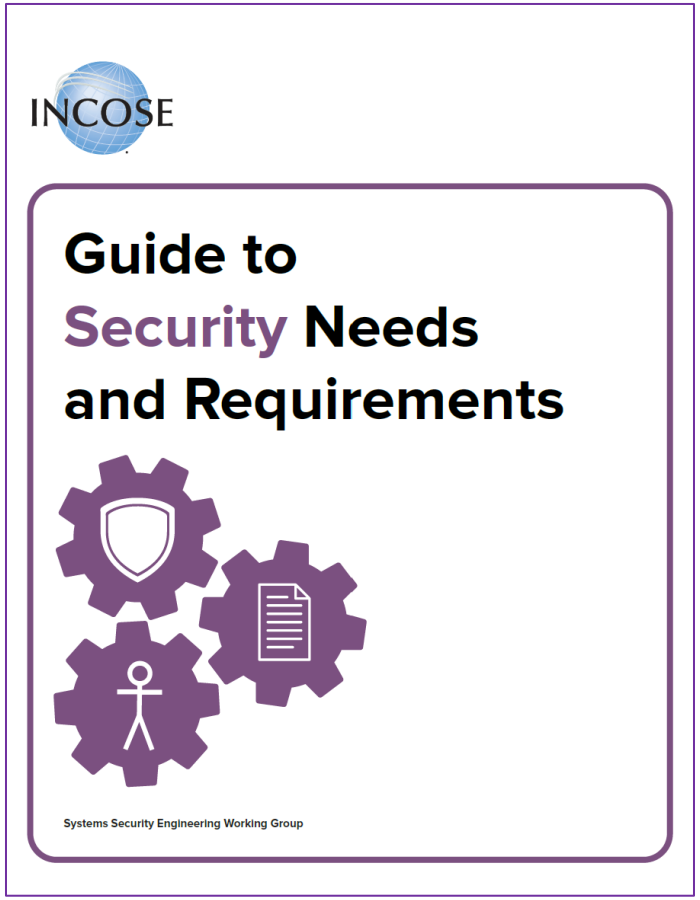
Guide to Security Needs and Requirements



