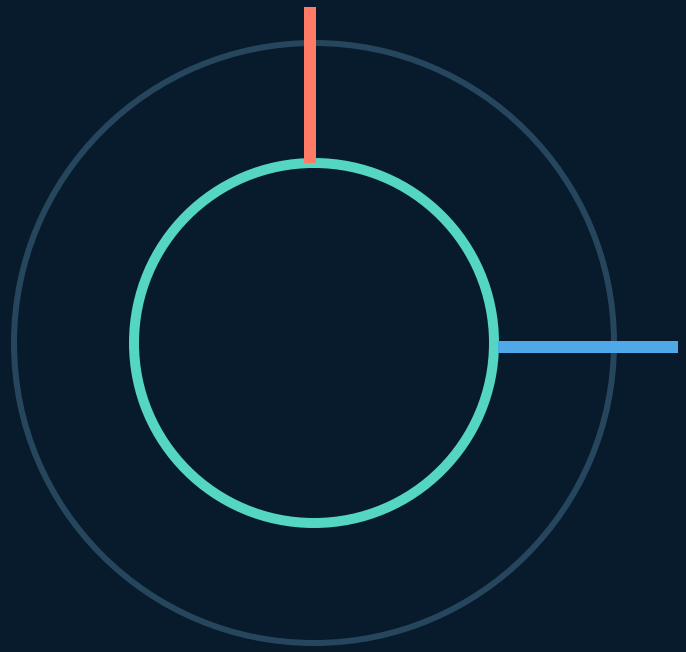
From Hazard Analysis to Controller Engineering



Extending STPA-SEC for secure digital operating environments

Jeff Greer
Assistant Professor of Practice, Cybersecurity
University of North Carolina Wilmington
Copyright 2026

MIT Partnership for Systems Approaches to Safety and Security Workshop
September 24, 2026

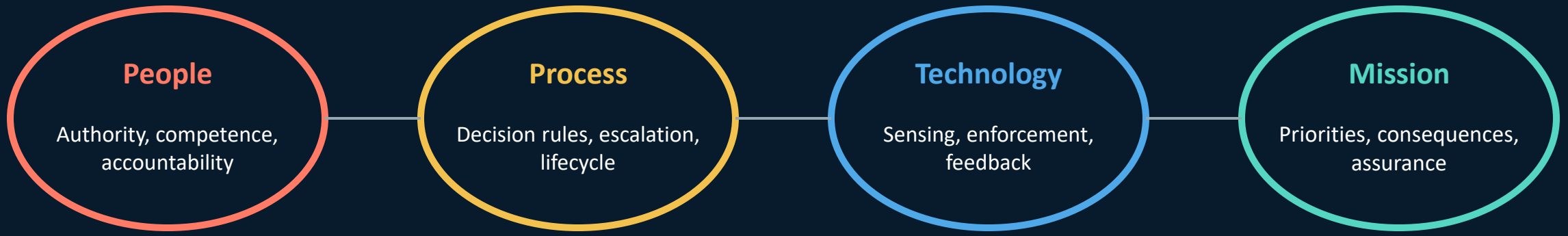
Three research shaping questions

01	**Adoption**	What has inhibited STPA-SEC adoption for enterprise cyber risk management?
02	**Comparative value**	Where does STPA-SEC add value beyond current NIST enterprise risk guidance?
03	**Improvement**	How can STPA-SEC be extended to better support enterprise cybersecurity and continuous mission assurance?

Working finding **The largest opportunity lies in the transition from analysis to engineered control.**

What is a secure enterprise digital operating environment?

A digitally enabled enterprise state in which interacting human, organizational, software, and physical controllers can maintain mission-critical constraints under normal, degraded, and adversarial conditions.



Security becomes a maintained system property tied directly to mission achievement.

