Defensive Cyber Security Architecture and Impact on Gen. IV Reactors

Dr. Rick Bodner

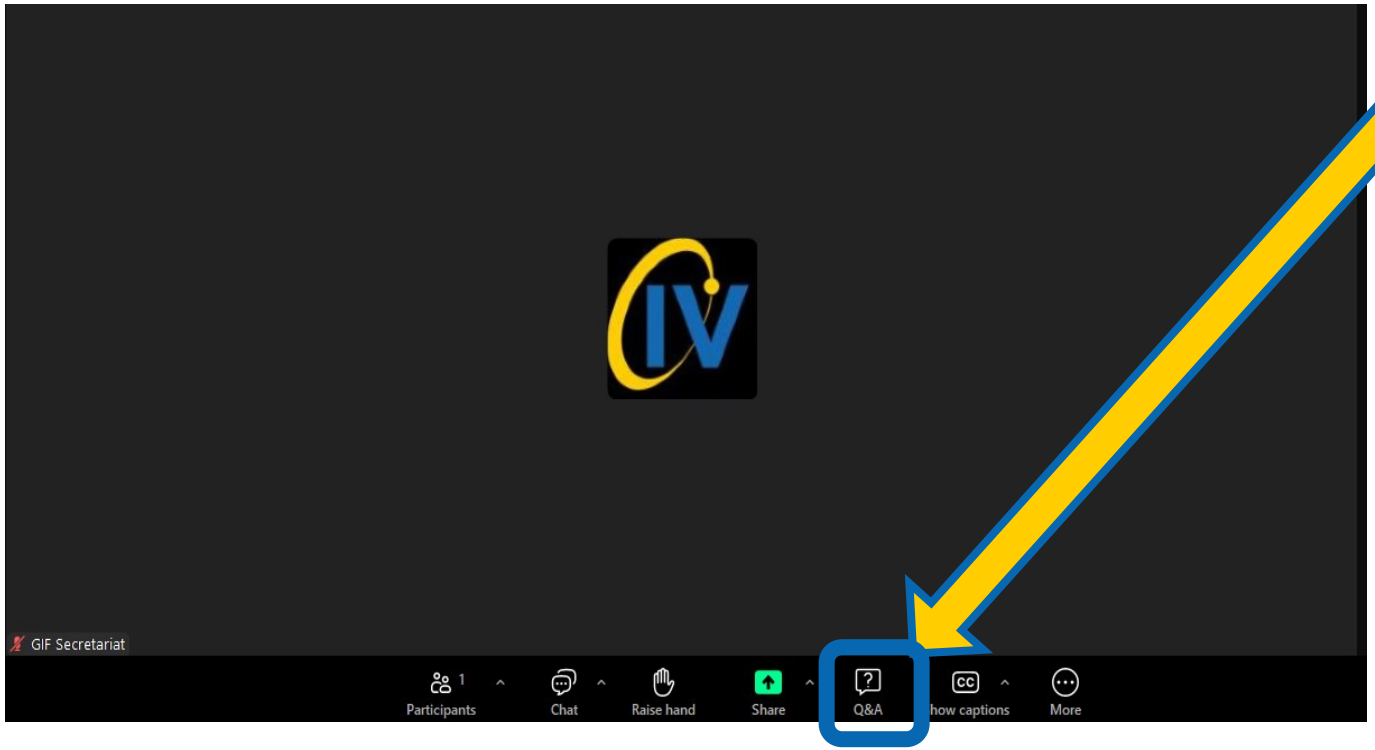
22 June 2026
GIF Education and Training Webinar 112

Some Housekeeping Items

Listen through your computer	Please select the “use computer audio” option and check that your speakers/headphones are not muted.
Technical Difficulties	Search the Zoom Webinars Support https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0064143
To ask a question	Select the “Q&A” pane on your screen and type in your question
Share with others or watch it again	A video/audio recording of the webinar and the slide deck will be made available at www.gen-4.org
Please take the survey	A brief online survey will follow the webinar.

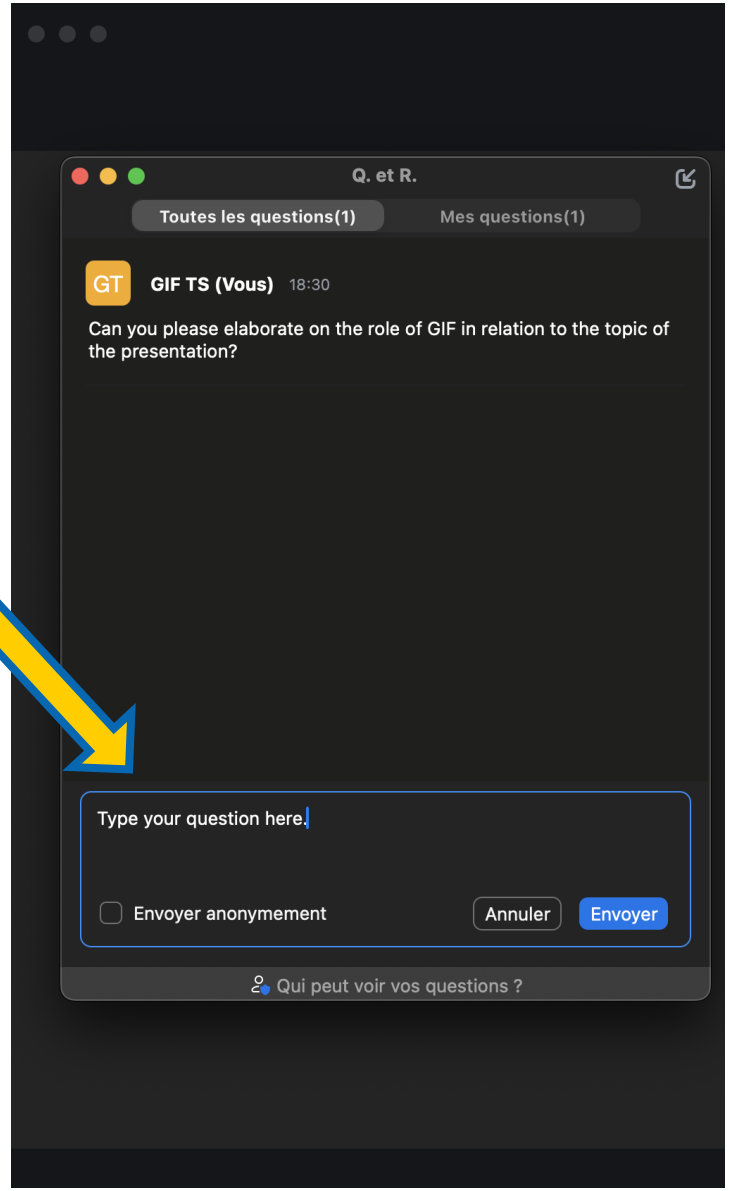
GEN IV International Forum

To Ask a Question – Use the Q&A function



Click the Q&A buton in the zoom menu.

You will then see a window that will allow you to type your question.



25 YEAR ANNIVERSARY GEN IV INTERNATIONAL FORUM
Expertise | Collaboration | Excellence

Defensive Cyber Security Architecture and Impact on Gen. IV Reactors

Dr. Rick Bodner

22 June 2026
GIF Education and Training Webinar 112

Meet the Presenter

Rick Bodner is a Cyber Security Research Specialist in the Cyber Resiliency Branch at Canadian Nuclear Laboratories (CNL), whose work has focused on supporting systems important to safety and other complex systems across the nuclear, aerospace, and defense sectors. His research and professional focus lie at the intersection of cyber security, human factors, and complex information systems, informed by academic training and applied research. His work spans software and systems development, the application of quality standards in the design of systems, and the application of standards and regulatory guides covering such aspects as cyber security for industrial control systems, digital hazards, human factors, supervisory control, and computer-based procedures.

Rick was a key contributor to the design of a control-centre plant display system for a Generation III reactor. At CNL, he examines how cyber security considerations influence digital system design, functionality, and regulatory compliance, with the goal of strengthening the cyber resilience of operational technology (OT) in nuclear and other critical infrastructure environments.

Rick earned his PhD in Industrial Engineering at the University of Toronto in Toronto, Ontario, Canada in 2004.

