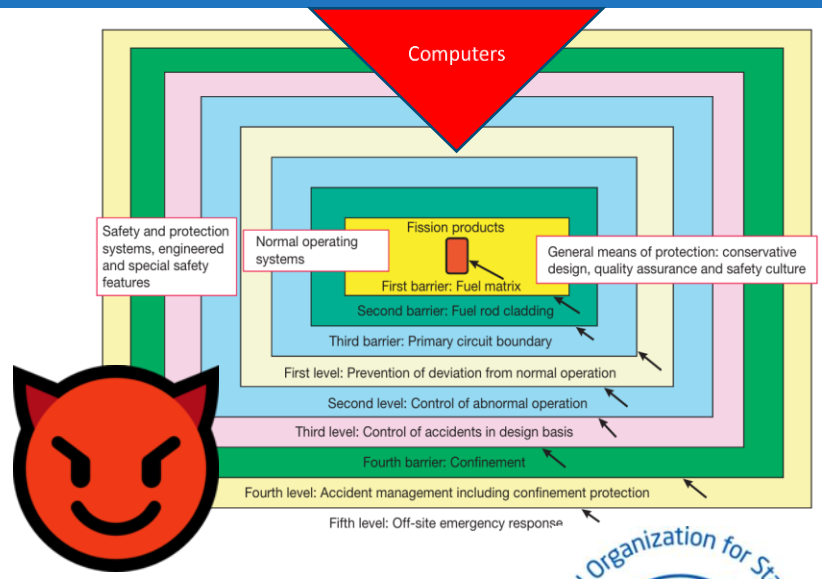
Computers in Nuclear

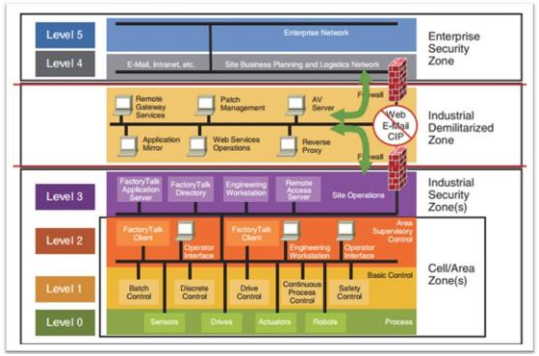
Topic	IT	I&C
Availability	Delays accepted	24 x 7 x 365
Time critical content	Generally delays accepted	Critical – time precision
Technology support lifetime	2 to 3 years	20+ years
Security upgrades	Regular/scheduled	No common practice
Antivirus	Very common, easily deployed and updated	Uncommon and can be difficult to deploy
Incident response	Well defined and deployed	Uncommon
Security testing/audits	Scheduled and practiced	Not well established
Risk	• Information centric • Loss or corruption of information can ruin a business • Relatively quick recovery	Safety, security, and operations centric Physical consequences of compromise Long recovery timelines

ANSTO

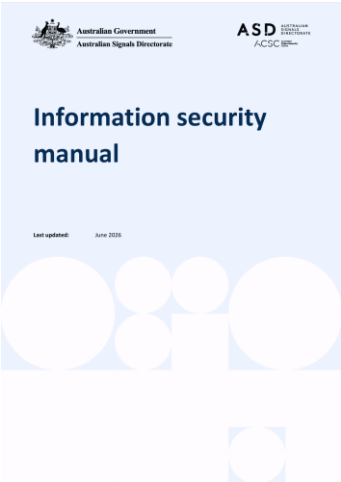
Why is Nuclear Different?

- Nuclear facilities are complex, tightly coupled systems.
- Additive, controls-based approaches treat symptoms, not the system. By focusing on individual components or known vulnerabilities, they apply countermeasures after the design is fixed.
- A single compromise can propagate across interconnected functions and cascade into consequences no single control was designed to prevent.
- Controls may be numerous and compliant yet remain disconnected from the outcomes that matter most: preserving safety and security.
- An engineering approach to cyber security inverts this logic. It begins with the consequences to be avoided and the functions that must endure, then designs security into the system from the outset. Integrating architecture, defence-in-depth, and functional requirements across the full lifecycle rather than bolting them on afterward.





International Organization for Standardization
ISO
27002



In high-hazard environments like nuclear, the question is not whether controls exist but whether important functions for safety and security continue when controls fail. Assurance over compliance.

ANSTO

Establishing an

effective* and *sustainable

nuclear security infrastructure is crucial for the

protection of individuals, society and the environment.

A Nuclear Security event can represent an unacceptable consequence.

Image Credit: Macrovector / Freepik

Computer Security

From securing computers to preserving functions.

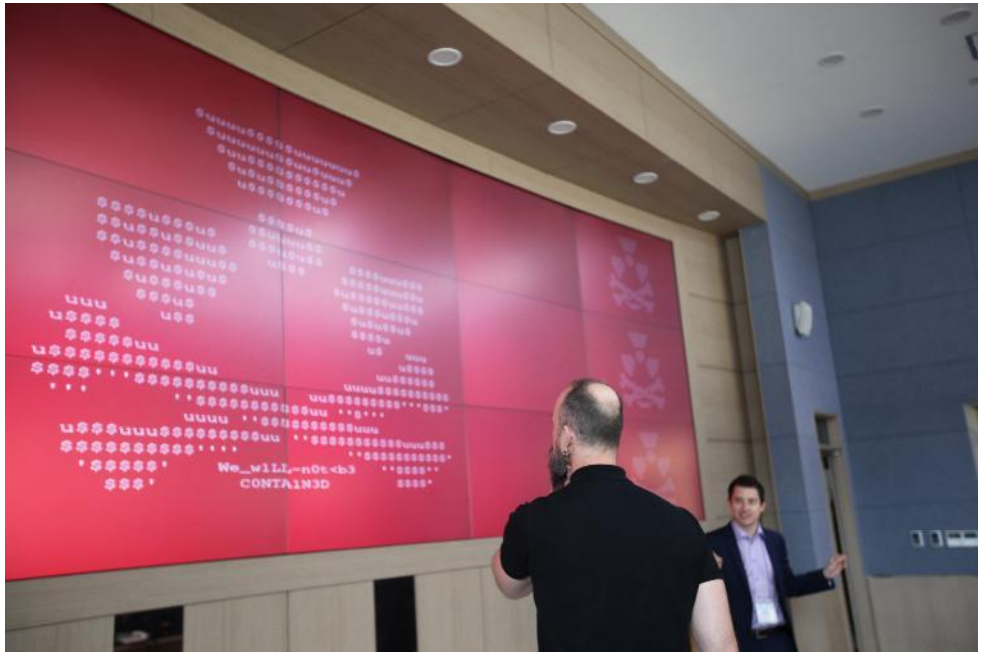
International Atomic Energy Agency (IAEA) Nuclear Security Series No. 42-G, “Computer Security for Nuclear Security,” Vienna, Austria, July 2021.
International Atomic Energy Agency (IAEA) Nuclear Security Series No. 17-T (Rev. 1), “Computer Security Techniques for Nuclear Facilities,” Vienna, Austria, September 2021.

ANSTO

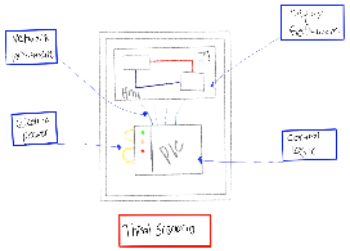
PoC Consequences of Compromise

Live-fire Exploitation of Nuclear-rated I&C while providing for boiler-level control to demonstrate consequences.

Silent modification of RID Firmware.



DoS of CAS (AC&D, Display, and Comms) from outside the perimeter fence via an undocumented wireless interface...



Training equipment for consequence-demonstrations and initial mock-up.

Exploited by an adversary in a ghillie suit on a grassy knoll.

ANSTO

Security – Functional Preservation Lens

Operational Functions

Safety and Security Functions

Emergency Preparedness and Response Functions

Computer based systems performing or supporting functions form an attractive target. They support the performance of these functions that provide for defence in depth.