Research- straw-man reference models

DIGITAL SHIP		DIGITAL PORT
MISSION Safe and secure vessel operation		**MISSION** Resilient cargo and vessel flow
FUNCTIONS Navigation, propulsion, communications	**SAME METHOD**	**FUNCTIONS** Marine, terminal, gate and intermodal operations
SYSTEMS Bridge, machinery, IT and data services	**DIFFERENT SYSTEMS**	**SYSTEMS** VTS, TOS, cranes, PCS and logistics interfaces
CONTROL Controllers, actions, feedback, constraints		**CONTROL** Controllers, actions, feedback, constraints
PROCESS Vessel movement and machinery state		**PROCESS** Cargo movement and port operating state

COMMON TEST - Can STPA-SEC security constraints become traceable, verifiable controls in both operating environments?

Identified gaps in cyber risk management theory and practice

NIST Guidance

- **Enterprise operating environment:** NIST guidance does not explicitly define a **secure enterprise digital operating environment** as an integrated system-of-systems to be continuously engineered and controlled for mission assurance.
- **Model-based engineering:** NIST provides extensive systems security engineering principles but limited prescriptive guidance for using **model-based engineering to translate cyber risk analysis into executable security architectures and controller designs**.
- **Control selection and traceability:** NIST provides extensive control catalogs and overlays, but lacks a systematic mechanism for **tagging, retrieving, and tracing controls from consequence-driven security requirements to the controllers responsible for enforcing them**.
- **Continuous cyber risk control:** NIST guidance supports continuous monitoring and cyber resilience but does not yet provide an integrated **near-real-time closed-loop cyber risk control architecture** capable of adapting at machine speed to rapidly changing threats and system conditions.

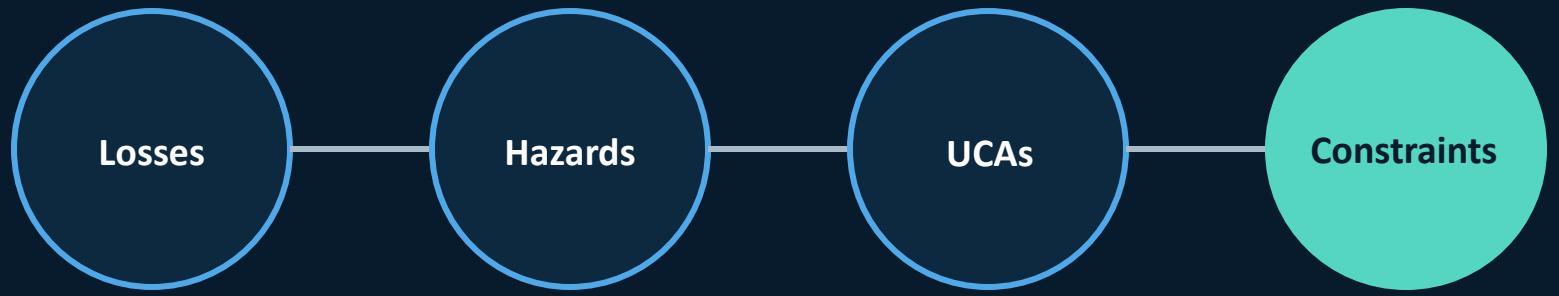
STPA-SEC Theory

- **Controller engineering:** STPA-SEC provides a rigorous basis for deriving security constraints but provides limited guidance for translating those constraints into **implementable, testable, traceable, and continuously monitored controllers and controls**.
- **Loss prioritization:** STPA-SEC identifies unacceptable losses and associated hazards but provides limited guidance for **prioritizing losses and derived security constraints** when resources require risk-based tradeoffs.
- **Risk treatment integration:** STPA-SEC does not explicitly integrate its constraint-derivation process with **enterprise risk-treatment decisions** such as avoid, mitigate, transfer/share, or accept, creating an opportunity for closer alignment with ISO 31000-style risk management.
- **Component-to-system integration:** STPA-SEC emphasizes unsafe or insecure interactions within the control structure; additional methods are needed to systematically connect **component vulnerabilities and failure modes to system-level loss scenarios, constraints, and controller requirements**.

Interpretation **Each of the identified gaps are an opportunity for further research and improvement**

Research area of interest … the transition gap after STPA-SEC analysis

STPA-SEC produces a rigorous account of unacceptable loss and unsafe control.