Email: rick.bodner@cnl.ca

Introduction

- Generation IV advanced reactors (e.g., micro-reactors) will depend extensively on digital I&C, automation, and remote operational concepts

  ➡ **This increases the coupling between nuclear safety concepts and cyber security**

- Cyber resiliency must therefore be addressed across the full facility lifecycle: **design**, **implementation**, **operation**, **maintenance**, and **decommissioning**
- A security-by-design approach treats cyber security as a core engineering consideration
- A defensive cyber security architecture (DCSA) helps preserve safety assumptions as systems become more digitally integrated and operationally autonomous

Outline

1 - Why conventional Operation Technology (OT) cyber approaches are not sufficient for Gen IV advanced reactors

2 - How safety principles inform DCSA design

3 - Core DCSA design activities and architectural concepts

4 - How early I&C and safety decisions shape later cyber implementation

5 - Design implications mapped to the NIST CSF functions

6 - Key takeaways for early Generation IV reactor design activities

Why Advanced Reactor Designs Change the Cyber-Safety Relationship

IT Environment

- Confidentiality is often the leading concern
- Frequent upgrades and user interaction are expected
- Outages and component refreshes are generally manageable
- Pervasive online monitoring and diagnostics through end-point oversight
- Bursty network traffic and component connections

OT Environment

- Availability and process integrity are usually paramount
- Systems often have long lifetimes and limited maintenance windows
- Upgrades may be constrained by safety, qualification, and licensing requirements
- Limited online monitoring, especially legacy / isolated systems
- Greater automation and lower tolerance for disruption change what security controls are acceptable

Nuclear OT Security is Different from IT Security

In nuclear facilities, safety, availability, determinism, and licensing constraints shape what cyber security measures are practical.

Deterministic timing

↓

impacts selection of security control such that it does not introduce unacceptable latency or jitter

Long asset lifetimes

↓

means patch-centric security models are insufficient

Safety-qualified hardware/software

↓

updates may require extensive justification and revalidation

Fail-safe design basis

↓

for security functions favours integrity or availability over confidentiality

Cyber security must be considered throughout the full plant lifecycle

OT Threat Evolution: Why Architecture Matters

OT malware

Single-site, single vendor targeting

has evolved

Key lessons from major OT incidents include:

- Attackers can manipulate process behaviour while appearing normal
- Legitimate industrial protocols can be abused for malicious purposes
- Safety-related systems can be directly targeted
- Multi-protocol and multi-vendor attacks are becoming more common

OT Threat Evolution: Why Architecture Matters

OT malware

Single-site, single vendor targeting

has evolved

Design implication:

Defense-in-depth is a main safety design consideration, and a cyber security architecture helps to ensure defensive-in-depth cannot be defeated

Cyber resilience cannot rely only on detection or patching; it must be engineered into architecture to bolster defenses

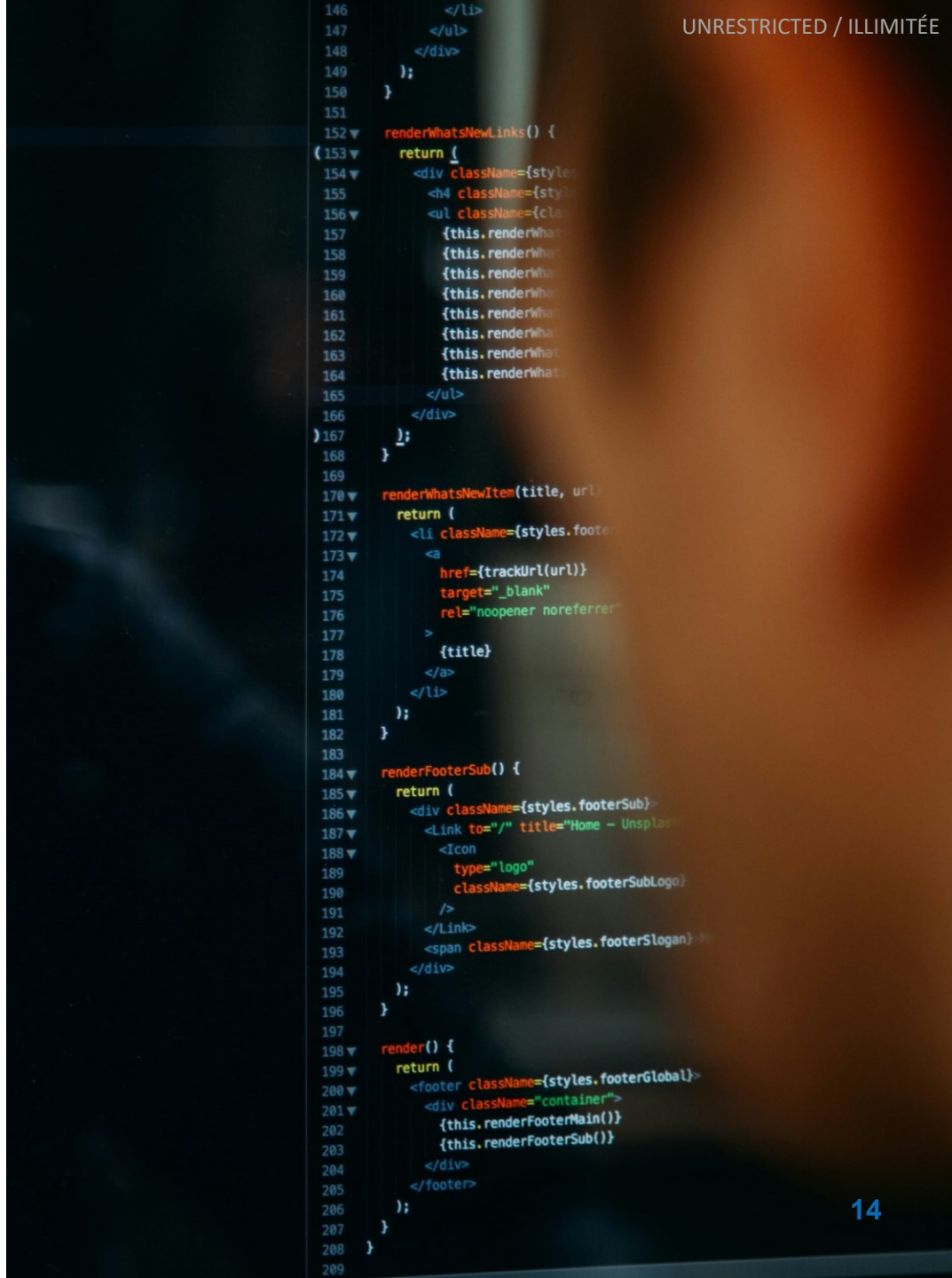
Why Gen IV Advanced Reactor Designs Changes Safety-Cyber Coupling

- Extensive digital I&C and software-based automation
- Reduced on-site staffing and increased remote operations
- Remote or non-traditional siting
- Factory fabrication and modular development
- Novel safety concepts, including passive and inherent safety features

These characteristics increase dependence on digital systems that may be safety-significant, indirectly cyber-reachable, and harder to access for response or recovery.

Why Traditional OT Security Models Are Not Sufficient

- Traditional nuclear OT models assume larger on-site staff and easier physical intervention
- SMR and microreactor concepts may rely on minimal staffing, remote operations, and limited maintenance access
- Conventional assumptions about recovery, maintenance, and incident response may not hold
- In advanced reactors, cyber resilience must be designed in early rather than applied operationally later

