International Council on Systems Engineering
A better world through a systems approach

Helping Future Nuclear Power Facilities Navigate Predatory & Hostile Environments:

Insights from Systems Security Engineering

Adam D. Williams

Distinguished R&S Systems Engineer

Center for Global Security & Cooperation

Sandia National Laboratories

INCOSE International Symposium 2025 | Ottawa, Canada

* SAND2025-04824C

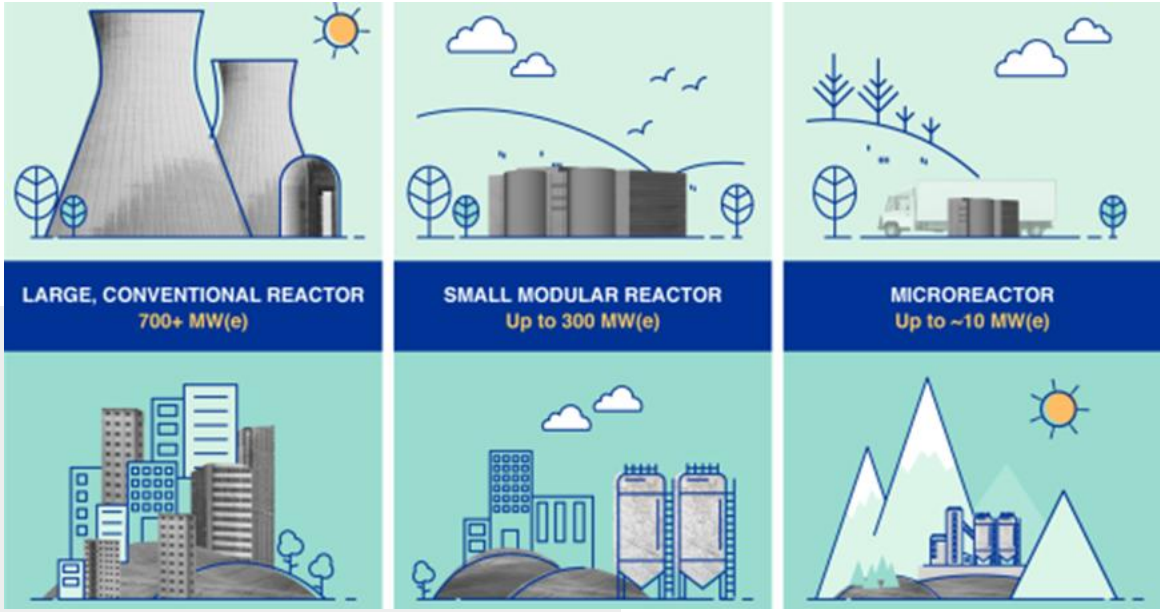
Today's Agenda

- Introduction
- Background & Problem Framing
- Systems Security Engineering (SSE): A New Approach
- SSE Approach for A/SMR Security-by-Design
- Conclusions

Introduction

Advanced & Small Modular Reactors (A/SMR) specifically noted to support global ***climate change mitigation*** & ***energy security*** goals

- Remote & urban deployment
- Novel fuel types & safer operations
- New fuel flows & handling systems
- Increased automation in operations
- Smaller onsite staffing



Courtesy: *International Atomic Energy Agency*

Introduction

Advanced & Small Modular Reactors (A/SMR) specifically noted to support global ***climate change mitigation*** & ***energy security*** goals

“that focused on ways to speed up deployment of SMRs … . The event showcased new partnerships, including a deal between Google and Kairos Power to deploy 500 MW of SMR capacity by 2035, and emerging opportunities for financing”

“to include nuclear power in … national energy planning in a sustainable way that adheres to the highest standards of safety, security, and safeguards”

Introduction

- Goal to “evolve the systems engineering capability” → A/SMR security needs
  - “*Threats must be continuously assessed throughout the system life cycle and solutions implemented, ensuring security and cyber-defense against both ad hoc and organized (national actor) threats* (pg. 11).”