Open design question

Which controller continuously enforces each constraint?

The method often ends where controller design must begin.

That gap separates hazard analysis from operational mission assurance.

Identified controller engineering improvement opportunities

The controller engineering extension requires **coordinated advances** in people, process, and technology.

People

STPA-SEC project leads need sufficient domain knowledge to model the system of interest and recognize meaningful control flaws.

Reference architectures can be a reusable referent when no named, instantiated system is available.

AI can accelerate domain familiarization and study practice but needs to be used properly.

Process

Define the secure digital enterprise operating environment and provide explicit guidance for managing cyber risk in support of mission achievement.

Model-based methods should address security domain boundaries, digital assets / resources, coupling, dependencies, and priority decisions.

Technology

Develop an integrated control workbook built from NIST SP 800-53, SP 800-82, and SP 800-161.

Use functional metadata to connect controls to controller capabilities, constraints, requirements, and verification evidence.

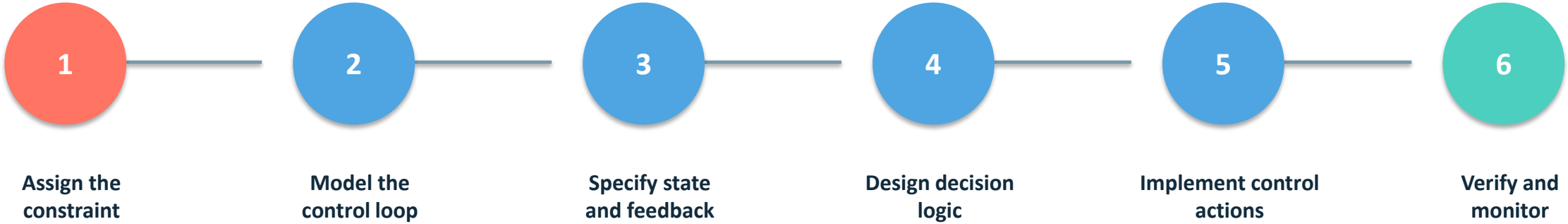
Research focus: turn STPA-SEC outputs into controller designs that are implementable, assessable, and maintainable throughout operations.

People – need to utilize First-Principles Cybersecurity Reasoning

	Specify	Model	Analyze	Synthesize	Engineer
What is it?	System of Interest	•	•	•	•
Why is it important?	Context	•	•	•	•
How does it work?	Functional Decomposition	•	•	•	•
How can it fail?	Failure Type & Propagation	•	•	•	•
How can failure be prevented?	Constraint Req & Controller Eng	•	•	•	•