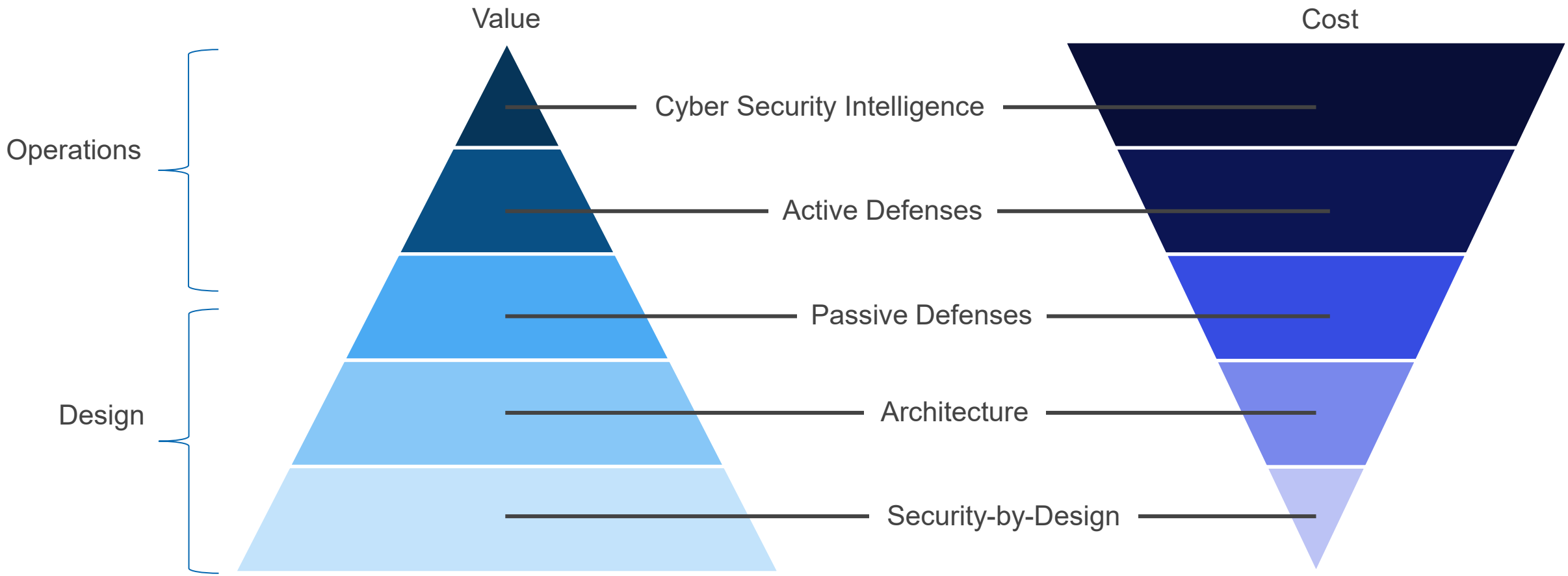


Safety Design Principles as the Foundation of DCSA

Security-by-Design for Advanced Reactor Facilities

- Security-by-design means incorporating cyber security requirements during system design, not after deployment
- In nuclear applications, cyber security measures must be integrated with safety requirements rather than treated separately
- Defense-in-depth, graded protections, and clear architectural boundaries are core design concepts
- A defensive cyber security architecture (DCSA) is a key mechanism for implementing security-by-design
- The objective is to preserve safety assumptions as systems become more digitally integrated and operationally autonomous

Cyber Security Value / Cost



Focusing on the bottom layers, Security-by-Design and Architecture, creates a massive "value" footprint. If these are weak, the top layers must work much harder (and potentially cost much more) to compensate.

Core DCSA Design Activities

1. Identify digital assets and assign significance

Determine which digital assets are cyber essential and how their significance relates to safety, security, and operational functions.

2. Establish zones and define interfaces

Group assets into zones based on significance, function, and dependency, then define all inter-zonal interfaces.

3. Apply boundary protection

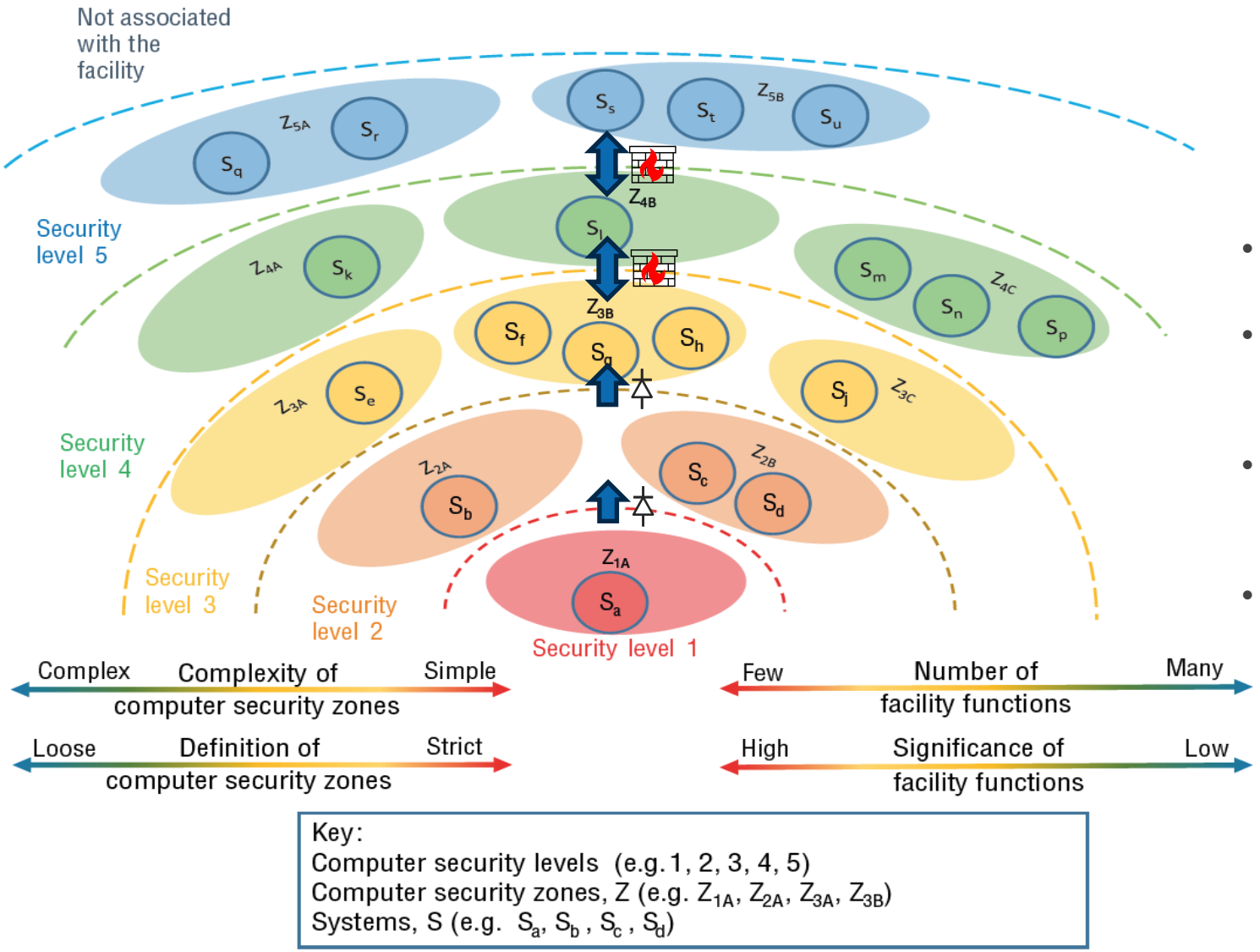
Protect interfaces according to the significance of the higher-value zone.

4. Enable monitoring

Monitor critical communications, boundary crossings, and device integrity in a way that supports safe operation.

Together, these activities organize digital assets into zones, define protected interfaces, constrain attack pathways, and establish layered protection.

Conceptual DCSA: Functions, Levels, Zones, Systems



- Significance-informed zones
- Controlled conduits and interfaces
- Boundary protection aligned to higher consequence functions
- Monitoring and management outside of safety-critical paths

Figure modified from IAEA NSS 17-T, Computer Security Techniques for Nuclear Facilities

Why I&C Safety Design and DCSA Must Be Co-Designed

- I&C architecture establishes how plant functions are implemented across systems and components
- Safety design already addresses reliability, independence, separation, and common-cause concerns
- A DCSA must preserve those same properties against cyber compromise
- In smaller or more integrated reactor designs, architectural consolidation can create new common-cause cyber pathways, if not designed appropriately
- DCSA design is not separate from I&C design; it is part of preserving the safety intent

Safety Design Principles that Inform DCSA

Defense-in-depth	Diversity	Independence	Separation
No single failure or compromise should defeat safety-significant functions	Use different technologies, platforms, design teams, etc. to reduce common-cause failure and shared exploitability	Ensure one system or channels cannot impair another through functional, electrical, logical, or management dependencies	Maintain separation between systems or channels so that faults or compromises do not propagate across safety boundaries

In cyber terms, these principles translate into zoning, controlled interfaces, layered protection, and diverse enforcement mechanisms

Security Zoning and Diversity Reduce Common-Cause Cyber Risk

- Safety-significant systems must be protected against interference from non-safety systems
- In cyber security terms, this requires meaningful isolation between zones, not only logical groupings
- Zoning constrains attack pathways and prevents compromise from propagating across boundaries
- Diversity reduces shared exploitability across channels, zones, or platforms
- Integrated vendor platforms should be examined for hidden concentrations of cyber risk