Beth Wilson

21 January 2025

New Addition to RWG Products Family

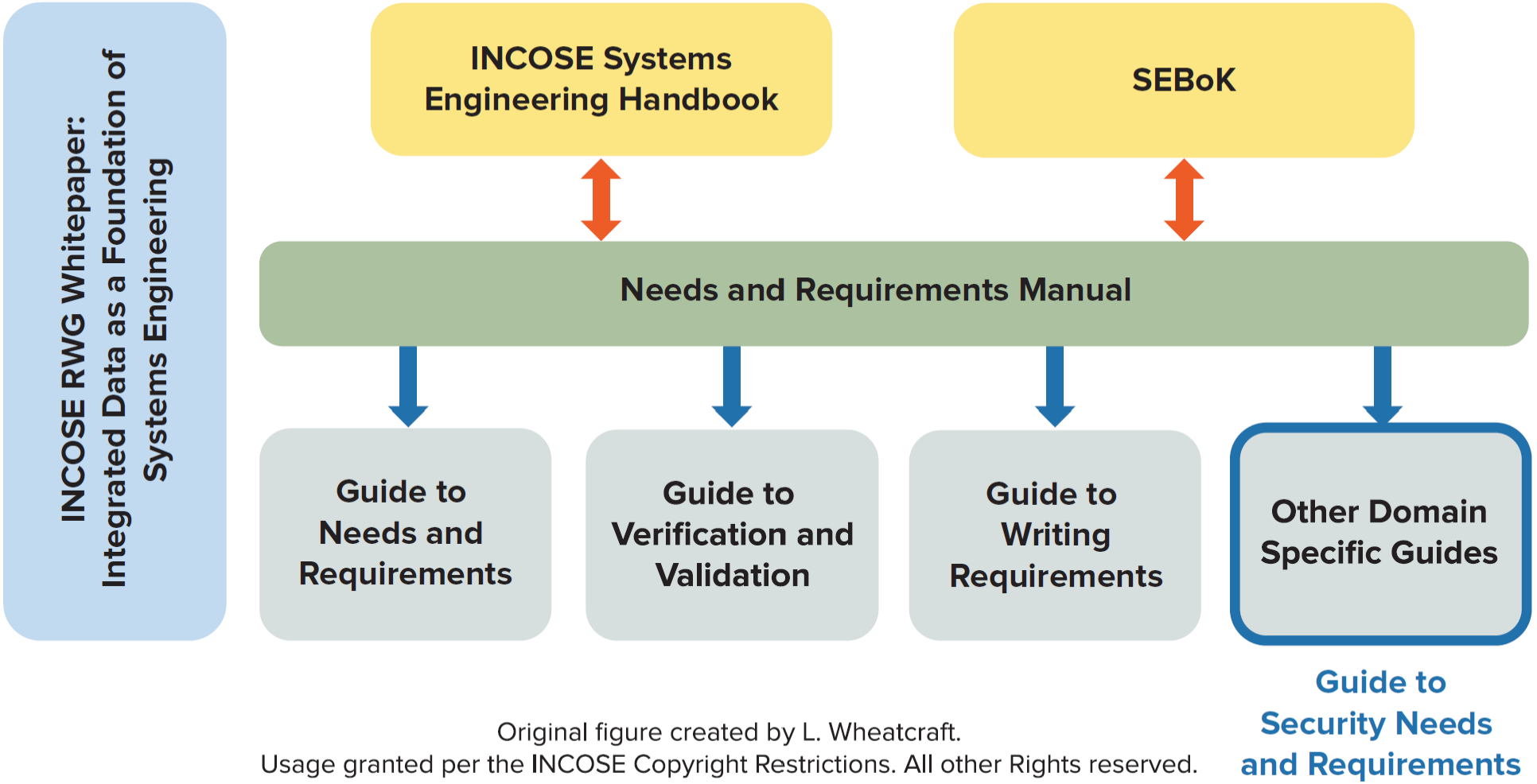


Figure 1: Requirements Working Group (RWG) Products