A "Reasoning Matrix" for validating AI responses and resolving cyber problems

Process for controller engineering design and deployment

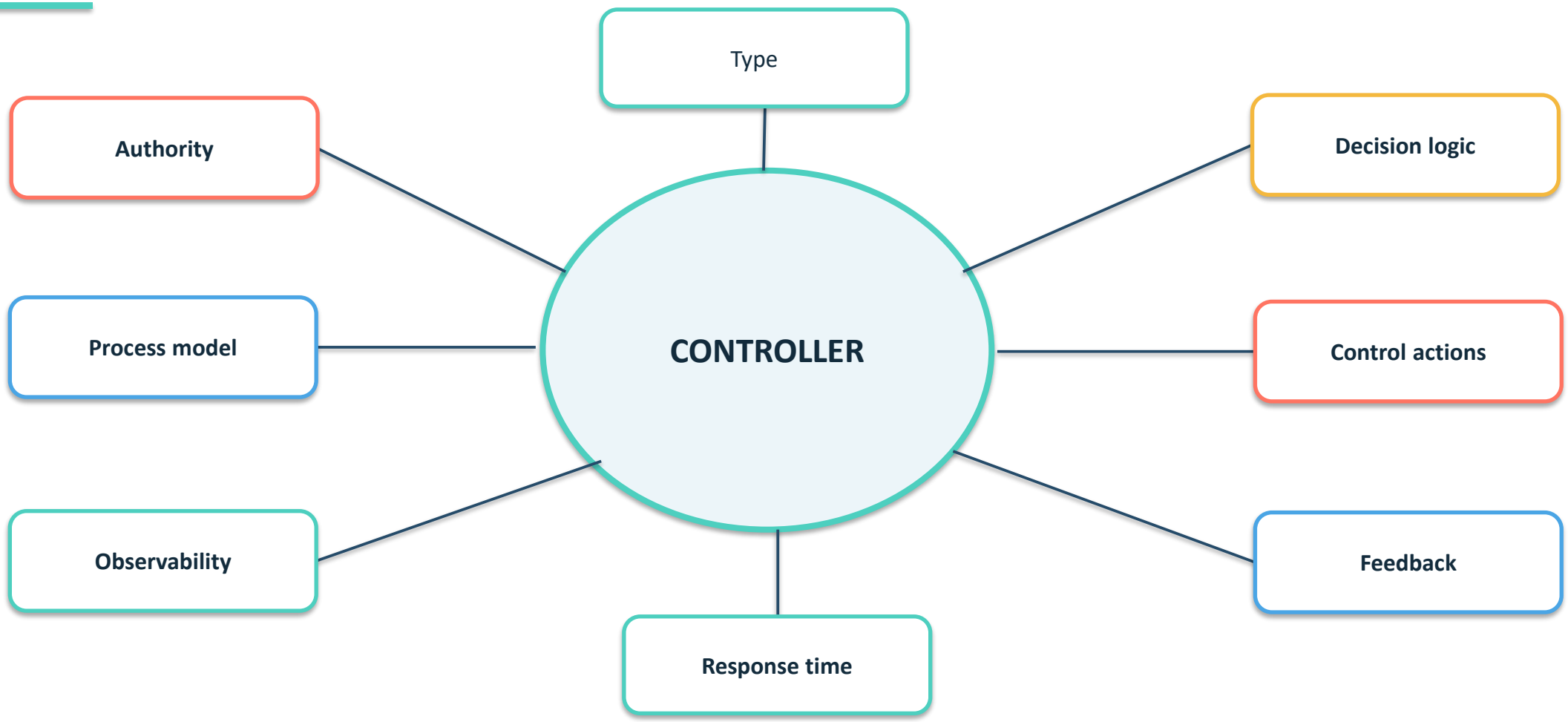


Required outputs

Controller responsibility • process-model variables • feedback sources • decision rules • control actions • verification evidence