Adversaries will seek to defeat these defences to cause a potential incident

Computer Security in the Nuclear Security Series – preserving the ability of organisations to operate normally and protect from, detect, respond to and recover from adversary action against computer-based systems

ANSTO

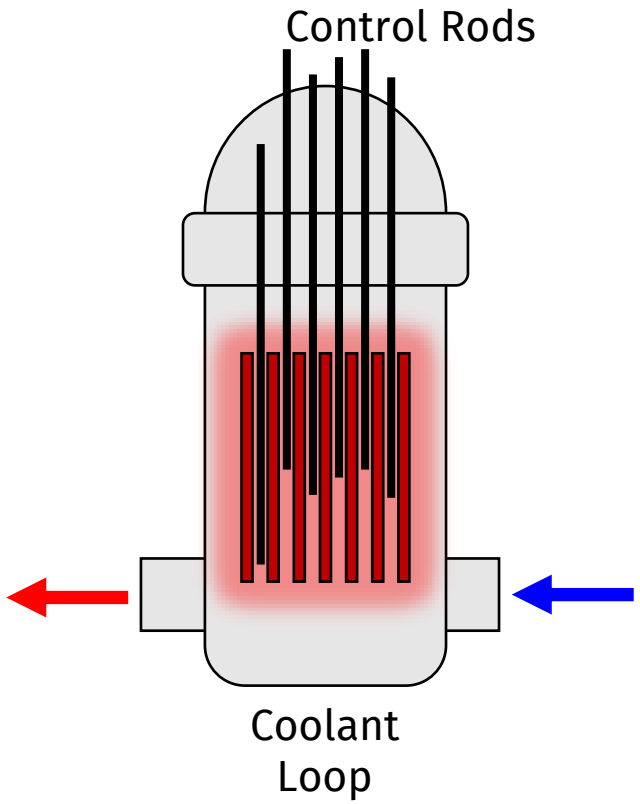
A Nuclear Safety Example

The function of PWR emergency core cooling does not rely on a single system

Nuclear safety relies on maintaining two independent but complementary functions:

- Reactivity control through control rods and neutron absorbers to regulate the reaction
- ***Continuous removal of heat (inc. decay heat)***

Each function is delivered through multiple, diverse and redundant systems, ensuring it can be maintained despite failure of individual components.



High Pressure Core Cooling
(HPI / CVCS)

Pressure Transition
(Relief Valves / ADS)

Low Pressure Core Cooling
(LPI / RHR)

Reflood & Stabilisation
(LPI / Accumulators)

Long-Term Heat Removal
(RHR / Spray)

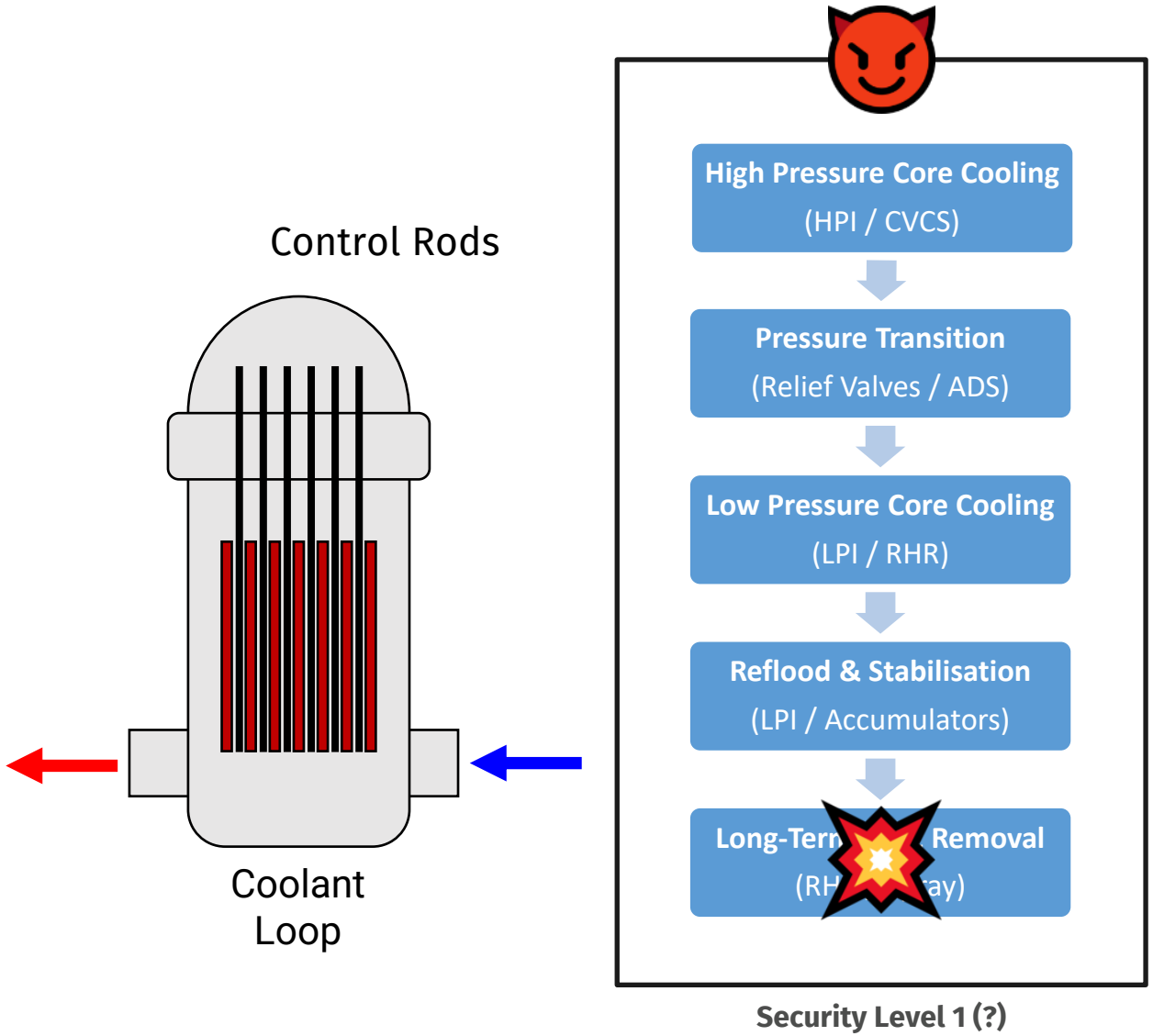
Emergency core cooling provides safety defence-in-depth through diverse systems.

Safety functions rely on computer-based systems and require protection.

Security must preserve the function, not just the systems that delivers it.

ANSTO

A Nuclear Safety Example



- Control systems never operate in isolation. To function, they depend on external factors that breach containment each becoming a potential pathway in or out.
- Safety defence-in-depth assumes random, uncoordinated failures. It relies on the statistical improbability of multiple independent systems failing at the same moment.
- Security defence-in-depth faces an intelligent, predatory adversary, one who actively studies those same systems and engineers the simultaneous failures that safety assumes will never coincide.
- Security must therefore reinforce the safety barriers, not merely sit alongside them preserving the important function even when an adversary targets the design itself.

Placing a complex web of dependent systems within a single security perimeter (while assuming safety barriers will prevent malicious acts) is a flawed security strategy.

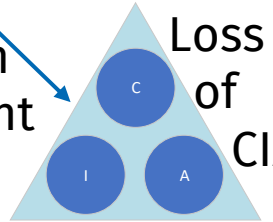
A Security Response

Adversary

Exploits vulnerability

Action on equipment

Results in equipment impact



Loss of CIA

NSS provides a view of function perseverance that goes beyond a single successful cyber-attack,

focusing on minimising impact and preserving functions.