- New insights for A/SMR security:
  - Complexity of both attacks & defenses is continuously evolving
  - Embed security throughout the lifecycle
  - Address “predatory” & “hostile” operational environments
  - Needs-oriented, loss-driven, capability-based SSE
  - Shift goal toward achieving ***functional persistence***

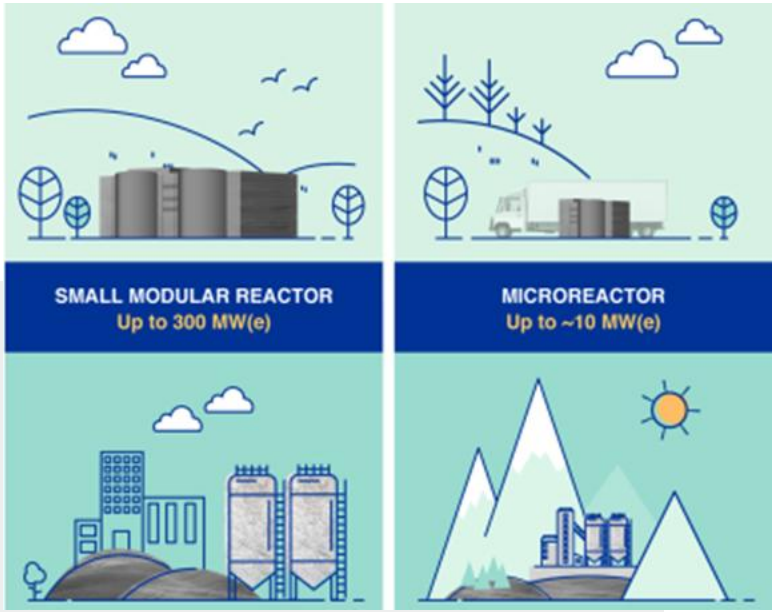
Background & Problem Framing

A/SMRs have unique deployment & operational characteristics:

- Reliance on *passive safety* systems
- Increased digitization & automation
- (Potential) Remote operations
- Remote & urban deployment

A/SMRs success closely tied to effectively addressing security concerns, as noted by:

- "the importance of nuclear security considerations" for A/SMRs
  - *Co-Presidents' Statement, IAEA International Conference on Nuclear Security (ICONS)*
- "maintaining high standards of nuclear safety and security" for A/SMRs
  - *Conference Report, IAEA International Conference on Small Modular Reactors & Their Applications*



Courtesy: *International Atomic Energy Agency*

Background & Problem Framing

Intentional desire to cause damage → "predatory environments"

- A/SMR flexible deployment ***increases*** predatory environments via potential for A/SMRs in locations
  - Where personnel may lack extensive experience in nuclear safety & security protocols
  - With regulatory may lead to situations where protection levels are not robust or appropriate

- A/SMRs also face constantly evolving threat landscapes, including
  - Increased digitization expands both cyber & physical "attack surfaces"
  - Capabilities of non-state actors have improved → more sophisticated attacks

- Improved A/SMR security suggests a need:
  - To shift away from traditional designs (e.g. costly "layers" of security)
  - For a comprehensive understanding of the increasing complexity of attack and defense mechanisms
  - To adopt a proactive and adaptive approach to security that considers the unique system & environment characteristics

Background & Problem Framing

"It is also imperative that the nuclear industry embrace a *proactive stance toward security* that prioritizes resilience and adaptability. INCOSE 2035 offers pathways toward this end … to develop comprehensive frameworks that address the multifaceted security concerns associated with A/SMRs."

SSE: A New Approach

INCOSE → Systems Theory Concepts & Approaches → Improved Security Performance

SSE: A New Approach

INCOSE → Systems Theory Concepts & Approaches → Improved Security Performance

Framework for ***embedding security into the systems engineering process***:

- **Planning** → establishing security decisions to address requirements
- **Risk assessment** → identifying & evaluating potential risks
- **Requirements definition** → translating identified needs into action statements
- **Design & architecture** → developing security controls to meet security needs
- **Implementation** → deploying security controls as part of the overarching design
- **Verification & validation** → ensuring that controls meet the requirements
- **Maintenance** → monitoring & maintaining controls during the operational life