How DCSA Activities Support I&C Safety Design Principles

I&C Architecture Safety Design Principles				
DCSA Design Activities	**Defense-in-depth**	**Diversity**	**Independence**	**Separation**
Identify critical digital assets and assign significance	Determines where layered protection is required	Informs platform and software diversity decisions	Informs grouping needed to preserve independence	Informs grouping needed to preserve separation
Establish zones and interfaces	Creates architectural layers and constrains attack pathways	Reveals shared dependencies and diversity gaps	Defines interfaces that preserve functional independence	Defines boundaries that preserve architectural separation
Boundary protection	Adds protective layers zone boundaries	Applies diverse protections to reduce shared exposure	Prevents cross-zone impairment and unintended influence	Enforces separation between zones and security levels
Monitoring	Provides detection to support layered defense and early containment	Avoids monitoring dependencies that create shared exposure	Preserves independence by avoiding monitoring-induced dependencies	Preserves separation by avoiding monitoring pathways that erode boundaries

Design Considerations Mapped to the NIST CSF Functions

Using the NIST CSF as a Communication Framework

The NIST Cybersecurity Framework (CSF 2.0) functions provide a useful organizing structure:

- **GOVERN** – establish expectations, roles, and risk management direction
- **IDENTIFY** – understand critical assets, dependencies, and data flows
- **PROTECT** – implement measures that reduce likelihood and impact
- **DETECT** – monitor for adverse events and assess significance
- **RESPOND** – contain and manage cyber events
- **RECOVER** – restore capability in a controlled and predictable way

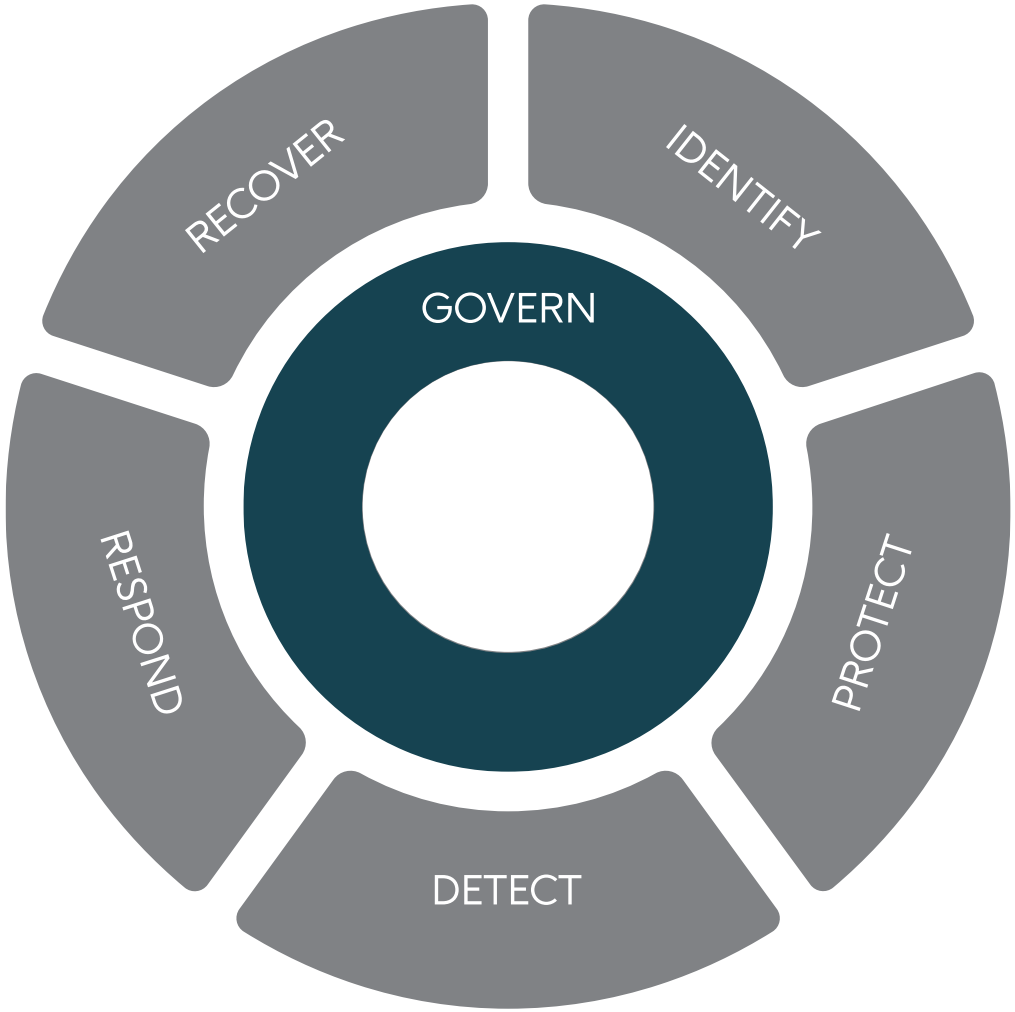
For nuclear applications, the CSF is most useful when interpreted through safety, design, and lifecycle constraints.

DCSA Activities Mapped to Safety Principles and CSF Functions

DCSA Design Activity	Safety Design Principles	Primary CSF Function
Identify critical digital assets and assign significance	Independence, separation	Identify
Establish zones and interfaces	Independence, separation	Identify / Protect
Boundary protection	Independence, separation	Protect
Monitoring	Independence, separation, operational assurance	Detect

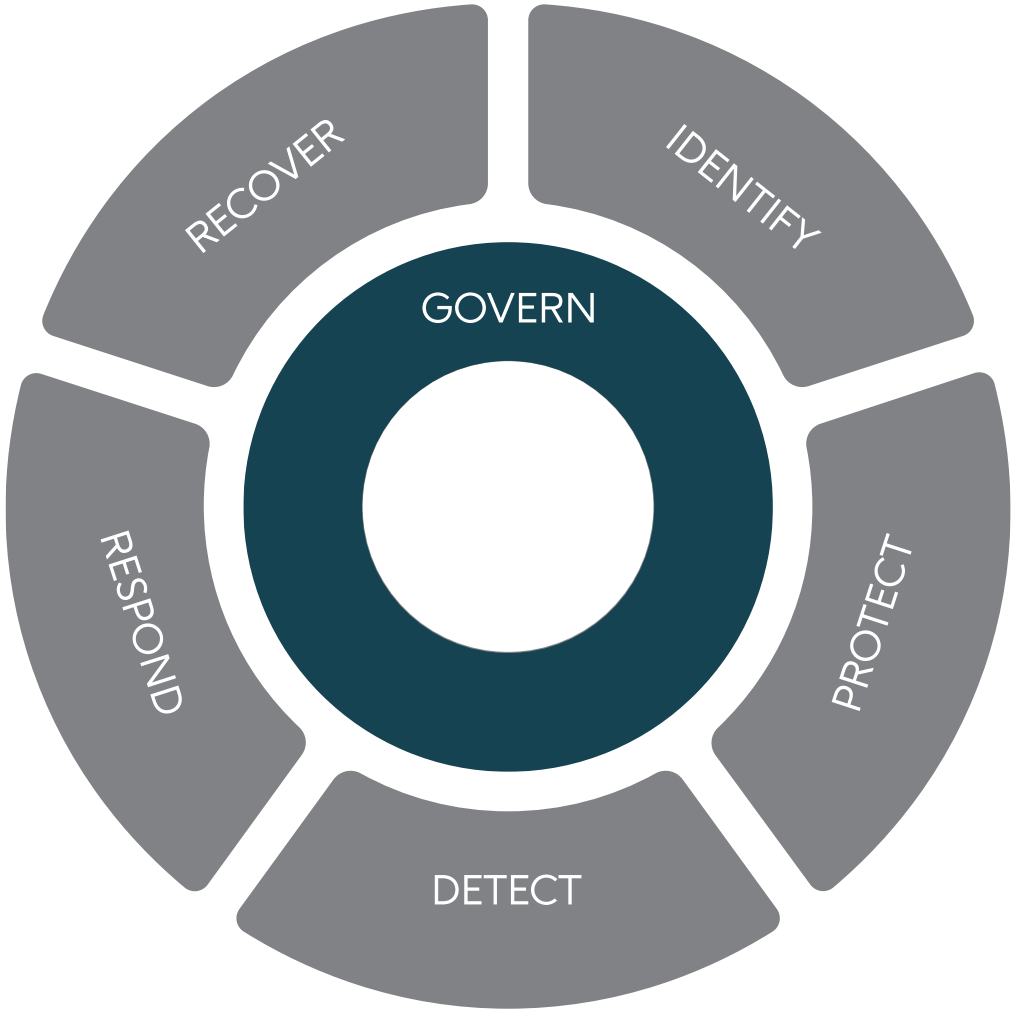
GOVERN: Governance as a Design Enabler

- Governance defines how cyber risk is owned, prioritized, and integrated into the project
- Cyber governance should align with the licensing basis, management system, and lifecycle controls
- Governance is also where roles, responsibilities, and accountability for digital assets are defined
- Supply-chain governance is particularly important for long-lived digital systems and remote support models