Results in impact to function

System Function

Unknown State

Unexpected Behavior

Failure

No effect

Possible Consequence

Manipulation
(Outside Safety Case)

Observable Failure
(Within Safety Case)

Function Continues

Control-based Risk Management
(e.g. ISM, ISO27K/IEC 62443, NRC RG 5.71 Rev. 0)

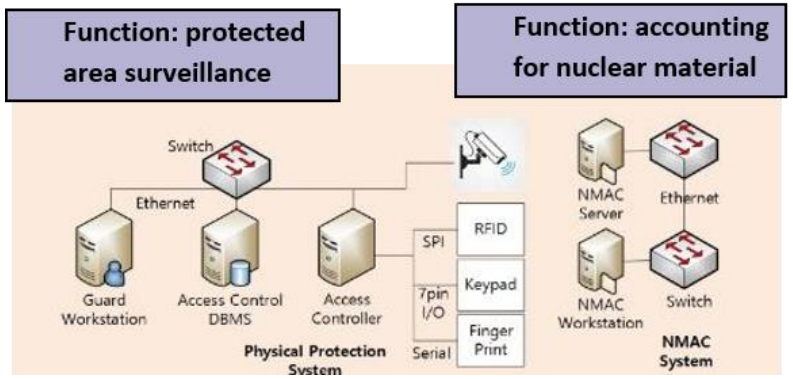
Function-based Risk Management
(e.g. IAEA NSS, IEC 62645, ONR TAG, NRC Adv. Reactor Draft Rulemaking, NIST SP 800.160 Vol.1 Rev.1)

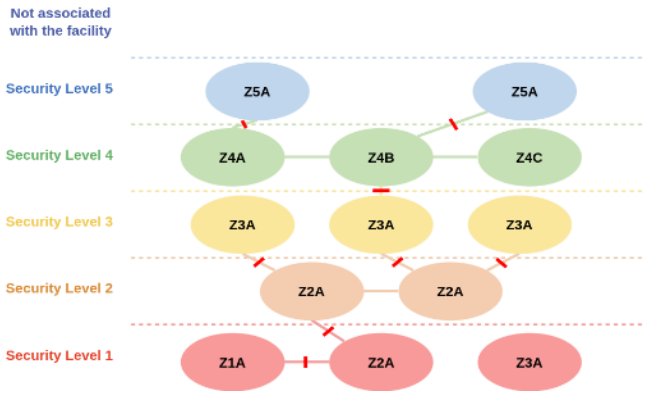
ANSTO

Managing Computer Security Risk

Facility computer security risk management **(FCSRM)**

- ✓ Identify all the functions in a facility and the relationships they have to maintaining operations and ensuring safety and security **defence in depth**
- ✓ Determine function "significance" by assessing how the **worst consequences** of C/I/A compromise may contribute to an event
- ✓ Assign each function to a security level using a **graded approach**
- ✓ Design the defensive computer security architecture (DCSA), defining functional computer security requirements for each security level.





System computer security risk management **(SCSRM)**

- ✓ For each system, identify the **function(s)** it contributes to
- ✓ Group **systems** into **zones**, considering their support to **defence in depth**
- ✓ Apply **computer security measures** to every **system** and **decoupling measures** between zones.
- ✓ Finalise the **DCSA**, describing the actual implementation of **design constraints**, **architecture**, and **computer security measures** for each **system** and **zone**.

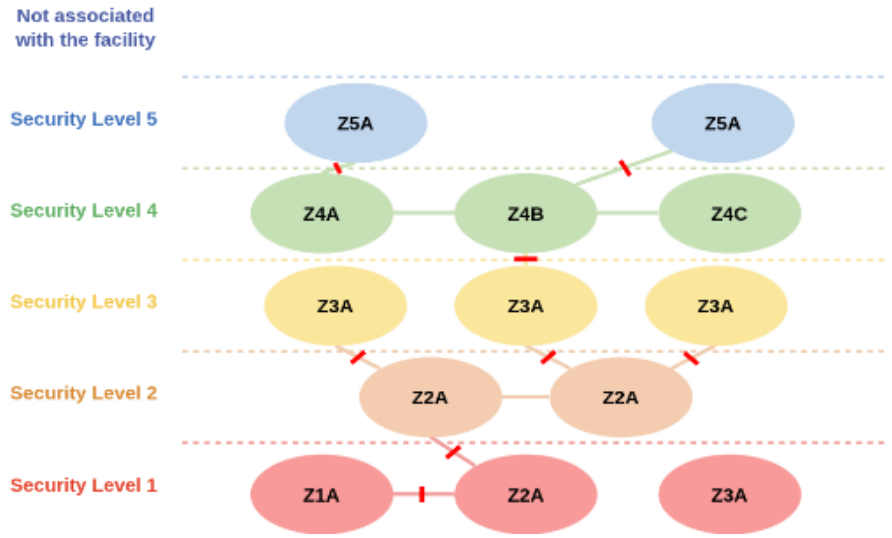
ANSTO

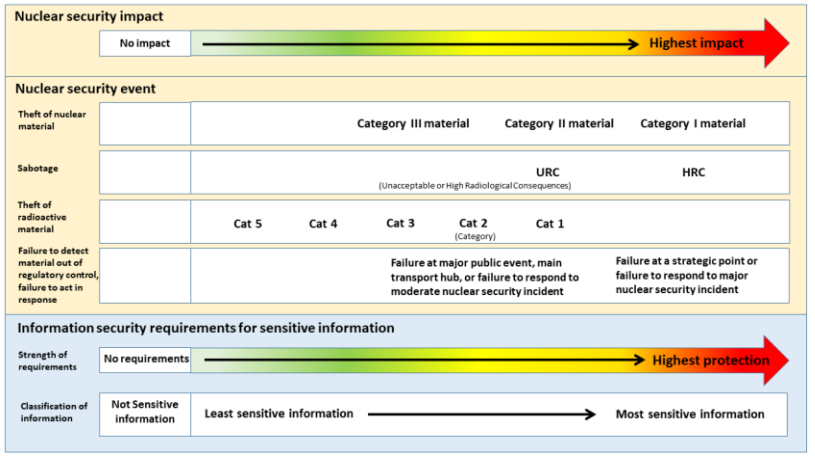
Defending Functions, Not Computers

When implemented correctly a DCSA:

- Focuses on preventing the consequences of cyber-attacks by preserving important functions through a graded, defense-in-depth approach.
- Results in establishing protection, detection, and response mechanisms that can demonstrate support to nuclear safety and nuclear security objectives.
- Enables secure integration of computer-based systems while allowing resource-effective adaptation to emerging threats.
- Requires subject matter expertise on both computer security and the functional design of the facility or activity.

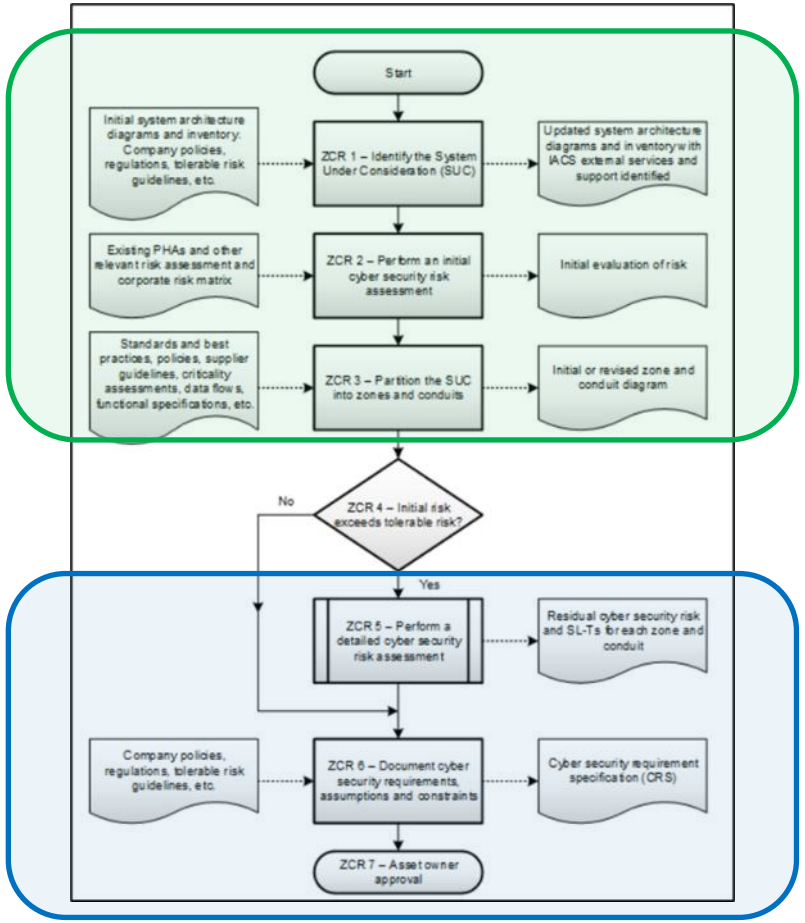
A DCSA changes the goal itself from “deploying controls and demonstrating compliance” to “assuring the continued, trustworthy performance of the functions that keep the facility safe and secure.”