Each output remains linked to the originating loss, hazard, UCA, and constraint

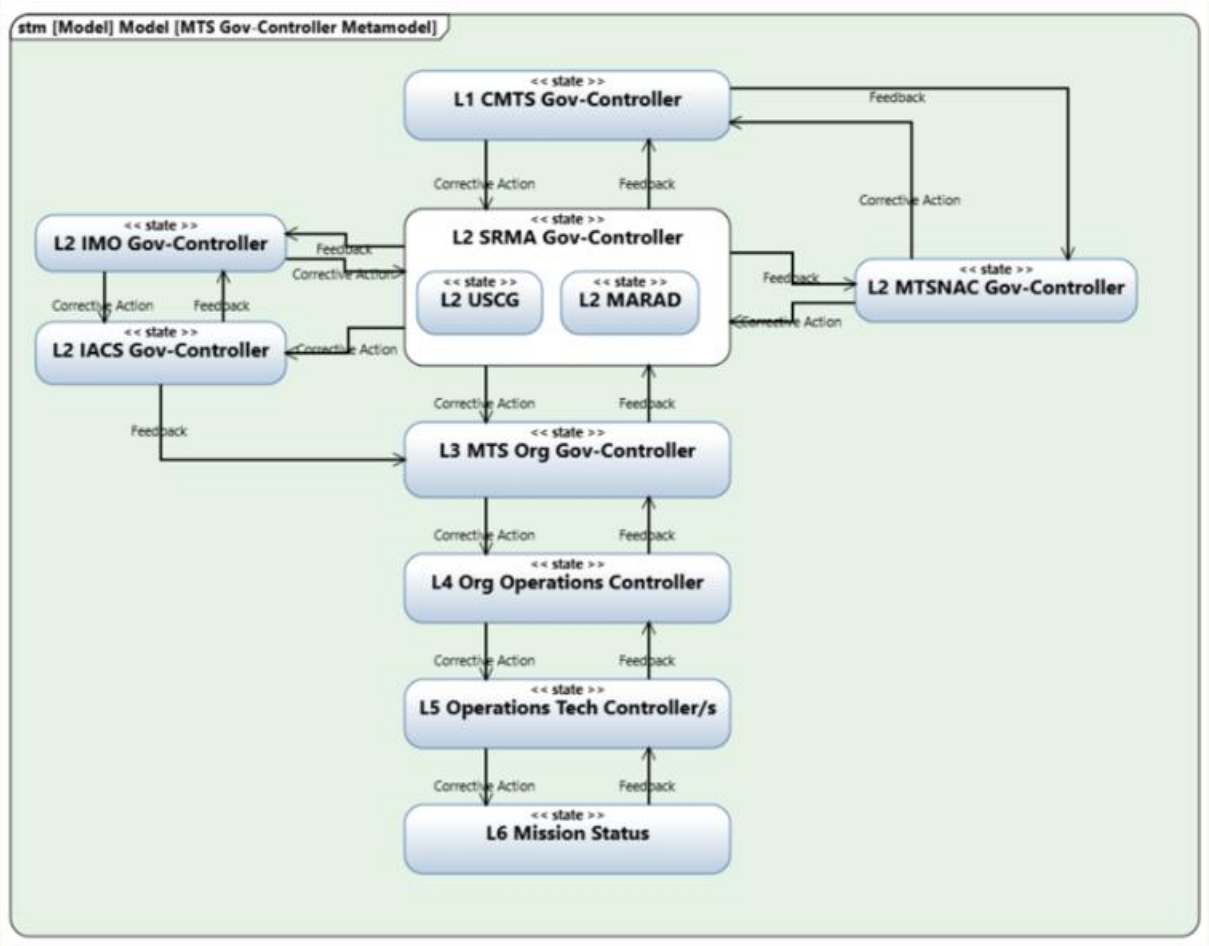
Controller requirement specification – 8 parameters



A constraint is enforceable only when the assigned controller can sense, decide, act, and confirm within the available time.

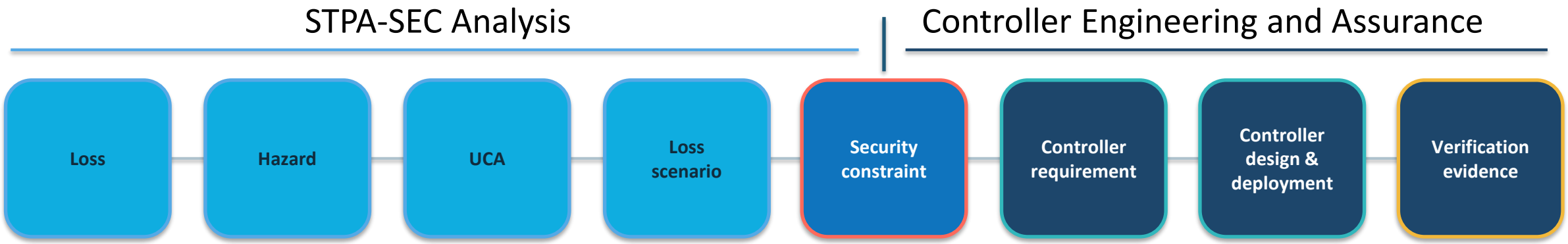
Marine transportation system controller types

- Statutory Authority Control
  - U.S. Congress
- Agency Authority Control
  - MTSNAC
- Regulatory Authority Control
  - International
    - IMO
    - IACS
  - U.S. Domestic
    - NIPP Co-SRMA - USCG
    - NIPP Co-SRMA - MARAD
- Critical Infrastructure Operator (CIO)
  - Organizational Controls
  - Operational Controls
  - Cyber-Phys- Sys Controls



Maritime Functional Control Metamodel

End-to-end traceability becomes an engineering backbone



The trace supports design reviews, change-impact analysis, verification planning, and operational accountability.