SSE: A New Approach

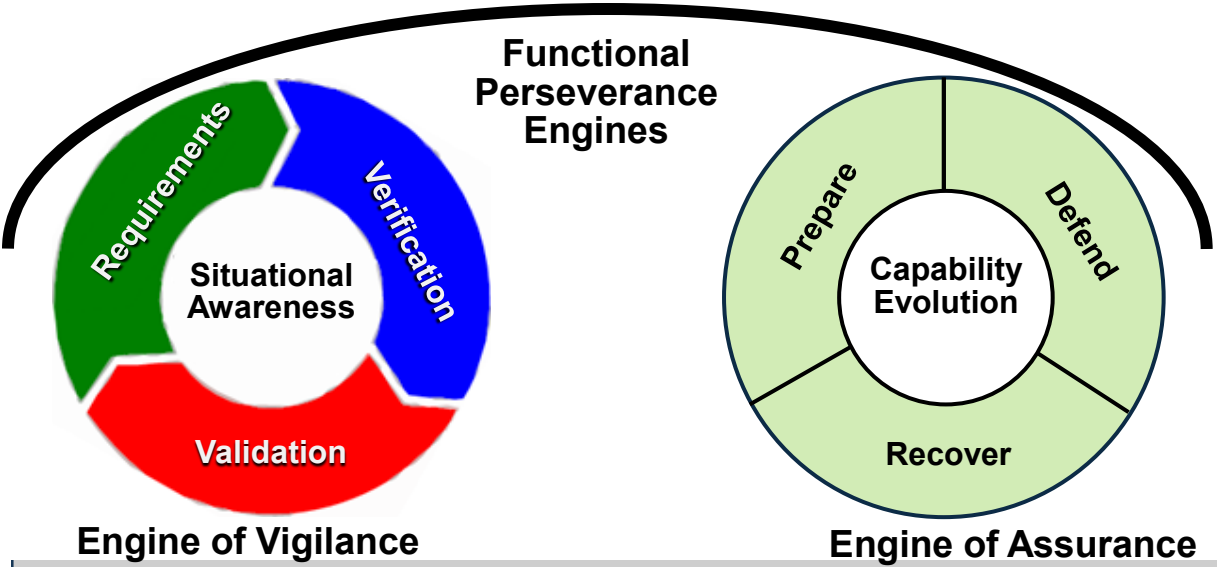
INCOSE → Systems Theory Concepts & Approaches → Improved Security Performance

Characteristics for ***embedding security into the systems engineering process***:

- **Evolve from passive mindset** → active ethos for security
- **SSE environment** → increasingly contested, hostile & predatory
- **Transition from mitigating vulnerabilities** → ensuring system functionality
- **(Re)emphasize key attributes** → (1) intentionality & (2) desire to cause harm
- **New SSE goal** → ensure functional system persistence in contested environments

SSE: A New Approach

INCOSE → Systems Theory Concepts & Approaches → Improved Security Performance



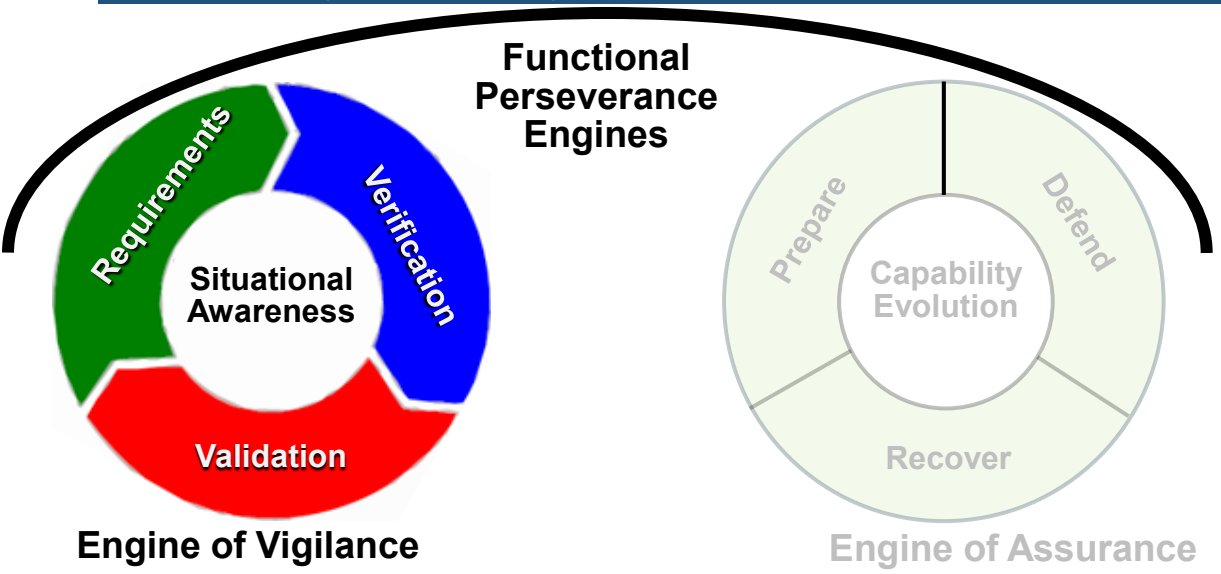
- **New SSE goal** → ensure functional system persistence in contested environments