Similar Guidance and Standards

IEC 62443-3-2 two level risk assessment



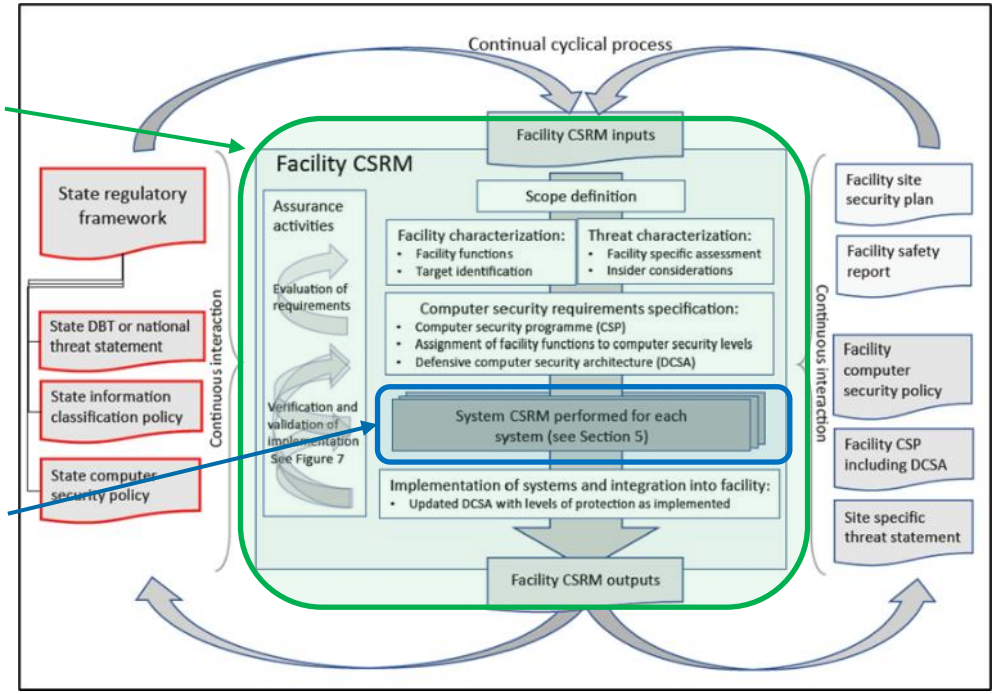
High level Risk Assessment

Detailed CS Risk Assessment

IAEA NSS 17-T (Rev 1) two level risk assessment

Facility CS Risk Assessment

System CS Risk Assessment



IEC 62645 also describes two levels of computer security risk assessment

INTERNATIONAL ELECTROTECHNICAL COMMISSION, "Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design", IEC 62443-3-2:2020, IEC, Geneva (2020).

INTERNATIONAL ELECTROTECHNICAL COMMISSION, "Nuclear power plants - Instrumentation, control and electrical power systems - Cybersecurity requirements", IEC 62645:2019, IEC, Geneva (2019).

While IEC 62443-3-2 uses functional safety as an input to developing secure architectures, the NSS approach was designed to allow the integration of cyber, physical, and functional risks across the entire facility lifecycle.

ANSTO

Information Security

Modern information serving as the basis for action.

International Atomic Energy Agency (IAEA) Nuclear Security Series No. 23-G, “Security of Nuclear Information,” Vienna, Austria, 2015.
International Atomic Energy Agency (IAEA) Draft Implementing Guide NST070 Step 12, “Information Security for Nuclear Security,” Vienna, Austria, 2025.

ANSTO

Limits of Containment

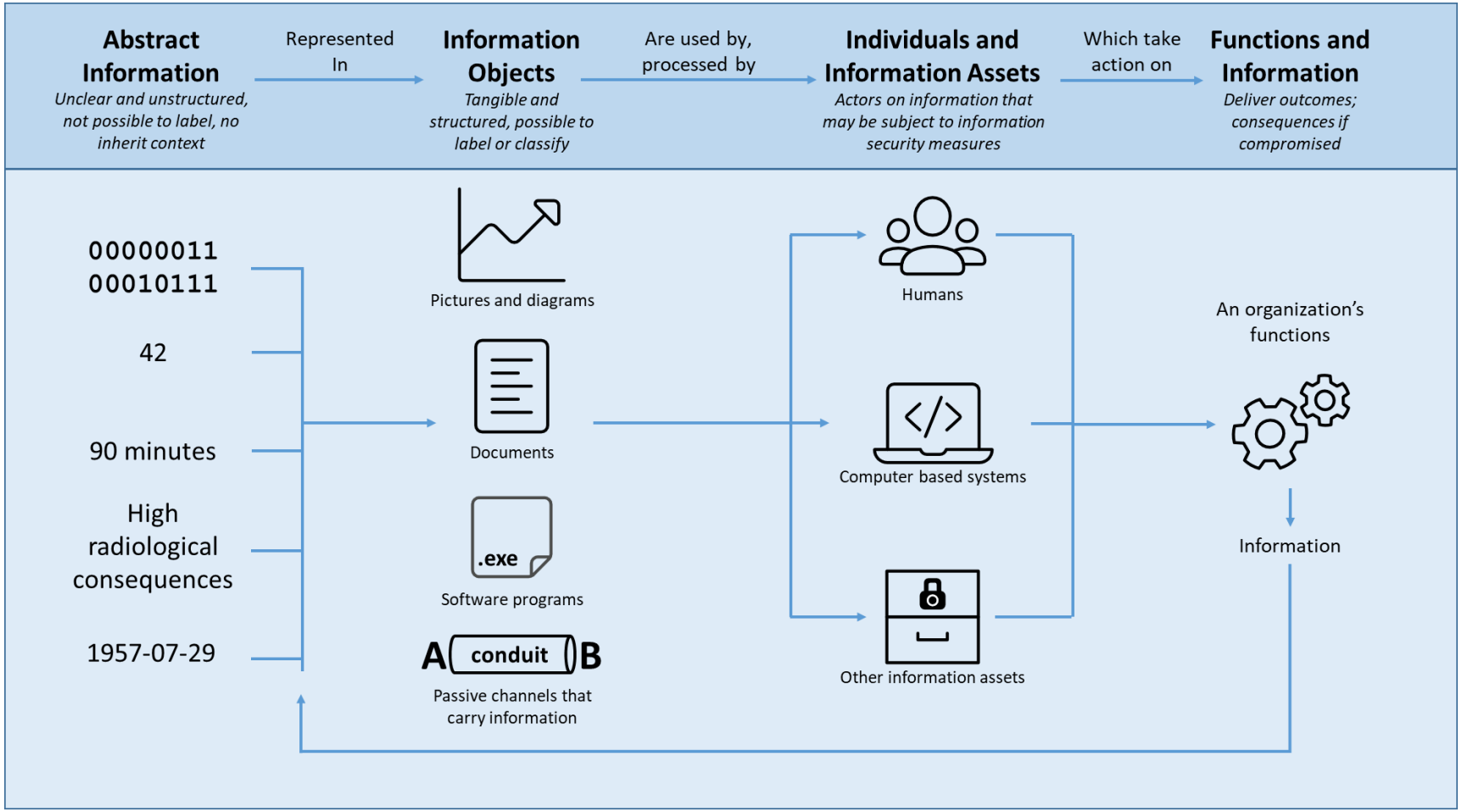
- Old models in the NSS relied on a containment-centric posture focused on the physical protection of tangible information based on an assumed static value. Information was equated to nuclear material.
- The assumption was that if the physical object (like a hard copy doc or MS Office file) was contained, the information itself remained secure.
- Modern Information is now a dynamic component necessary for nuclear safety and security functions, not just a static asset to be locked away.
- Traditional containment models fail to address how information is used, trusted, and potentially exploited.