GOVERN: Special Challenges for SMR/MMR Deployments

- Multi-site fleets may share common digital designs and therefore common cyber exposures
- Vendor-managed or highly integrated digital platforms can complicate accountability
- Responsibility may be distributed across designer, supplier, integrator, and operator
- These conditions increase the importance of governance for configuration control, support access, and supply-chain oversight



IDENTIFY: Digital Dependencies and Deployment-Driven Risk

- Begin with functions important to nuclear safety, nuclear security, emergency preparedness, and safeguards
- Then identify the digital assets and dependencies that support those functions
- In integrated platforms, dependency mapping is often more useful than a simple asset list
- The output should support significance assignment, zoning, and interface definition

IDENTIFY: Risk Assessment for Remote and Small-Staffed Reactors

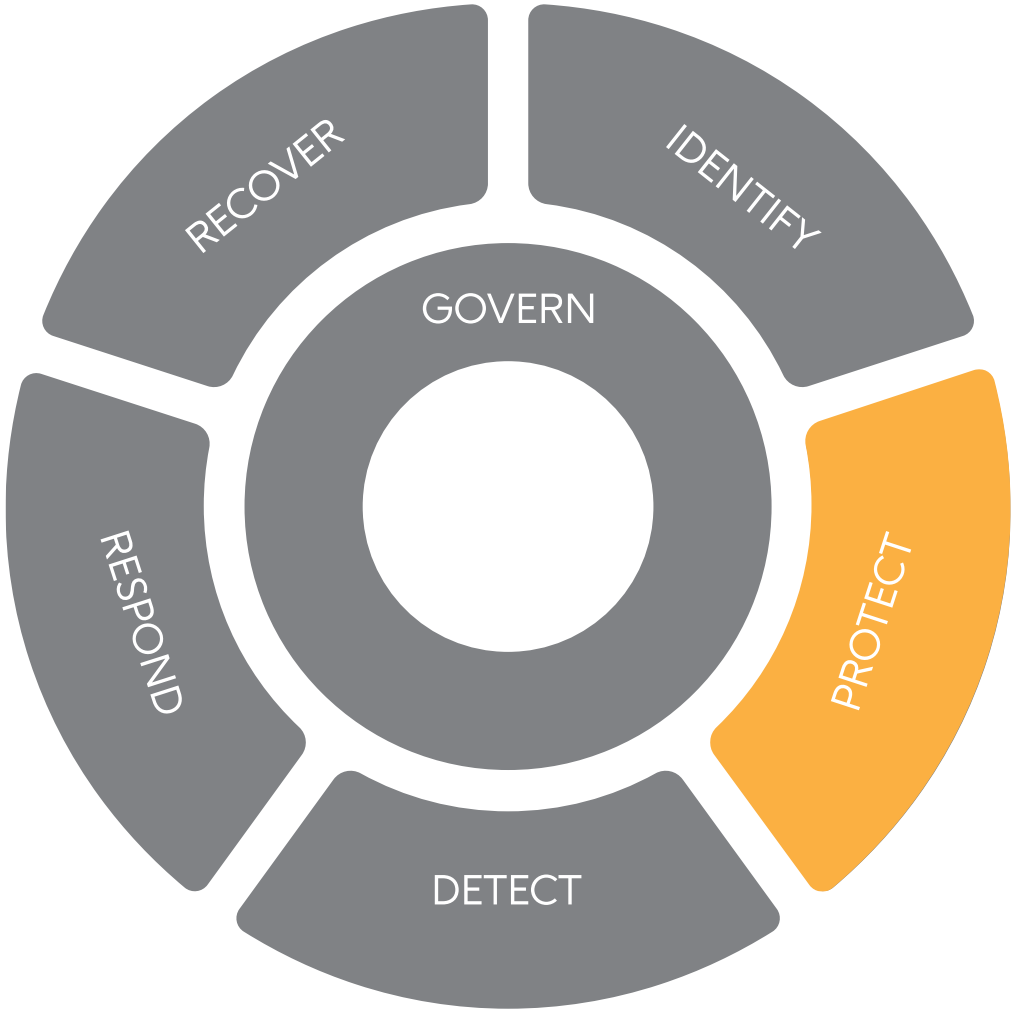
- Risk assessment should account for design conditions such as:
  - remote operation,
  - harsh or inaccessible deployment environments,
  - delayed detection of abnormal conditions,
  - delayed human response, and
  - limited recovery options

Key point:

- Risk identification must reflect intended operating concept, not only nominal plant topology

PROTECT: Early I&C Design Choices Determine DCSA Effectiveness

- Cyber architecture decisions are also reactor design decisions
- Zones should align with safety-relevant functional boundaries, not vendor product boundaries alone
- Conduits should be minimal, deterministic, and verifiable
- DCSA should be co-developed alongside preliminary I&C architecture, safety functional allocation, and hazard analysis
- Late-stage cyber controls increase licensing burden, create fragile workarounds, and may be harder to sustain in remote or low-staffed deployments

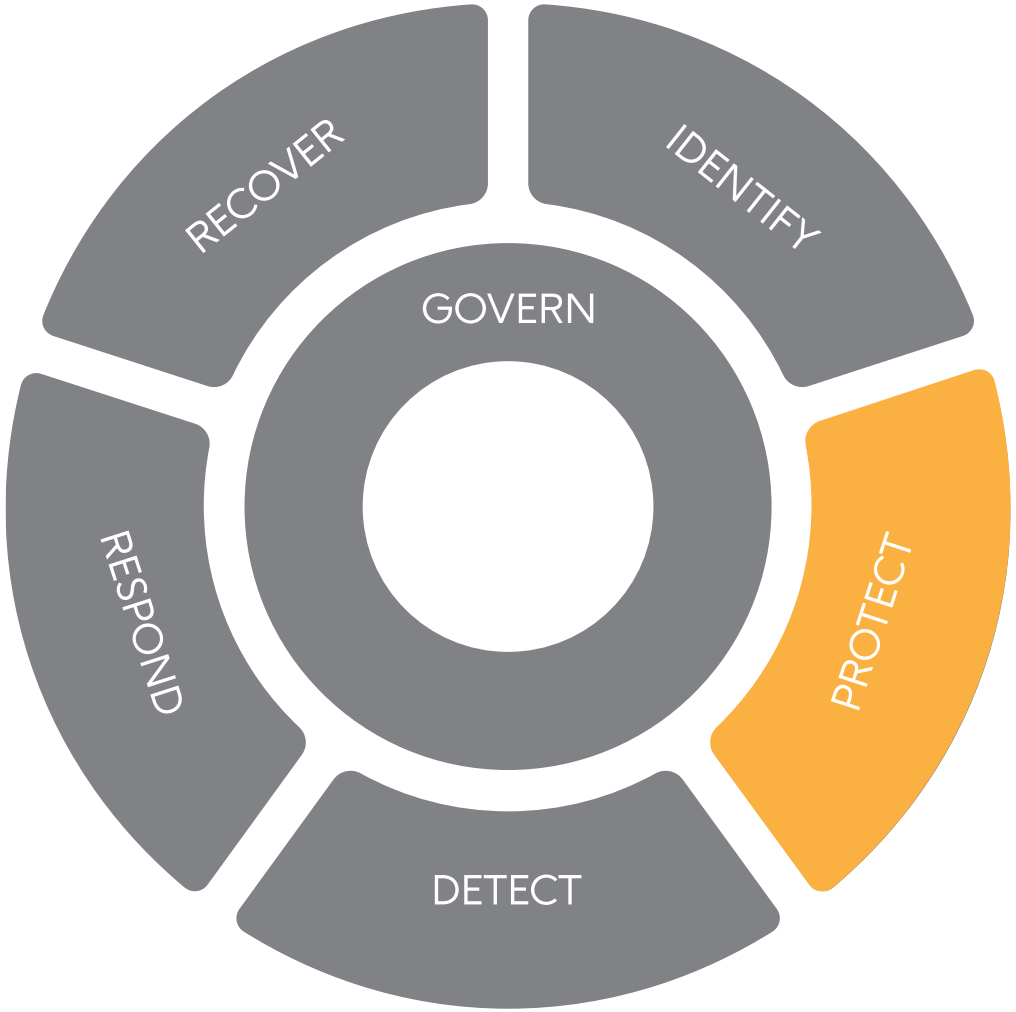


PROTECT: Boundary Protection

- Higher-significance zones require tightly constrained, deterministic, and fail-secure communications
- Unidirectional transfer should be used where mission and design permit
- Protective devices should be assigned and managed according to the higher-consequence side of the boundary