Create a unified control library for security architect use

RESEARCH OPPORTUNITY

Existing controls are distributed across statutory requirements, regulations, standards, and NIST guidance and are generally organized for compliance rather than constraint implementation and controller design.

STATUTORY & REGULATORY
Required outcomes & obligations

NIST SP 800-53
Enterprise security & privacy controls

NIST SP 800-82
OT guidance & tailoring

NIST SP 800-161
Cyber supply-chain risk controls

INTEGRATNG THE CONTROL LIBRARY

1) Consolidate multiple control guidance documents into a master (machine readable) data source
2) Develop a metadata schema/s to facilitate control use when developing an enterprise security architecture
3) Using the schema, create a multi-dimensional overlay index for the existing controls
4) Index each control by the architecture decision it supports

Promoting ease of control discovery & application

Loss → Hazard → UCA → Security Constraint → Requirement → Controller / Control → Verification

Interpretation: The opportunity is not simply to create more controls. It is to reorganize existing controls around the engineering problem of selecting and designing controllers capable of enforcing STPA-SEC-derived security constraints.

Potential control metadata overlay dimensions

Index each control by the architecture decision it supports

AUTHORITY & INTENT	ARCHITECTURAL PLACEMENT	CONDITIONS OF USE	ASSURANCE & TRACEABILITY
Source / authority	Enterprise / mission layer	Threat / failure mechanism	Loss, hazard and UCA
Control objective	Controller and controlled process	Lifecycle phase	Security constraint and requirement
Control function	Asset / resource type	Control timing	Feedback and observability
Control mechanism	Dependency and interface	Sector and technology overlay	Verification evidence

Interpretation **A port crane overlay retrieves controls by context, controller role, failure mode, and evidence**

Overlay dimension 1: control function example

Illustrative primary tag for each family; individual controls may need several tags.

AC	Access Control	ACTION
AT	Awareness and Training	AUTHORITY
AU	Audit and Accountability	FEEDBACK
CA	Assessment, Authorization, and Monitoring	ASSURANCE
CM	Configuration Management	MODEL / DECIDE
CP	Contingency Planning	MODEL / DECIDE
IA	Identification and Authentication	ACTION
IR	Incident Response	MODEL / DECIDE
MA	Maintenance	ASSURANCE
MP	Media Protection	ACTION
PE	Physical and Environmental Protection	ACTION
PL	Planning	AUTHORITY
PM	Program Management	AUTHORITY
PS	Personnel Security	AUTHORITY
PT	PII Processing and Transparency	AUTHORITY
RA	Risk Assessment	MODEL / DECIDE
SA	System and Services Acquisition	ASSURANCE
SC	System and Communications Protection	ACTION
SI	System and Information Integrity	FEEDBACK
SR	Supply Chain Risk Management	AUTHORITY

Control-level tags: assigned controller function • sensed variable • decision rule • control action • verification evidence

Source: NIST SP 800-53 Rev. 5, Table 2. Labels are a proposed engineering interpretation.

Overlay dimension 2: OT operating context example

Applying NIST SP 800-82 to a Port Crane Controller

SECURITY-DEPENDENT SAFETY CONSTRAINT

Hoist motion shall occur only when spreader-lock state is trustworthy and the command is authorized.

OT engineering questions informed by SP 800-82 Rev. 3

CONTROL PATH	**What components and information flows implement the hoist control loop?** Lock sensors → PLC logic → hoist drive; HMI and terminal interfaces
BOUNDARY	**What external systems can reach or influence the crane control path?** Segment crane OT; permit only required traffic across managed boundaries
AUTHORITY	**Who or what may issue commands or modify control logic?** Authenticate operators and vendors; constrain and monitor remote access
INTEGRITY	**Can corrupted state, commands, or logic defeat the safety constraint?** Protect sensor state, PLC configuration, commands, and event records
FAIL-SAFE / RECOVERY	**What should the controller do when state or communications cannot be trusted?** Inhibit motion; alert operator; verify state before restoring operation

Controller-engineering output: safeguards assigned to controllers, control paths, feedback, and verification evidence.