"Engines of Functional Perseverance" Model

- Guiding principle is to maintain system operations & success
- Mitigates ever-changing gap between attack complexity & defense capability
- Better address potential threats throughout design & deployment

SSE: A New Approach

INCOSE → Systems Theory Concepts & Approaches → Improved Security Performance



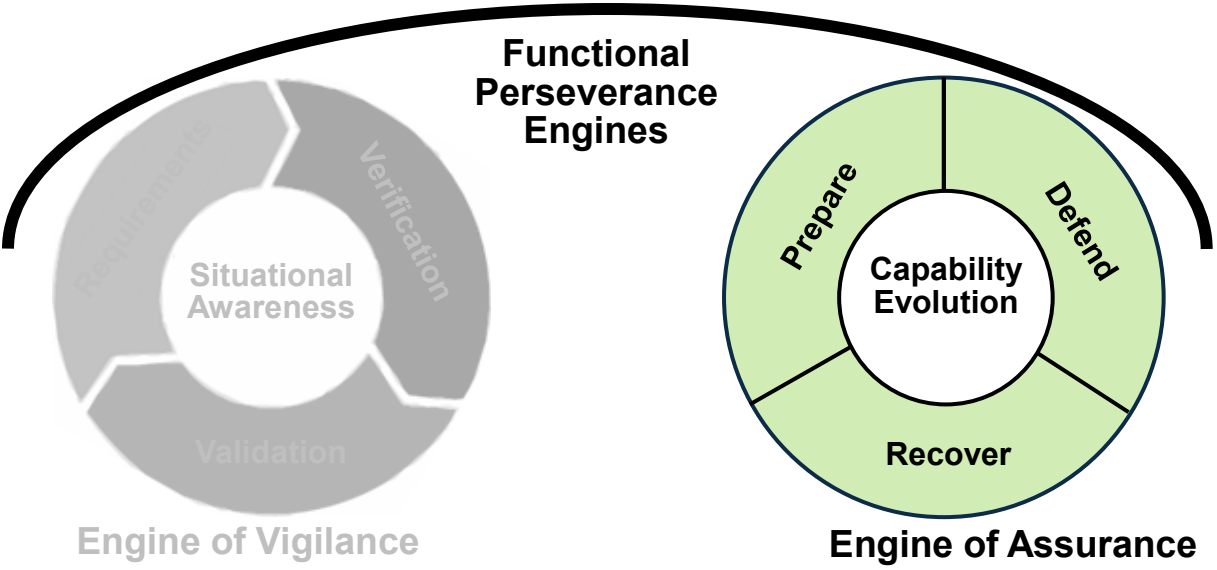
"Engine of Vigilance"

- Per M-W Dictionary, ***vigilance***:
  - "being alertly watchful"
  - "to avoid danger"
- Aligns with INCOSE's Guide to Security Needs & Requirements
- Engine elements:
  - Requirements
  - Verification
  - Validation