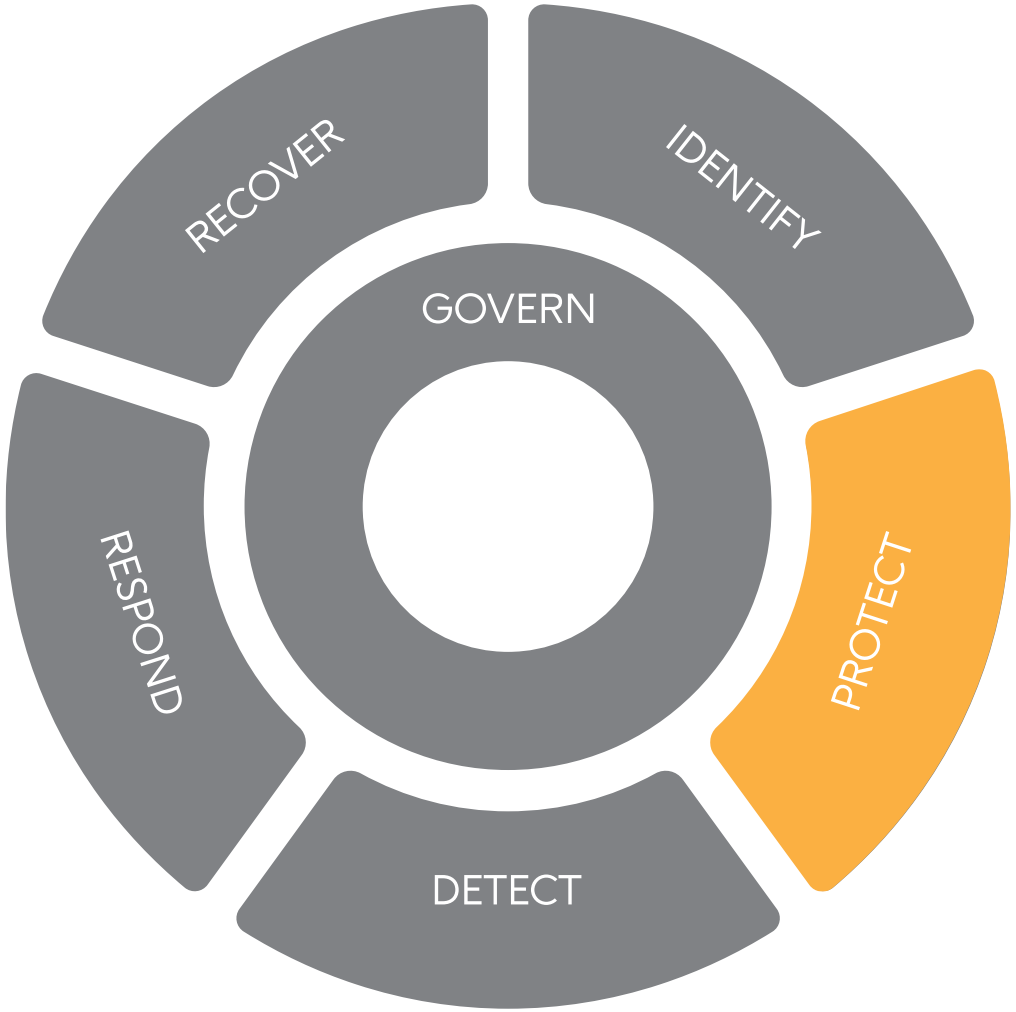
Key point:

- Where automation exists, the architecture must still prevent compromise from propagating into higher-significance functions



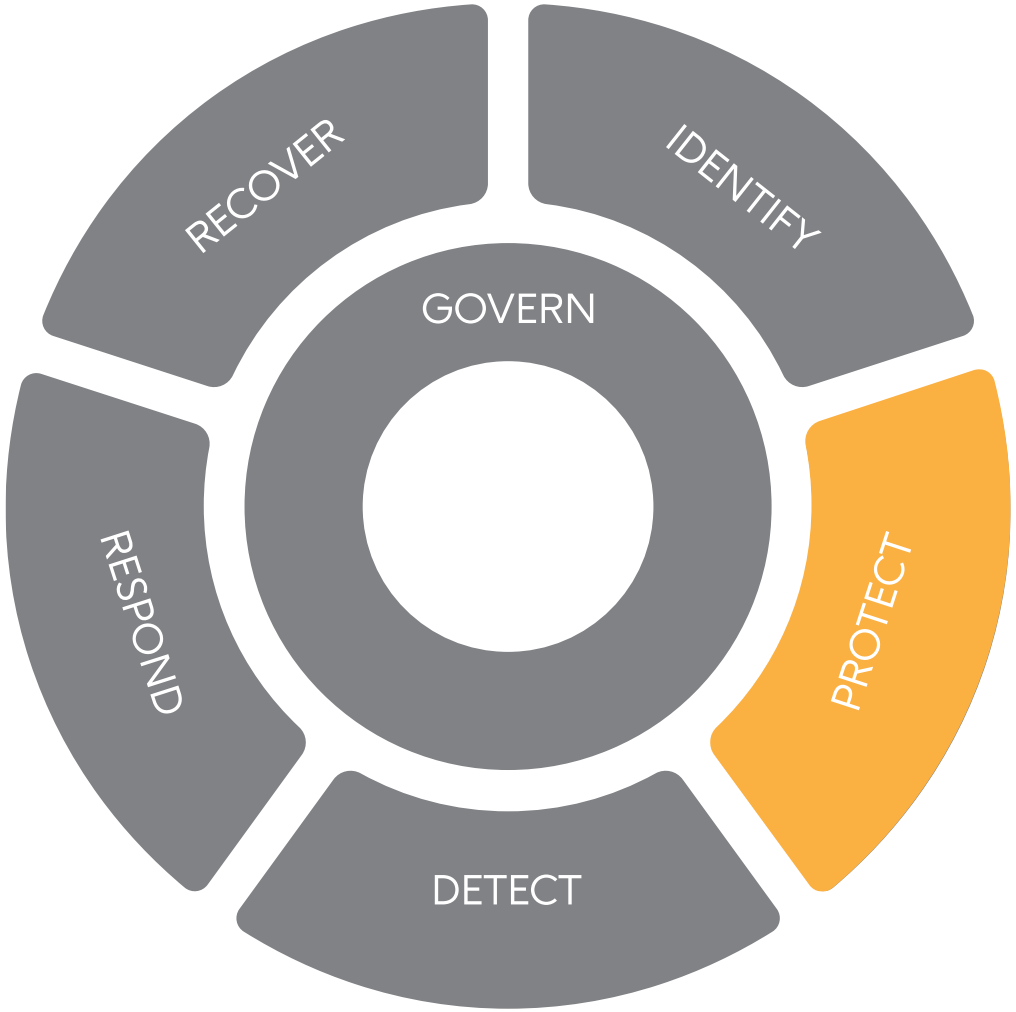
PROTECT: Align Logical and Physical Boundaries

- Cyber boundaries are stronger when they align with physical layout, enclosures, and cable routing
- High-significance zones should have tightly coupled logical and physical protections
- Unused interfaces should be disabled or removed where practical
- Any inter-zonal communication that traverses less trusted areas must be secured and justified
- In compact reactor designs, physical layout decisions and cyber zoning decisions are often