Security Focus for NRVV Concepts

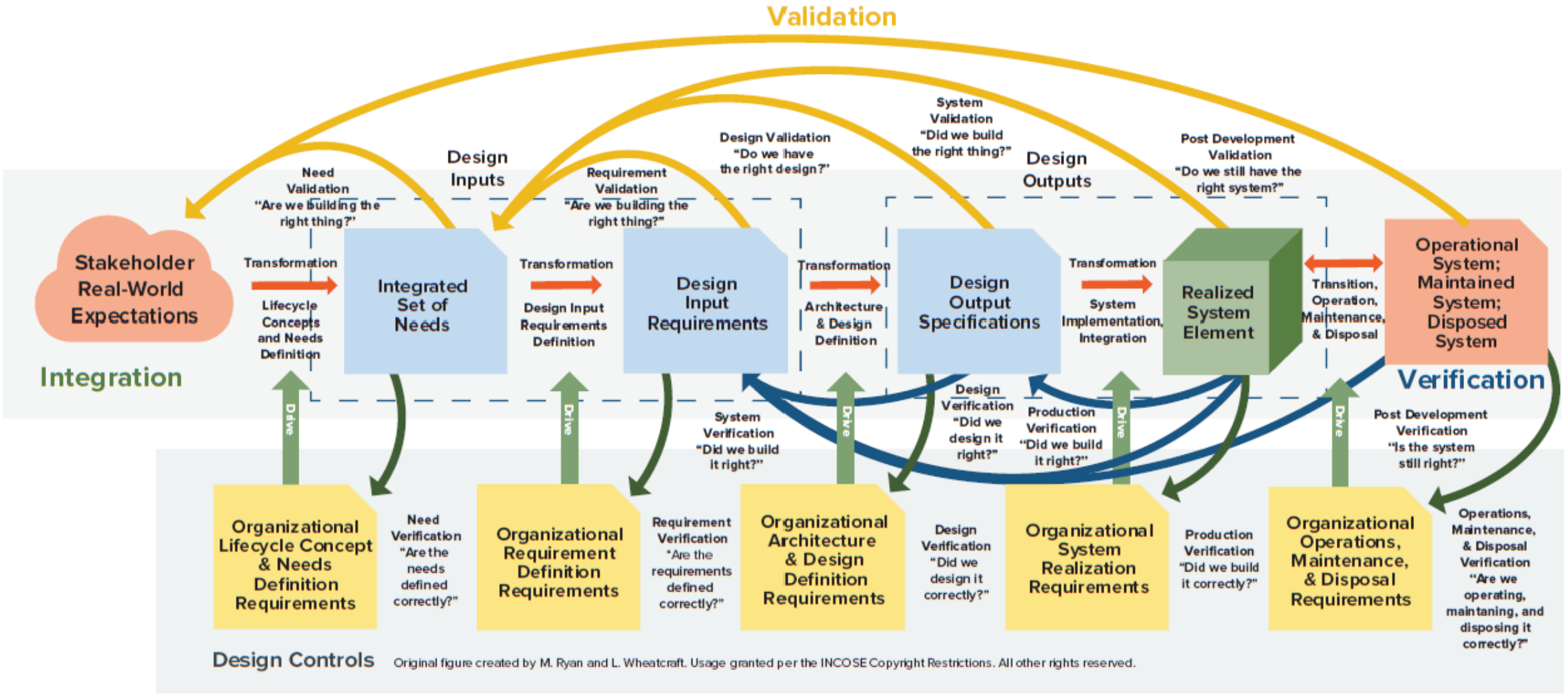


Figure 2: Needs, Requirements, Verification, and Validation (NRVV) Concept Overview (from NRM)