Four Identified Problems

1. Information resists containment
2. Automation amplifies vulnerability
3. Recognition of asymmetric value
4. Information security lifecycles mirror records management.

HEWES, M., STJOHN-GREEN, M., "Why Nuclear Security Needs Information Security: The Promise Of NST070", IAEA CyberCon26, Vienna, (2026).

Functional Assurance for Information

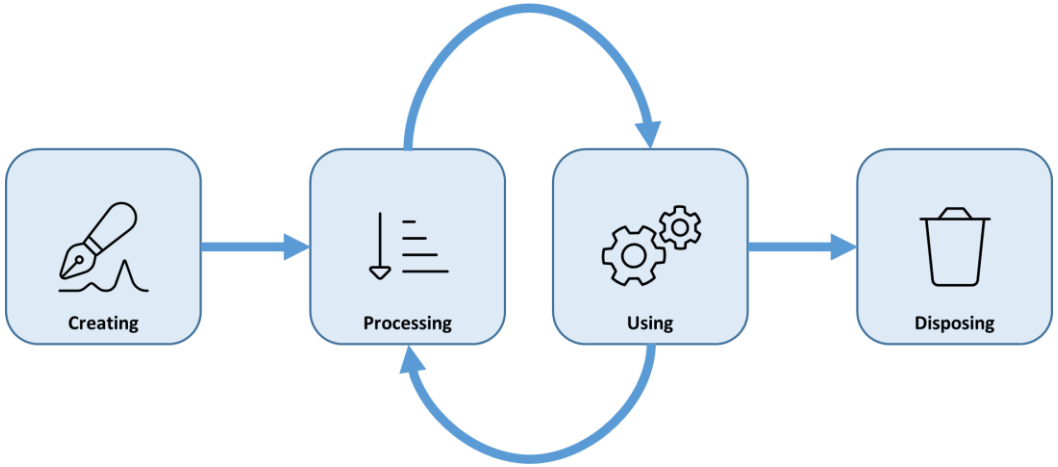


The model utilises a risk-informed, graded approach that prioritises the trustworthy performance of important functions over simply preventing unauthorised disclosure.

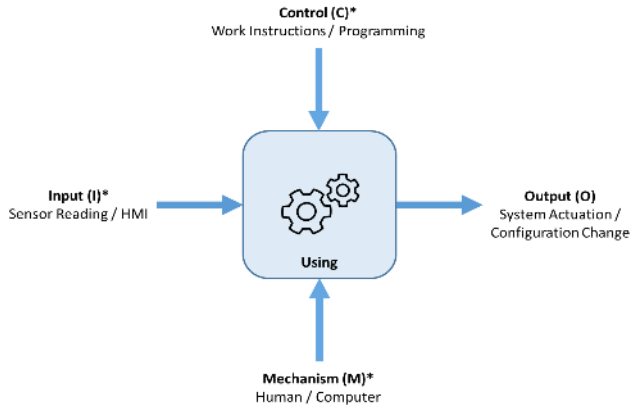
Realigning the Information Lifecycle

- Most information security lifecycles mirror administrative records management, prioritising the custody of an object over its contribution to functions.
- NST070 simplifies and redefines the lifecycle into four action-oriented stages directly tied to functional outcomes:

1. **Creating**: Activities performed to identify or assemble an information object from abstract information or other information objects.
2. **Processing**: Activities performed on information/information objects, affecting C/I/A.
3. **Using**: Activities performed using information/information objects, reliant on C/I/A.
4. **Disposing**: Activities performed to archive or destroy information/information objects ensuring they can no longer impair a function.



NST070 Fig. 6. The four stages of the information life cycle and the relationships between them.

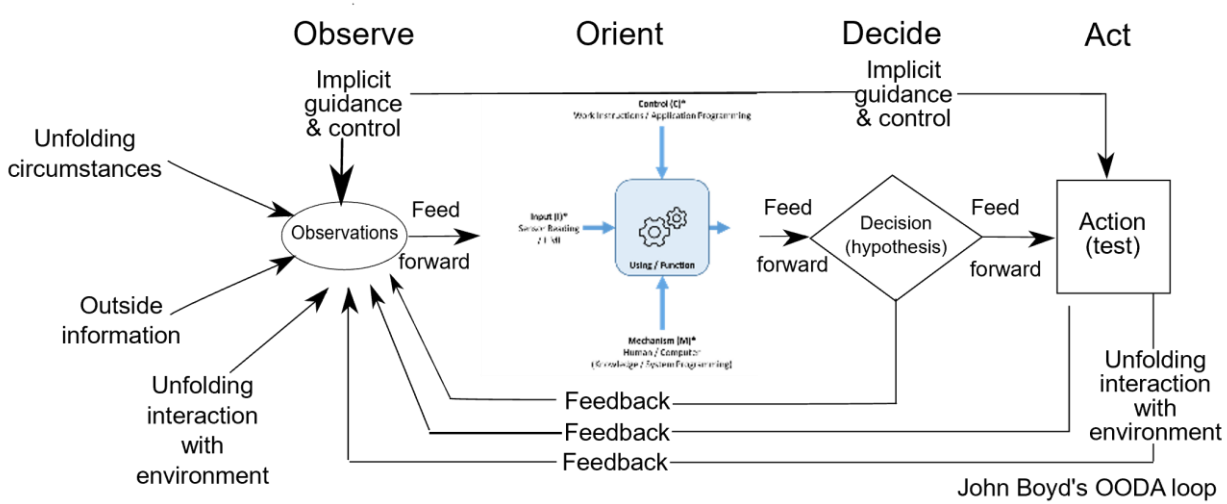


** Vulnerability to a loss of Confidentiality, Integrity, and Availability of Sensitive Information*

HEWES, M., STJOHN-GREEN, M., "Why Nuclear Security Needs Information Security: The Promise Of NST070", IAEA CyberCon26, Vienna, (2026).

Preserving the Orientation

- Nuclear facilities operate with a fixed orientation defined by strict procedures, known capabilities, and operate on real-time environmental sensor readings.
- When executing an attack adversaries do not target information for its own sake; they target this fixed decision-making process to map limitations or covertly corrupt the orientation.
- An attacker can decouple the facility's orientation from reality, turning the system into an unwitting agent of their intent.
- By securing sensitive information relative to its use, defenders can take systemic actions to preserve their orientation during an active encounter.



Systems Engineering

Towards a future of security assurance, not just control compliance.

ANSTO

Engineering Computer Security

- IAEA guidance calls for a function-based approach to risk management.
- But traditionally computer security is driven by details of exploitable vulnerabilities.

- Computer security adds security measures to protect digital technology.
- But *good engineering* should mean building security into the digital technology.

- Safety relies on the security of its digital technology.
- If it's not secure; it's not safe!

What does this all mean?