Source: NIST SP 800-82 Rev. 3, §§2.3.7, 5–6 and App. F. Crane application and constraint are illustrative.

Technology – develop a controller engineering workbench

A workbench would make controller engineering repeatable for students and working professionals.

Model the enterprise

Innoslate supports system models, architecture views, traceability, and evidence management.

Google Earth supports enterprise digital operating environment modeling.

VisualPro supports STPA-SEC analysis and decision making.

Design and test control

AnyLogic offers a potential environment to explore controller behavior in socio-technical and cyber-physical systems.

NIST overlays can tailor control guidance to sector and technology contexts.

Maintain assurance

AI-assisted architecture audits using applied STPA-SEC and control engineering logic. Run scans like what is done with networks and cloud environments for vulnerability discovery. A digital twin with a persistent data fabric and high-frequency scans would enable continuous versus episodic cyber risk management.

Notional idea

Integrate 1) Innoslate MBSE functionality with 2) VisualPro STPA-SEC decision-making support, 3) Anylogic simulation capabilities, 4) a GIS application, and 5) AI into a single application purpose built for socio-technical system cyber risk management.

UNCW's Blue Cyber Lab research capabilities – workbench candidates



MBSE



STPA-SEC Analysis





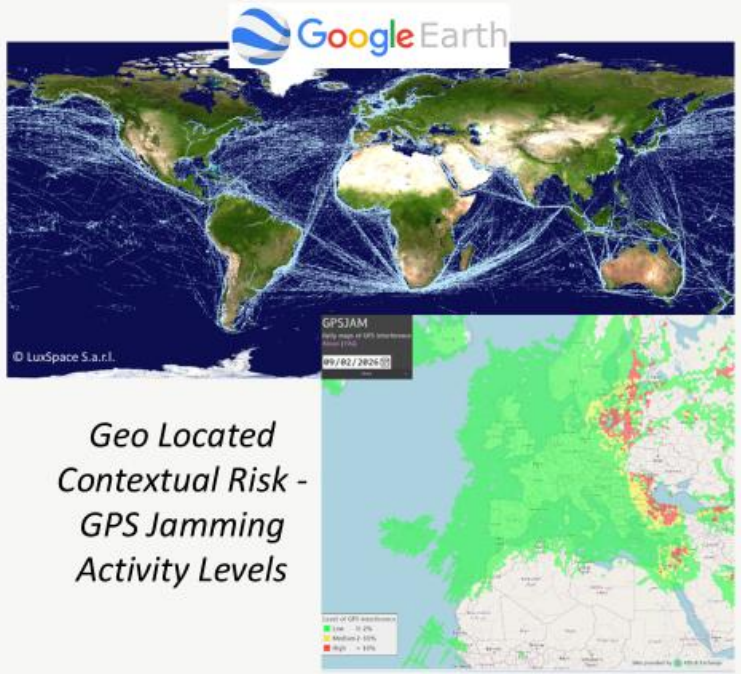
Simulation





Reference Architectures





Geo Located Contextual Risk - GPS Jamming Activity Levels

Known Losses & Threat Intel Sources

Near Future => OSCAL + MCP + AI: the next engineering bridge

Security architect→ Web App → MCP Client → MCP Server → OSCAL service/repository → security-control data

OSCAL (Open Security Control Application Language) | (MCP) Model Context Protocol

01

STPA-SEC analysis

What losses, hazards and UCAs define the required security constraints?

02

OSCAL control substrate

Which machine-readable controls, components and evidence can satisfy them?

03

STPA-SEC engineering overlay

Which controller, context, failure mode, mission thread and verification apply?

04

MCP + AI controller engineering

How can controls be queried, mapped, composed, traced and continuously assured?