- **Engine goal** → ensure enhanced & continuous situational awareness

SSE: A New Approach

INCOSE → Systems Theory Concepts & Approaches → Improved Security Performance



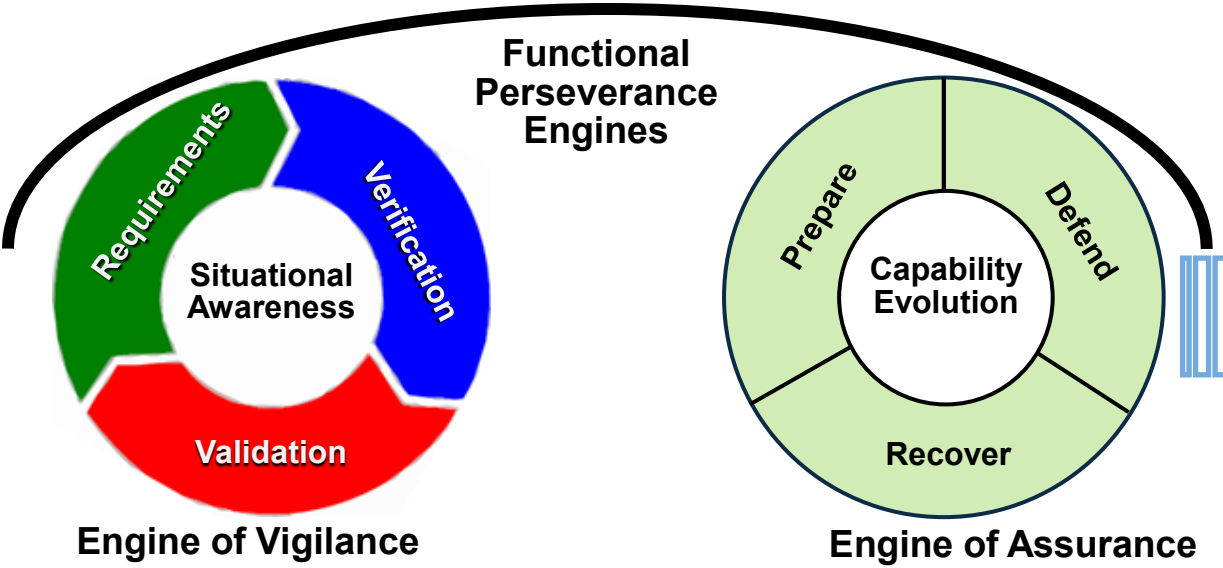
"Engine of Assurance"

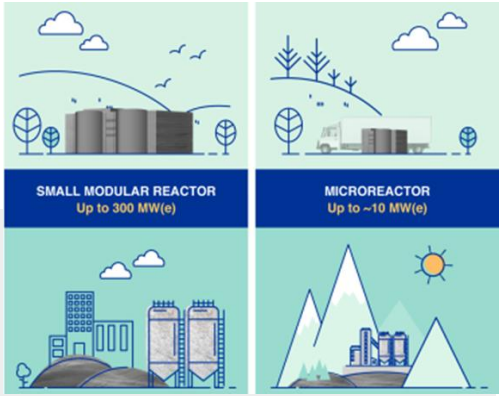
- Per M-W Dictionary, ***assurance***:
  - "confidence of mind"
  - "freedom from … uncertainty"
- Aligns with INCOSE's Guide to Security Needs & Requirements
- Engine elements:
  - Preparation
  - Defense
  - Recovery

- **Engine goal** → mitigate impacts of evolution in attacker/defender capability gaps
  - *NOTE: Engine name updated to "Engine of *Resilience*"

SSE: A New Approach

INCOSE → Systems Theory Concepts & Approaches → Improved Security Performance





Courtesy: *International Atomic Energy Agency*

- **INCOSE/GSNR** → early, frequent, & continuous inclusion of security
- **INCOSE/SSE-WG Model** → needs-oriented, loss-driven, capability-based security

SSE: A/SMR Security-by-Design

SSE → robust logic for SeBD

- Incorporate security as early as practical
- SSE basis → enhanced adaptability agility

Lifecycle models are instrumental

- System decisions evolve as the design matures
- Help map different system maturity with uncertainties

Engineering + Regulatory Elements

- Similar scaffolding to add regulatory requirements
- Identify where technical decisions align with regs