What is the suitable response to an Operational Environment increasingly characterised by

Predatory Hostility

With intended or ransomed outcomes of:

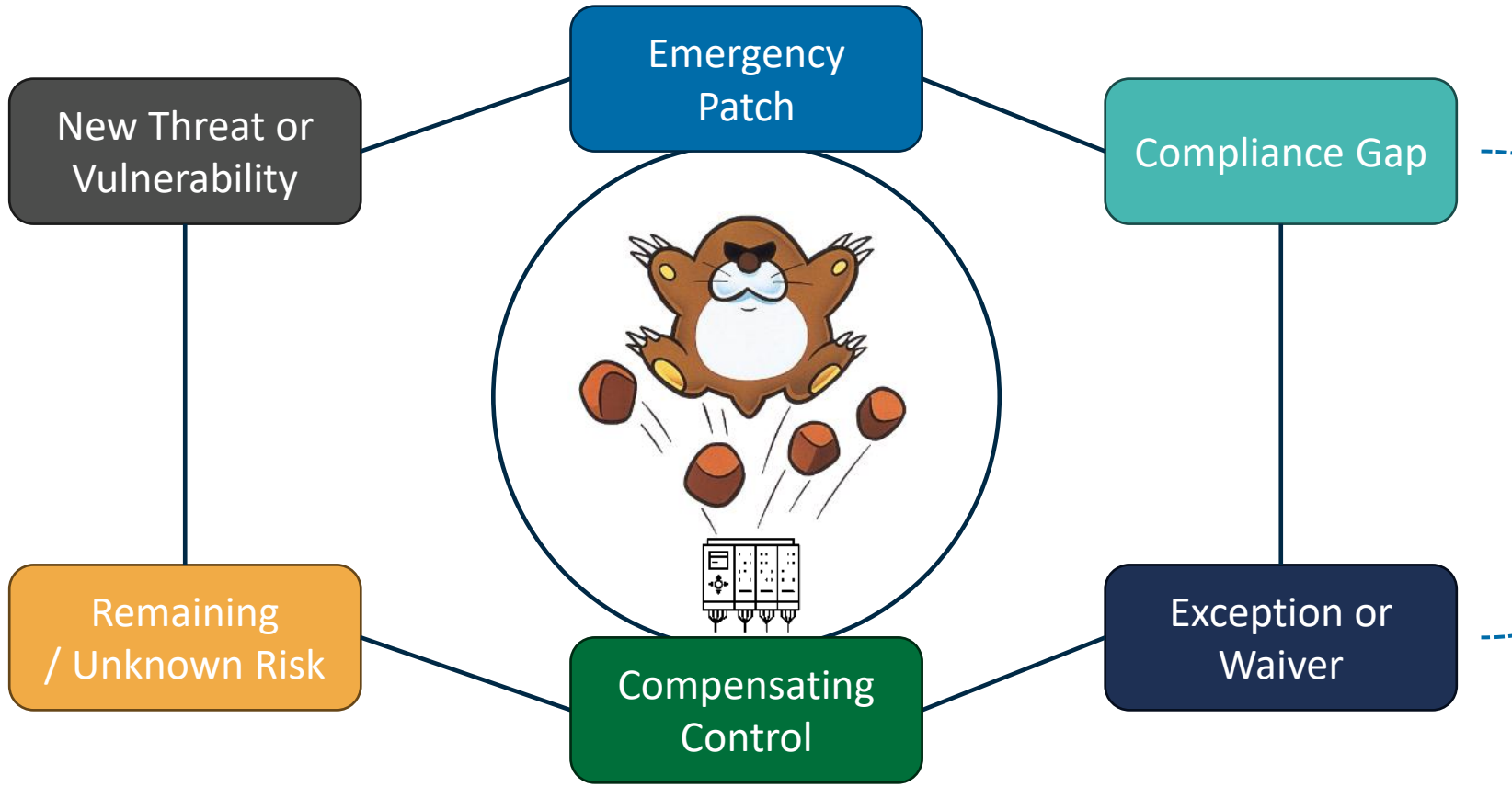
Damage **Disrupt** **Destroy**

This section brings together ideas from:

INCOSE IAEA ANSTO

STJOHN-GREEN, M., HEWES, M., "Where To Start — The System or the Function? How the V-model Clarifies Effective Computer Security", IAEA CyberCon26, Vienna, (2026).
WINSTEAD, M., SSE WORKING GROUP, "Systems engineer's security orientation", 36th Annual INCOSE International Symposium, INCOSE (2026).

Calling It Like It Feels: Whac-a-Mole



Activity can look like progress while architecture and assurance remain fragile.

Security keeps everyone busy without making systems inherently more trustworthy.

Prescriptive controls miss system-specific, emergent, and mission-driven risks while encouraging barriers and patches after design, increasing cost, schedule pressure, and complexity.

HUMES, M., WINSTEAD, M., HEWES, M., "Beyond Mogura Taiji security for executives and leaders toward building inherently secure and resilient systems", 36th Annual INCOSE International Symposium, INCOSE (2026).

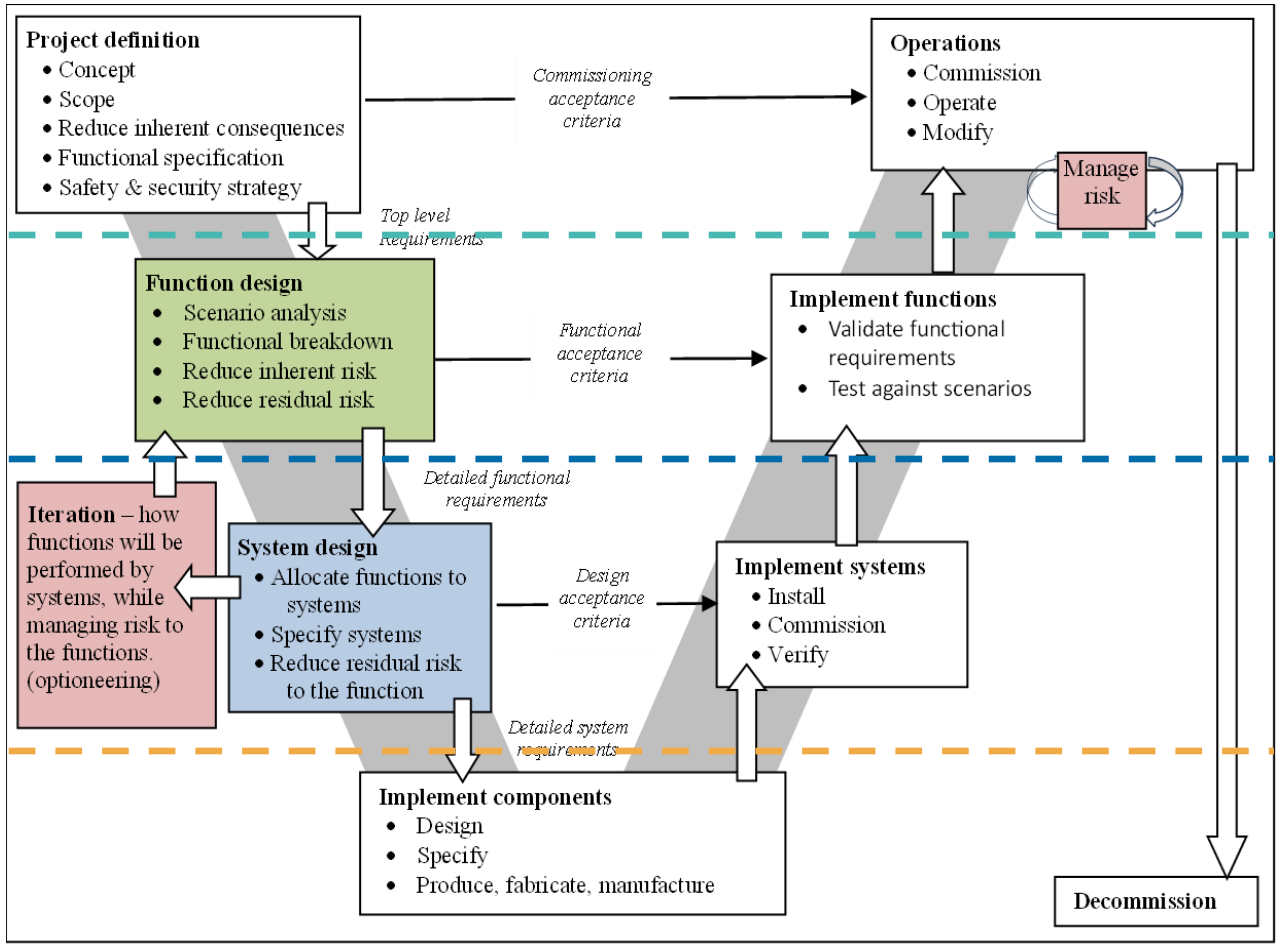
How It Should Feel: Engineering Assurance

Future State Goals

Function-based Standards

System-based Standards

Control Catalogues



Key Outcomes:

- Deliver coherence, mutual reinforcement, and assurance of adequate security with all aspects of design.
- Functional level: identify and remove avoidable risk of harm, by design.
- Modify the design to reduce the residual risk, where possible.
- System level: manage vulnerabilities against risk of harm to functions.