Systems Security WG FuSE Effort

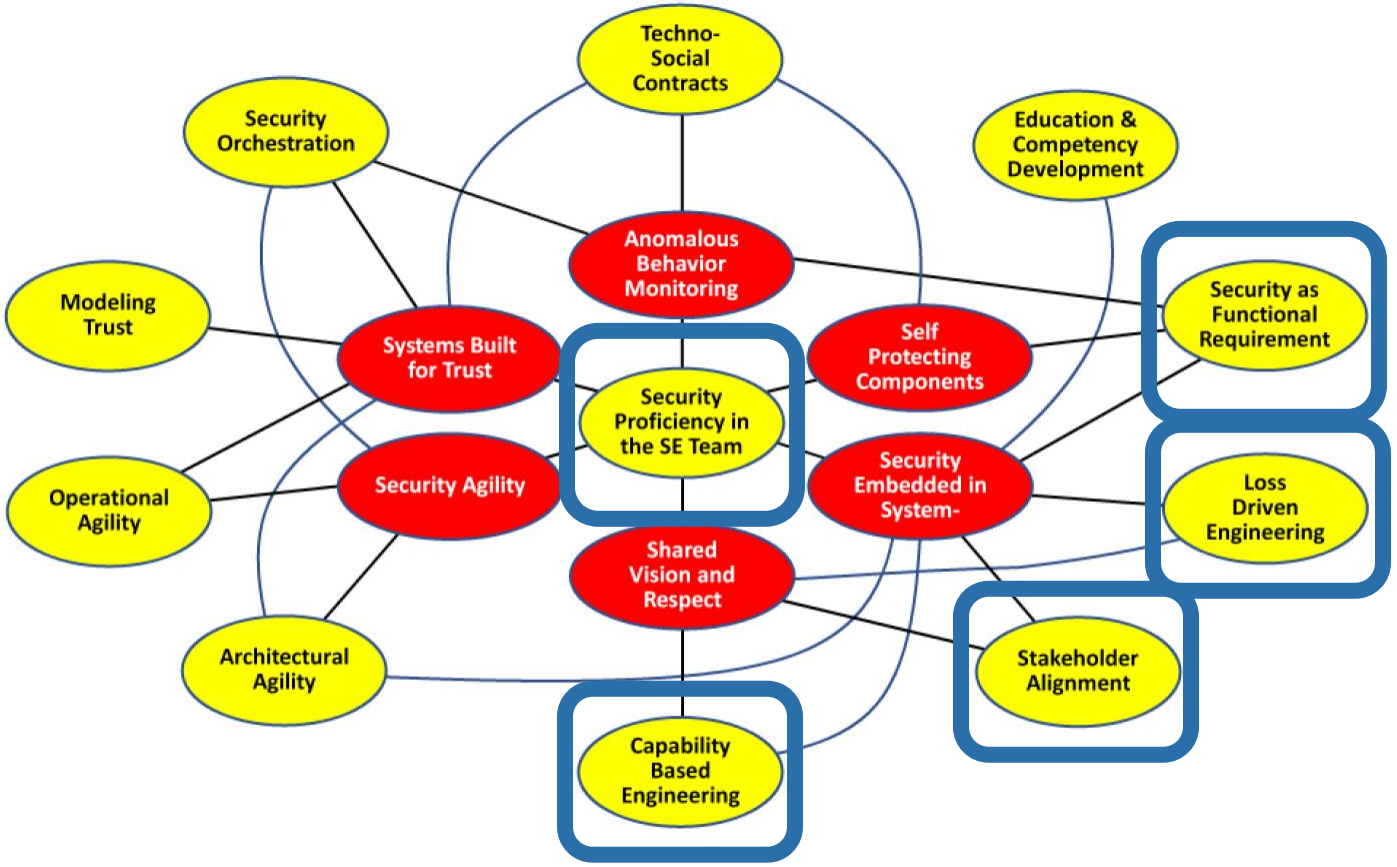
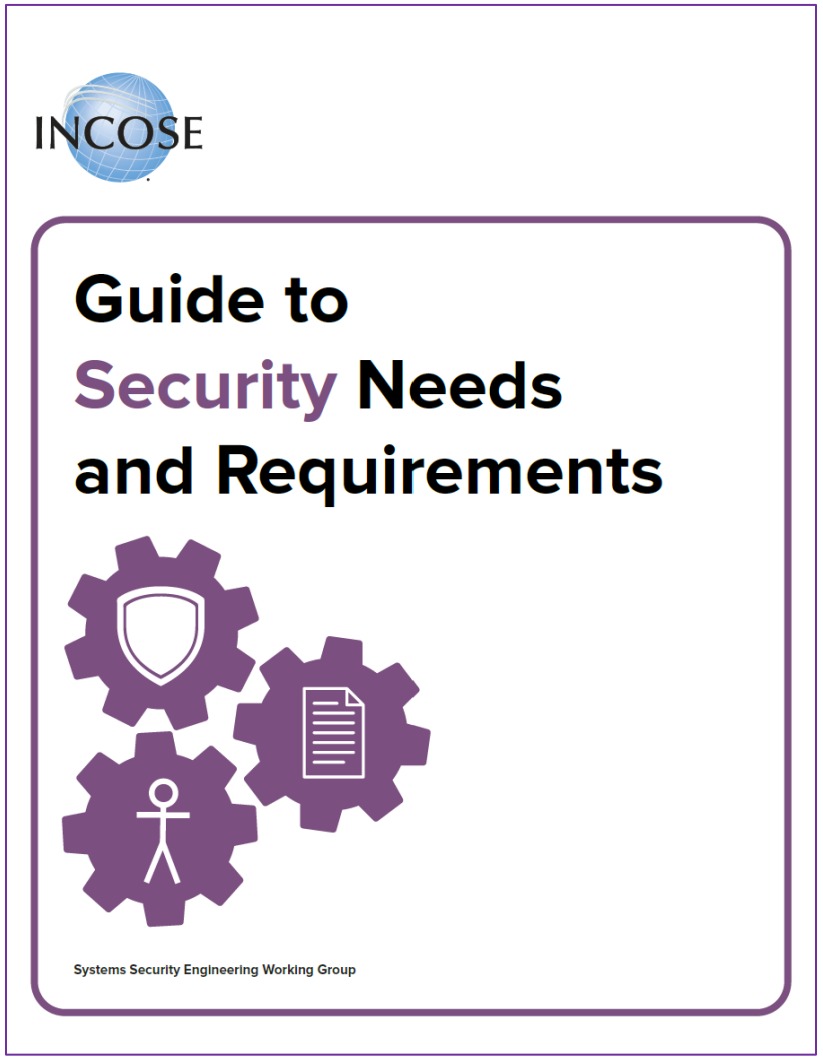


Figure 2. Synergistic linkage of Foundation Concepts (yellow/light ovals with black text) to Objectives (red/dark ovals with white text).