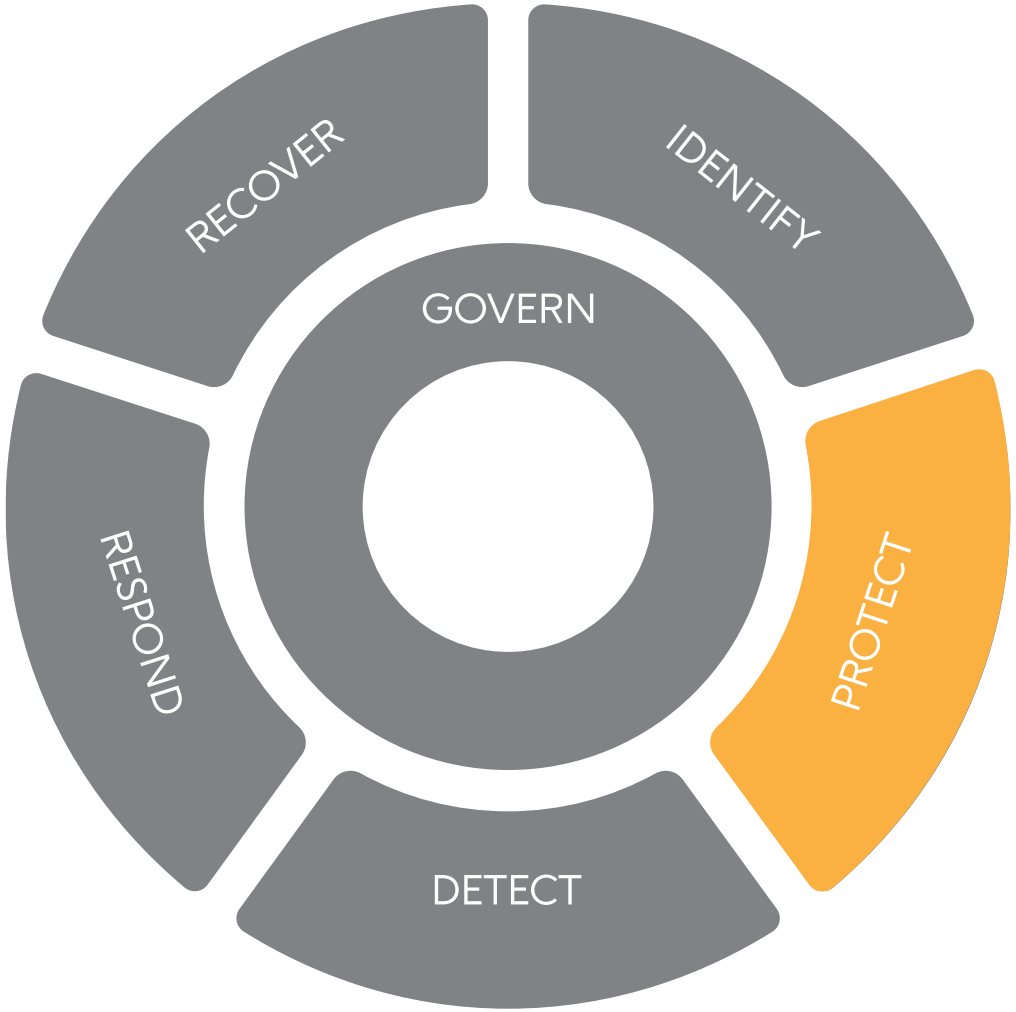
PROTECT: Security Controls Must Preserve Safety Performance

- Cyber security measures must not adversely affect safety-significant functions or performance
- Where practical, avoid embedding complex security mechanisms directly into safety systems
- Security measures should not impair operator awareness, required control actions, or deterministic behavior
- The preferred outcome is improved resilience without compromising safety claims



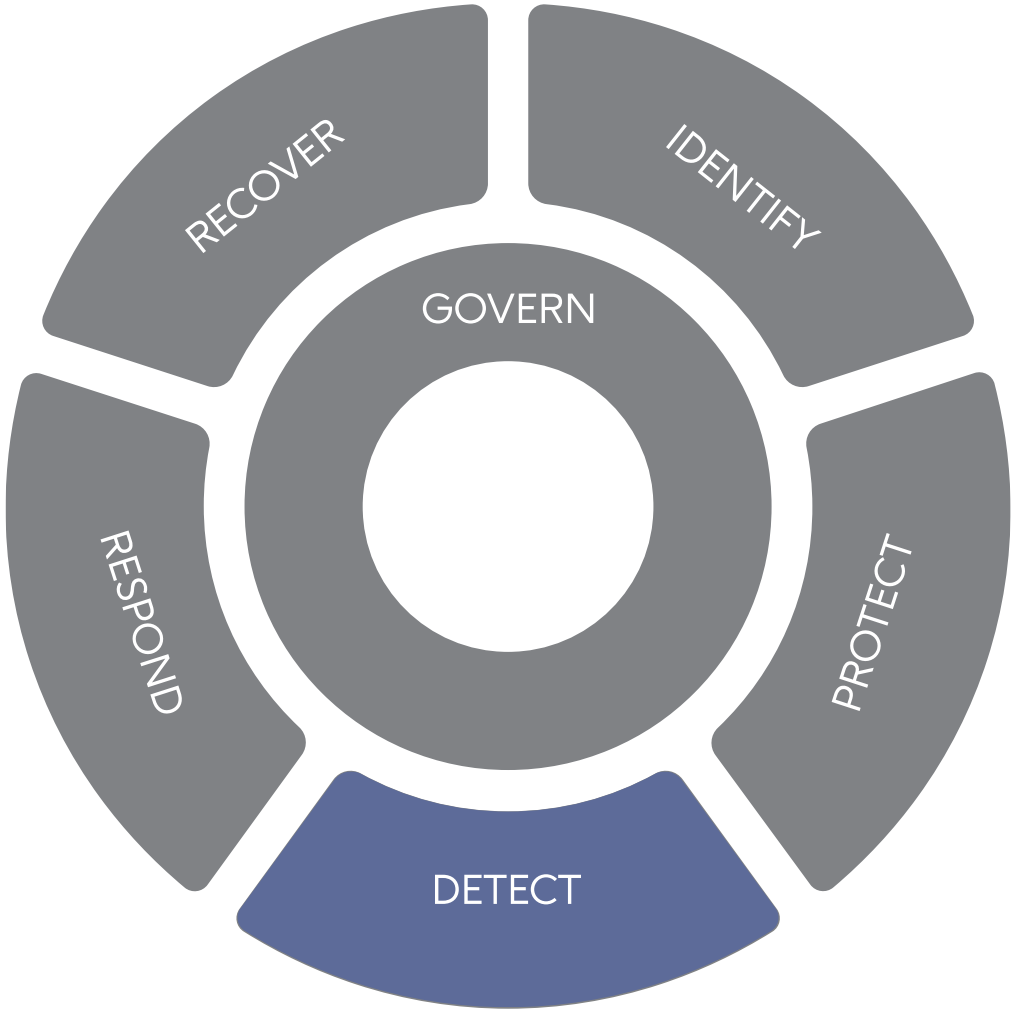
PROTECT: Remote and Wireless Access Requires Strict Treatment

- Remote access should not be permitted to high- or moderate-significance critical digital assets unless a case-specific justification exists and risk is controlled
- Wireless access should be prohibited for higher-significance critical digital assets
- Any use of wireless for lower-significance assets should be justified using a graded approach
- For remote operations concepts, off-site control or monitoring facilities should be treated as part of the overall DCSA
  - Difference between remote operations as an operating concept and remote access as an architectural pathway



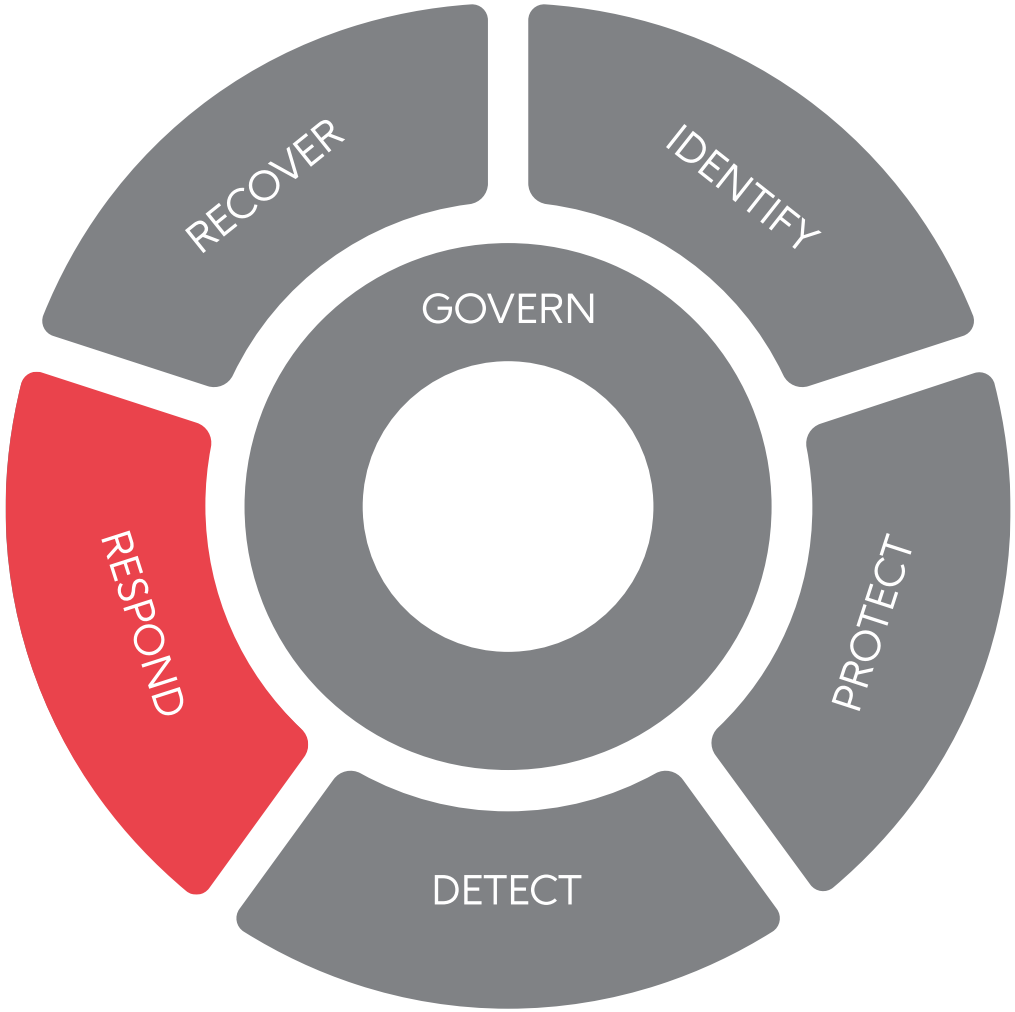
DETECT: Monitoring Must Respect Safety Constraints