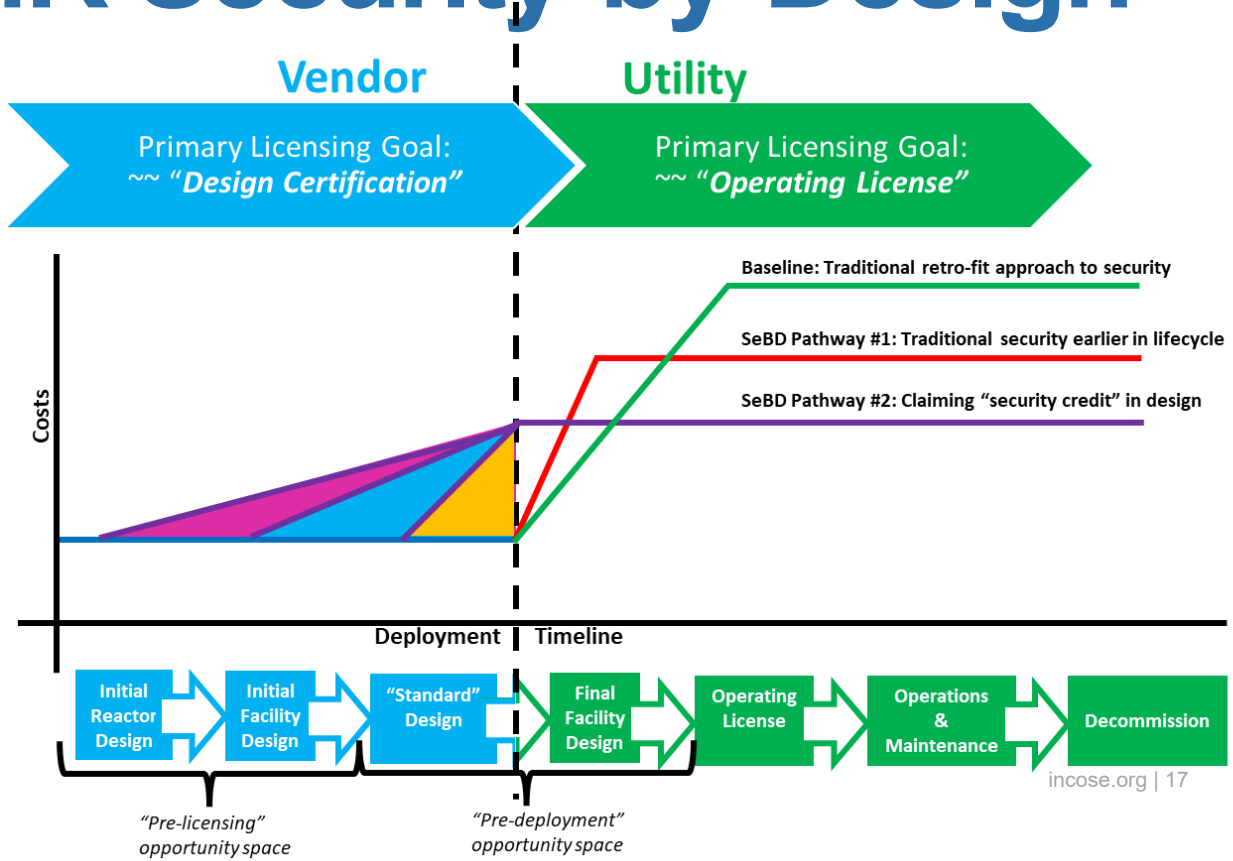
Impacts on SeBD for A/SMRs

- Framework maps vendor & utility security roles
- Options to optimize the security-cost-licensing trade space

- **INCOSE/GSNR** → early, frequent, & continuous inclusion of security
- **INCOSE/SSE-WG Model** → needs-oriented, loss-driven, capability-based security