IMPACT ON THE FUTURE OF CYBER RISK MANAGEMENT

Documents → executable knowledge
Machine-readable controls

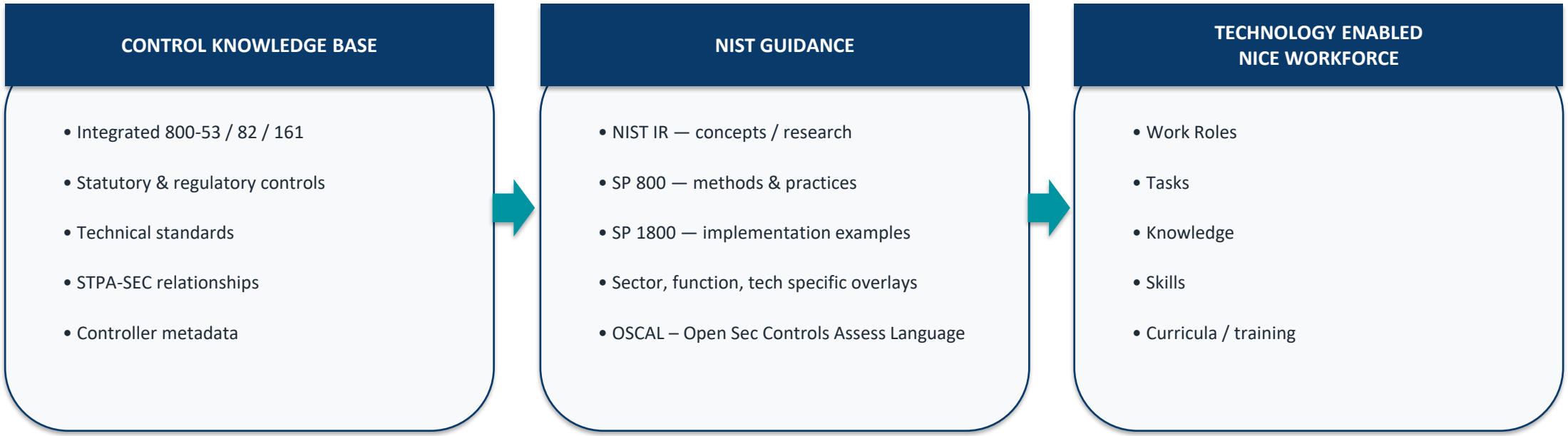
Threat-first → consequence-driven
Loss and hazard anchored

Selection → controller design
Authority, action, feedback

Periodic → continuous assurance
Traceability as systems change

Research opportunity: define the semantic bridge that turns STPA-SEC security constraints into AI-assisted, traceable controller requirements and verified controls.

Integration from the control library to NIST guidance and NICE workforce development



CENTRAL RESEARCH PROPOSITION

STPA-SEC Constraints + Structured Control Library → Controller-Engineering Guidance → Sector / Technology Overlays → Reference Implementations → NICE TKS

Interpretation: A common controller-engineering model could connect what must be controlled, how controls are engineered and implemented, and what the workforce must know and be able to do.

Selected references and foundations

This work extends STPA-SEC control-theoretic analysis through a more explicit controller-engineering bridge to lifecycle systems-security engineering.

01 **Leveson, N. G. (2011).**
Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.

02 **Young, W., & Leveson, N. G. (2014).**
An Integrated Approach to Safety and Security Based on Systems Theory. Communications of the ACM, 57(2), 31–35.

03 **NIST SP 800-160 Vol. 1 Rev. 1 (2022).**
Engineering Trustworthy Secure Systems.

04 **NIST SP 800-160 Vol. 2 Rev. 1 (2021).**
Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.

05 **NIST CSF 2.0 (2024).**
The NIST Cybersecurity Framework (CSF) 2.0.

06 **ISO 31000:2018.**
Risk management — Guidelines.

Questions, constructive feedback, and collaboration inquiries are always welcome!

Jeff Greer

University of North Carolina Wilmington

greerj@uncw.edu

Extending STPA-SEC from analysis to controller engineering

AI Use Disclosure: ChatGPT was used to assist with research, drafting, and presentation development. The author reviewed and is responsible for all technical content, interpretations, and conclusions.