- If we start with systems, we still need to understand functions.
- Design should anticipate managing risks in operations.

STJOHN-GREEN, M., HEWES, M., "Where To Start — The System or the Function? How the V-model Clarifies Effective Computer Security", IAEA CyberCon26, Vienna, (2026).

Protective Mindset: Reaching its Limit?

Traditional protective mindset

- Broaden standards
- Extend compliance
- Add controls
- Patch after discovery

Functional perseverance

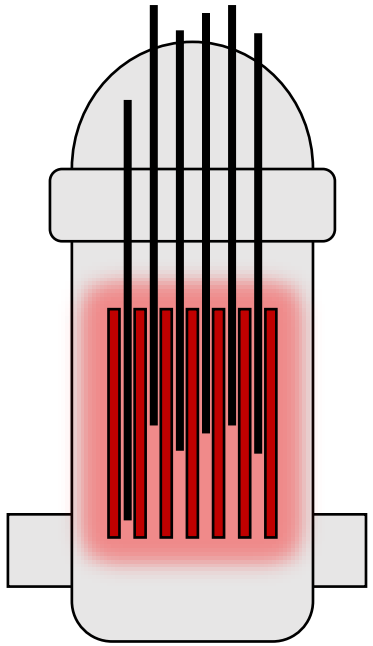
- Engineer capability
- Evolve through life cycle
- Balance system tradeoffs
- Keep mission relevance

Important inversion: controls become a representation of engineered capability, not a substitute for good engineering.

WINSTEAD, M., SSE WORKING GROUP, "Systems engineer's security orientation", 36th Annual INCOSE International Symposium, INCOSE (2026).

ANSTO

Loss-Driven Requirements



1. **Needs**: What constituents require to function and trust
2. **Loss**: What would be intolerable if impaired or destroyed
3. **Ability**: What the system must be able to do before, during, and after confrontation
4. **Requirements**: Verifiable statements that drive architecture and V&V

Losses may arise from more than just the traditional system/component failures.

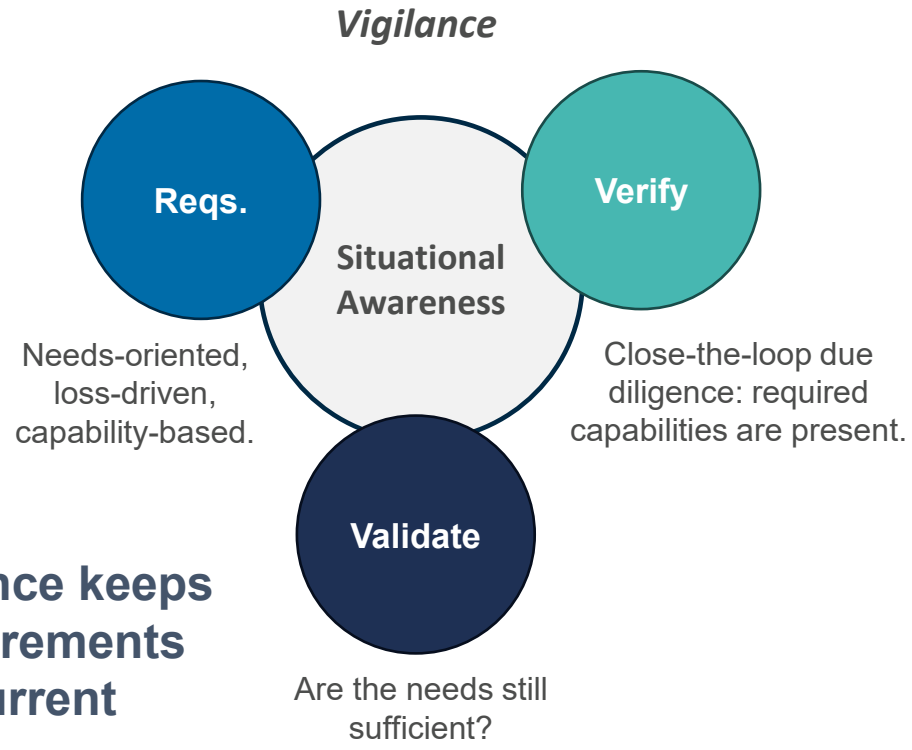
UCA Category	Description (STPA)
Not Provided	A control action required for safety is not provided or is not followed.
Provided	An unsafe control action is provided that leads to a hazard.
Timing/Sequence	A potentially safe control action is provided too late, too early, or out of sequence.
Duration	A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action).

Identifying intolerable loss requires common sense and mission knowledge; it does not require knowing every attack path.

WINSTEAD, M., SSE WORKING GROUP, "Systems engineer's security orientation", 36th Annual INCOSE International Symposium, INCOSE (2026).
LEVESON, N.G., Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, Cambridge, MA (2012).

ANSTO

Engines of Functional Perseverance



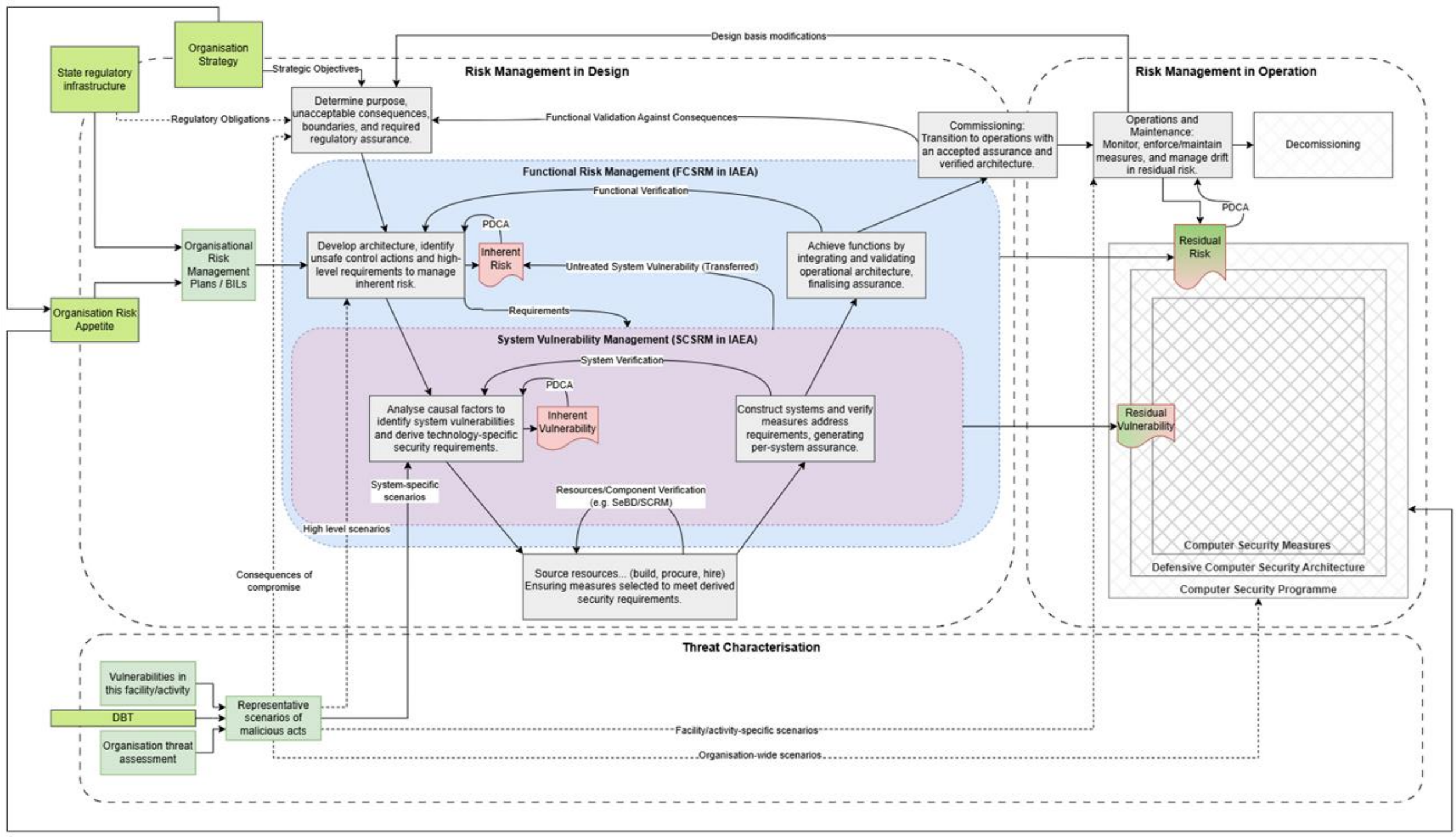
Vigilance keeps requirements current

Resilience keeps capability viable

Predatory attack evolution means security mechanisms evolve, or the system eventually ceases to be viable.