- Safety systems often cannot host traditional IT monitoring agents or active inspection tools
- Poor observability is often a design problem created by weakly defined interfaces
- A practical approach is to monitor conduits, gateways, and deterministic communications rather than safety assets directly
- Centralized monitoring can effectively support detection if strong isolation is maintained
- Monitoring design should be established early so that observability is not lost by default



RESPOND: Prioritize Containment and Safety Preservation

- In remote or low-staffed reactor concepts, immediate human intervention may not be available
- Therefore, response should emphasize architectural containment rather than rapid manual eradication
- DCSA can support response by isolating affected zones, limiting lateral movement, and preserving deterministic safety behavior
- The response objective is first to prevent safety impact, then to support recovery and remediation



RECOVER: Is a Design Outcome

- Recovery should be treated as an architectural outcome, not only a procedural activity
- Remote and small-staffed deployments may have limited maintenance access and delayed restoration options
- Safety-aligned DCSA design can support recovery through known-good baselines, deterministic restoration paths, and constrained revalidation scope
- Early I&C and cyber design choices directly affect time to restore and confidence in restored operation

Conclusions

Key Takeaways

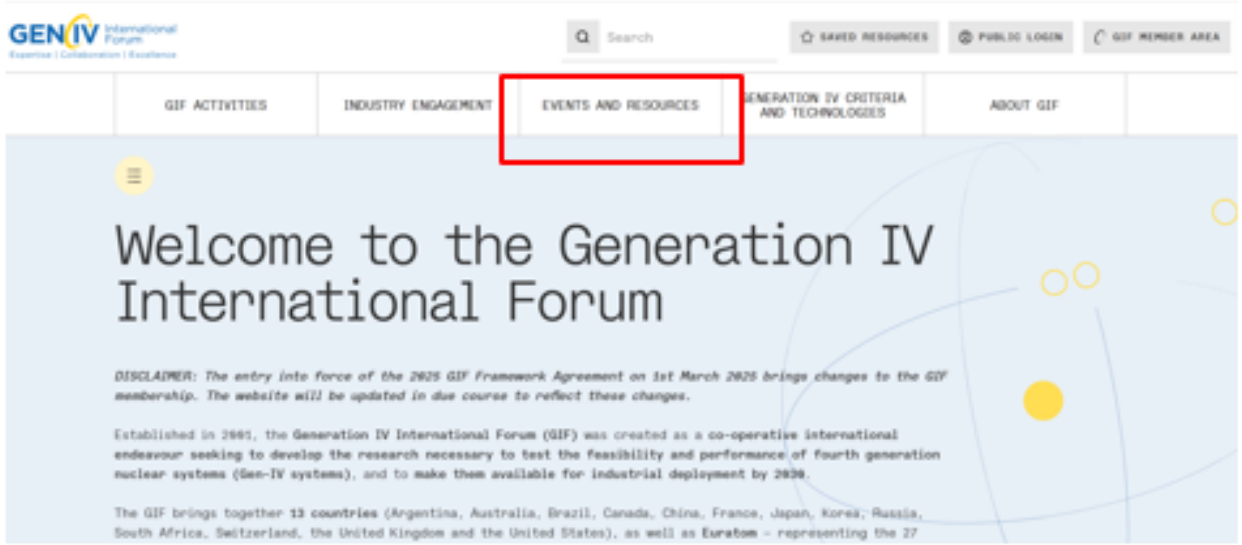
- Generation IV reactor designs should employ a security-by-design methodology and focus on the architecture
- Increased digital dependence of advanced reactors strengthens the coupling between nuclear safety and cyber security
- Defense-in-depth, diversity, independence, and separation are shared principles across safety and cyber design
- Early I&C and safety design choices enable or limit later cyber implementation, remote operations, remote maintenance, response, and recovery
- DCSA provides a structured means to zone critical digital assets, protect interfaces, constrain attack pathways, and establish layered protection

Upcoming GIF ETWG Webinars

Date	Title	Presenter
8 July 2026	The Wider Role of Nuclear in the Energy System – Engagement and education activities to enable	Mr. Robert Alford, UKNNL, United Kingdom
12 August 2026	Diamonds are a Reactor's Best Friend: Novel Sensor to Investigate High-Valence Actinides in Molten Salts	Dr. Hannah Patenaude, Los Alamos National Laboratory, USA
10 September 2026	Thermal properties of molten salts: crucial data for the development of MSRs	Dr. Juliano Schorne-Pinto, University of South Carolina

How to find the recorded GIF Webinars – www.gen-4.org

1- Click on "Events and Resources Tab

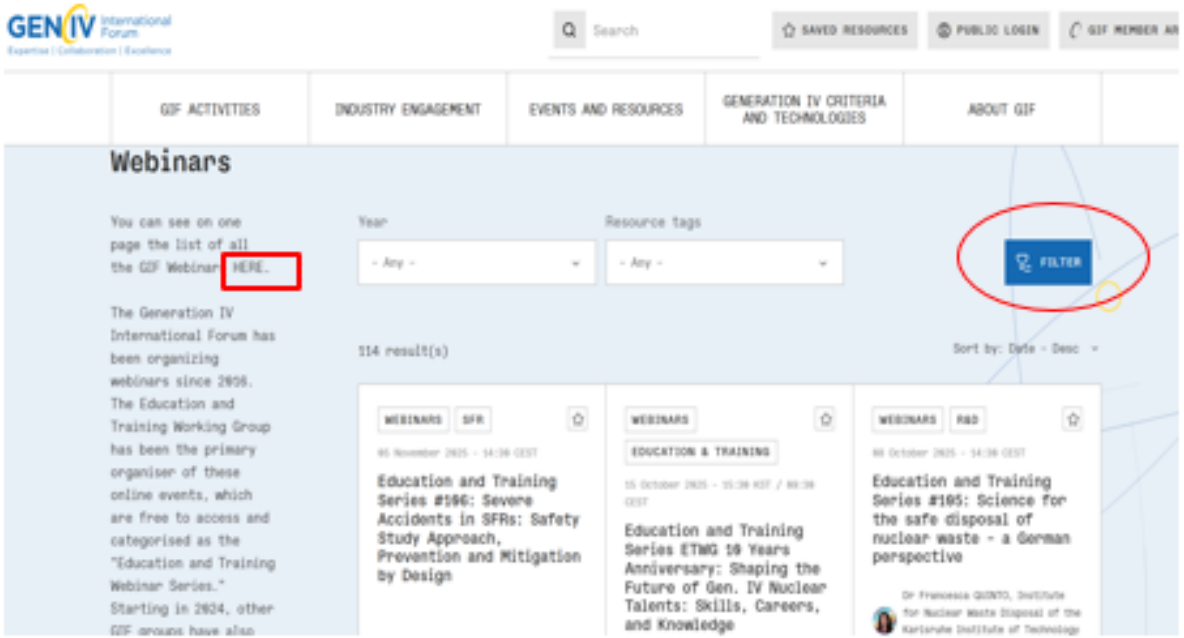


2- Click on "Webinars" tab on the left

3- Click on "HERE" to see all the webinars

Or

4-Use the Year and Resource tag and click on Filter



Thank you!
Questions?

All GIF webinars can be found here: https://www.gen-4.org/list-gif-webinars

A feedback survey will be circulated following this webinar.
Please kindly take the time to fill it to help us improve this series of webinars.