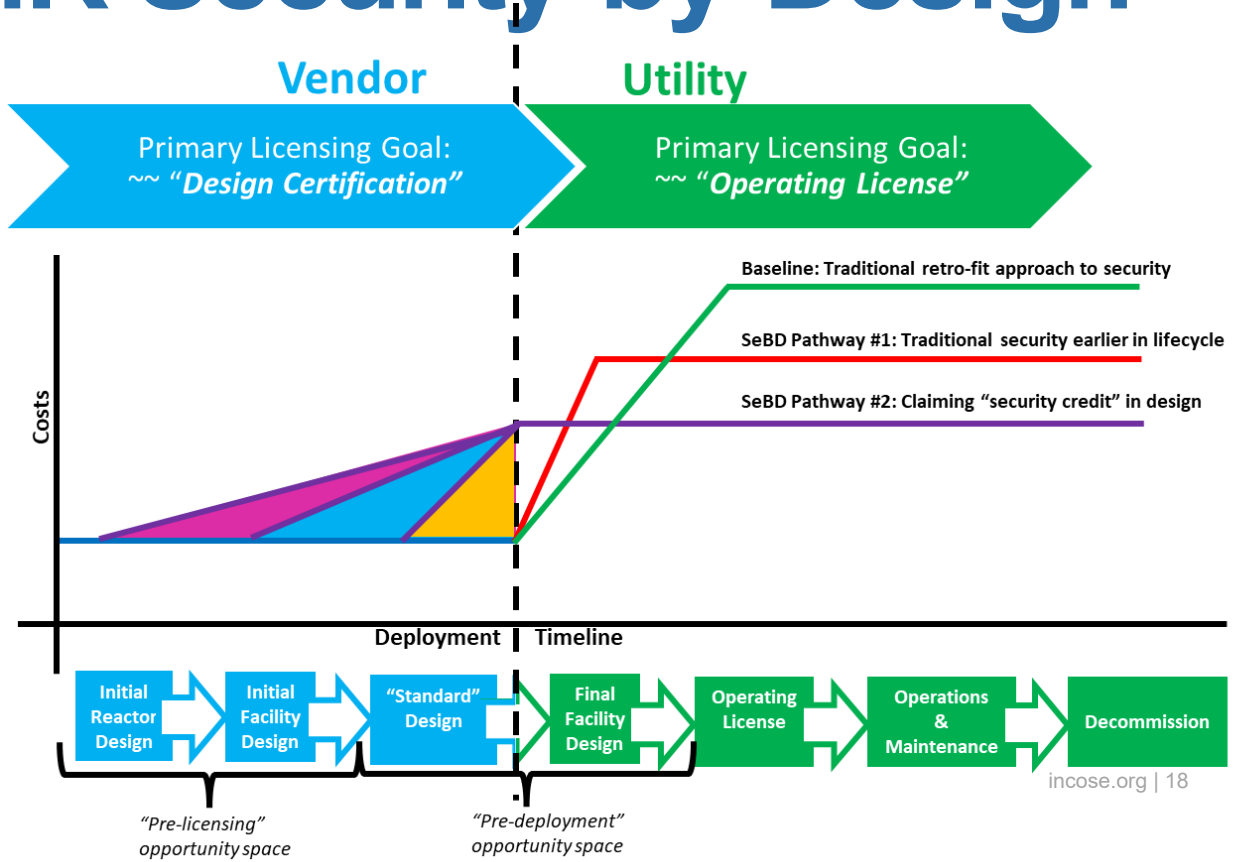
SSE: A/SMR Security-by-Design

- Combined lifecycle model:
  - Mitigate “retrofit” approach
    - Green lines
  - Goal → ID options for “security credit”
    - Red & Purple Lines
    - || to improving vigilance & assurance
- New pathways to meet ***vigilance*** or ***assurance*** objectives:
  - ***pre-licensing*** → security controls addressed in the vendor portion
  - ***pre-deployment*** → security controls addressed early in the utility portion