WINSTEAD, M., SSE WORKING GROUP, "Systems engineer's security orientation", 36th Annual INCOSE International Symposium, INCOSE (2026).

ANSTO


Organisation Strategy
State regulatory infrastructure
Strategic Objectives
Design basis modifications
Risk Management in Design
Risk Management in Operation
Regulatory Obligations
Determine purpose, unacceptable consequences, boundaries, and required regulatory assurance.
Functional Validation Against Consequences
Commissioning: Transition to operations with an accepted assurance and verified architecture.
Operations and Maintenance: Monitor, enforce/maintain measures, and manage drift in residual risk.
Decomissioning
Functional Risk Management (FCSRM in IAEA)
Functional Verification
PDCA
Organisational Risk Management Plans / BILs
Develop architecture, identify unsafe control actions and high-level requirements to manage inherent risk.
Inherent Risk
Untreated System Vulnerability (Transferred)
Achieve functions by integrating and validating operational architecture, finalising assurance.
Residual Risk
Organisation Risk Appetite
Requirements
System Vulnerability Management (SCSRM in IAEA)
System Verification
PDCA
Analyse causal factors to identify system vulnerabilities and derive technology-specific security requirements.
Inherent Vulnerability
Construct systems and verify measures address requirements, generating per-system assurance.
Residual Vulnerability
System-specific scenarios
Resources/Component Verification (e.g. SeBD/SCRM)
High level scenarios
Computer Security Measures
Defensive Computer Security Architecture
Computer Security Programme
Consequences of compromise
Source resources... (build, procure, hire) Ensuring measures selected to meet derived security requirements.
Threat Characterisation
Vulnerabilities in this facility/activity
DBT
Organisation threat assessment
Representative scenarios of malicious acts
Facility/activity-specific scenarios
Organisation-wide scenarios

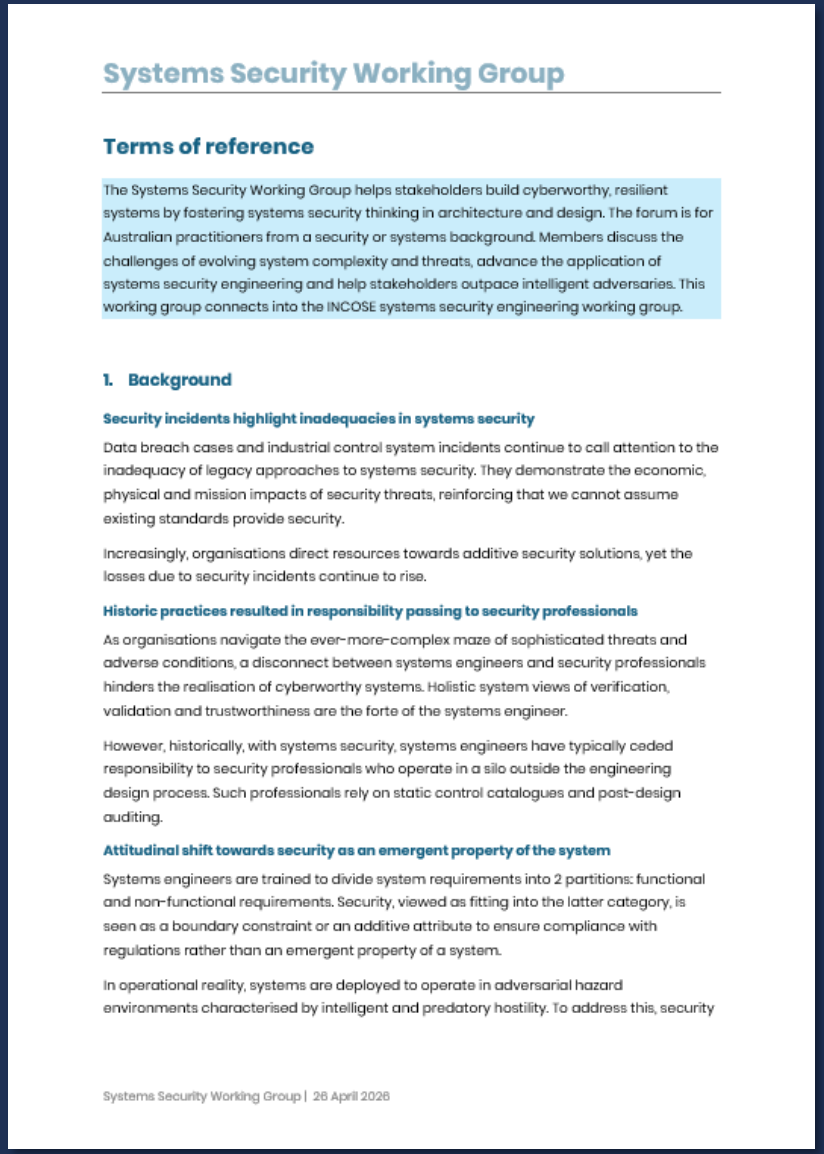
Working Together?

Professional Exchange in Aus

- Currently, there appears to be no dedicated forum for professional exchange in Australia for anyone approaching security through an engineering lens.
- We are in the process of looking at the establishment of a working group on Systems Security.

Context Driving This Proposal:

- Additive security and post-design audits are now less effective.
- Isolating security professionals from the core engineering design process leaves systems vulnerable and security unable to demonstrate the reduction of functional risk.
- Security should be designed into systems from the start and be delivered as an emergent property, not treated as just compliance.
- There is value in a forum for exchange to overcome the language barrier (capability/performance vs. compliance/risk) and successfully integrate methodologies.



Systems Security Working Group

Terms of reference

The Systems Security Working Group helps stakeholders build cyberworthy, resilient systems by fostering systems security thinking in architecture and design. The forum is for Australian practitioners from a security or systems background. Members discuss the challenges of evolving system complexity and threats, advance the application of systems security engineering and help stakeholders outpace intelligent adversaries. This working group connects into the INCOSE systems security engineering working group.

1. Background

Security incidents highlight inadequacies in systems security

Data breach cases and industrial control system incidents continue to call attention to the inadequacy of legacy approaches to systems security. They demonstrate the economic, physical and mission impacts of security threats, reinforcing that we cannot assume existing standards provide security.

Increasingly, organisations direct resources towards additive security solutions, yet the losses due to security incidents continue to rise.

Historic practices resulted in responsibility passing to security professionals

As organisations navigate the ever-more-complex maze of sophisticated threats and adverse conditions, a disconnect between systems engineers and security professionals hinders the realisation of cyberworthy systems. Holistic system views of verification, validation and trustworthiness are the forte of the systems engineer.

However, historically, with systems security, systems engineers have typically ceded responsibility to security professionals who operate in a silo outside the engineering design process. Such professionals rely on static control catalogues and post-design auditing.

Attitudinal shift towards security as an emergent property of the system

Systems engineers are trained to divide system requirements into 2 partitions: functional and non-functional requirements. Security, viewed as fitting into the latter category, is seen as a boundary constraint or an additive attribute to ensure compliance with regulations rather than an emergent property of a system.

In operational reality, systems are deployed to operate in adversarial hazard environments characterised by intelligent and predatory hostility. To address this, security

Systems Security Working Group | 26 April 2026

ANSTO

Thank You!