SSE: A/SMR Security-by-Design

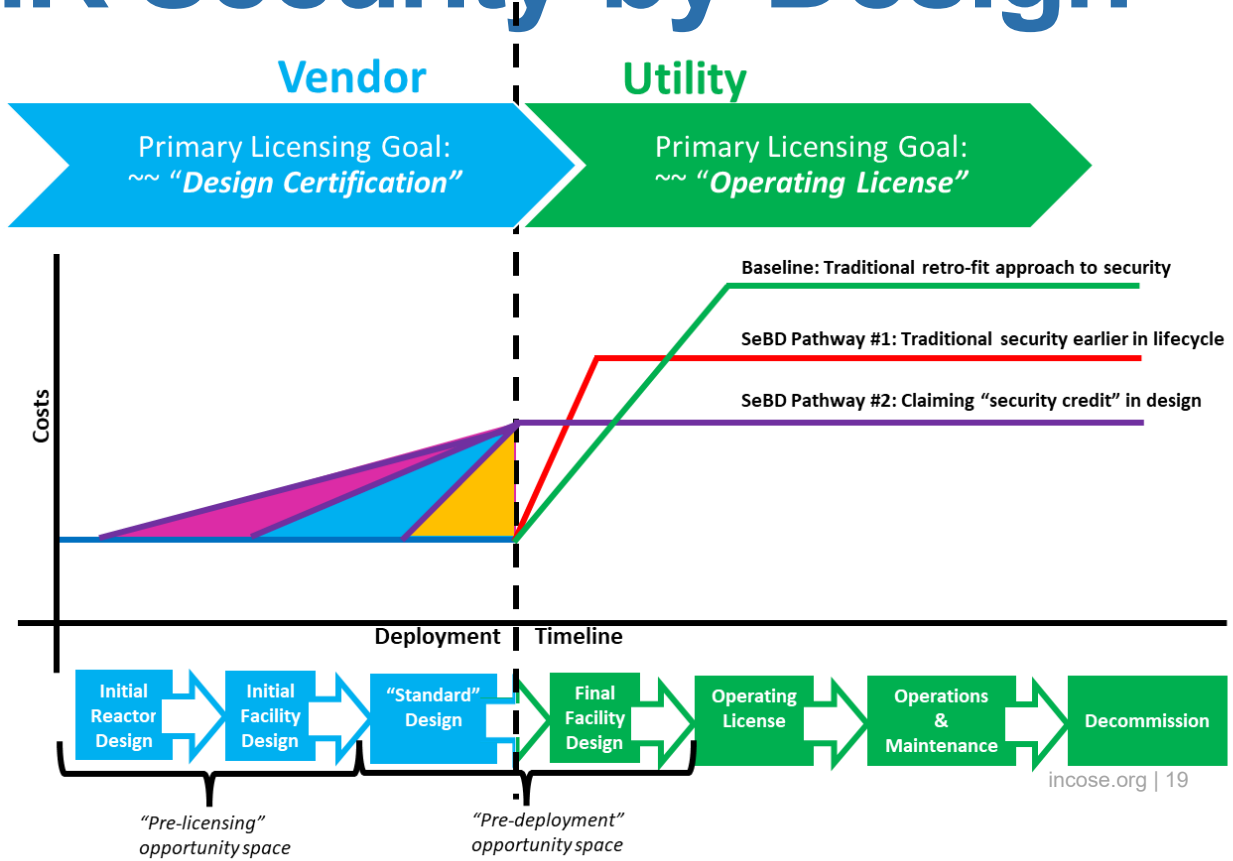
- Security-related Insights:
  - Retrofitted security costs reduced/eliminated
  - New strategies for evaluating security controls:
    - ***Incorporate security controls*** into the initial reactor design
      - Ex: enhanced nuclear fuel tracking efforts or offering sealed reactor cores
    - Address ***vigilance & assurance actions*** in the initial facility design
      - Ex: hardening connections between the reactor and support systems



SSE: A/SMR Security-by-Design

Use Case: Research Reactors

- Case #1: IAEA (SSG-20, Rev 1)
  - redesigning cooling & operability to address manipulation (SAR Ch. 6, 7)
  - evaluating digital accounting & control to minimize access (SAR Ch. 12)
- Case #2: NRC (PSAR & FSAR)
  - preventing safety limits exceedence, including manipulation (PSAR Ch. 4)
  - preventing attempts to render auxiliary systems (PSAR Ch. 9)
- "security-by-design" → ***vigilance*** & ***assurance*** SSE goals



Conclusions

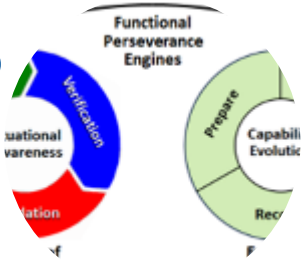
Systems security engineering, then, becomes a focus on ensuring ***functional system persistence*** in predatory and hostile environments

(SSE) incorporates design thinking for proactive, adaptive self-preservation capabilities to counter intelligent, determined attacks into systems engineering, through requirements, trade space navigation, and systems architecture

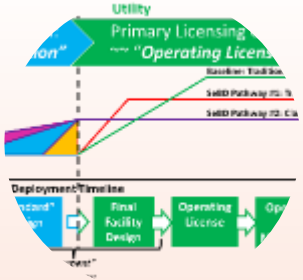
A shift from traditional, reactive security strategies to a proactive and adaptive approach augments continuous threat and advanced technology assessment with seeking innovative self-preservation capabilities to counter sophisticated attacks in SSE

Conclusions

SSE provides insights to help A/SMRs achieve improved security performance ***to overcome the challenges of tomorrow's threat landscape*** & meet global climate change and energy security needs



Security solutions should be investigated in terms of their ability to increase the robustness of situational awareness (ie., the "Engine of Vigilance") and to reduce defensive or recovery uncertainty (ie., the "Engine of Assurance")



A combined lifecycle model helps map system maturity levels and associated uncertainties, the underlying SSE concepts support early, frequent, and continuous incorporation of security controls