IS21 Paper "Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts"

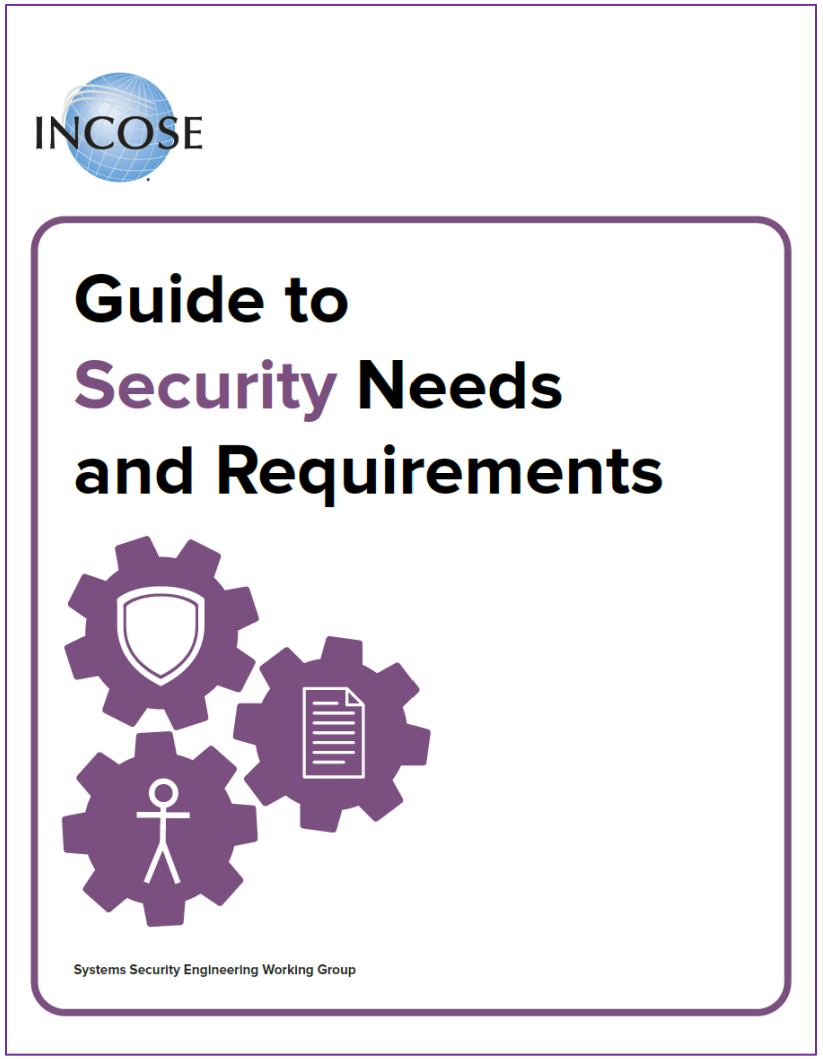
- **Security as a Functional Requirement**: move away from security as NFR
- **Security Proficiency in SE Team**: collaboration and interaction between SE and SSE
- **Security Needs and Requirements Approach**:
  - **Needs-Oriented**
  - **Loss Driven**
  - **Capability-Based**

Joint SSWG/RWG Project



- **October 2022 Kickoff**
- **Anti-Patterns → Desired Pattern**
  - Anti-patterns for security
    (what we don't want because it isn't working)
  - Needs-oriented, loss-driven, capability-based analysis
    (what we want)
- **Domain-Specific Guide Format Experiments**
  1. Stand-alone security implementation of NRVV
  2. "Rosetta Stone" translation of NRVV to security
  3. Security focus for NRVV terms
- **August 2024 Publication**

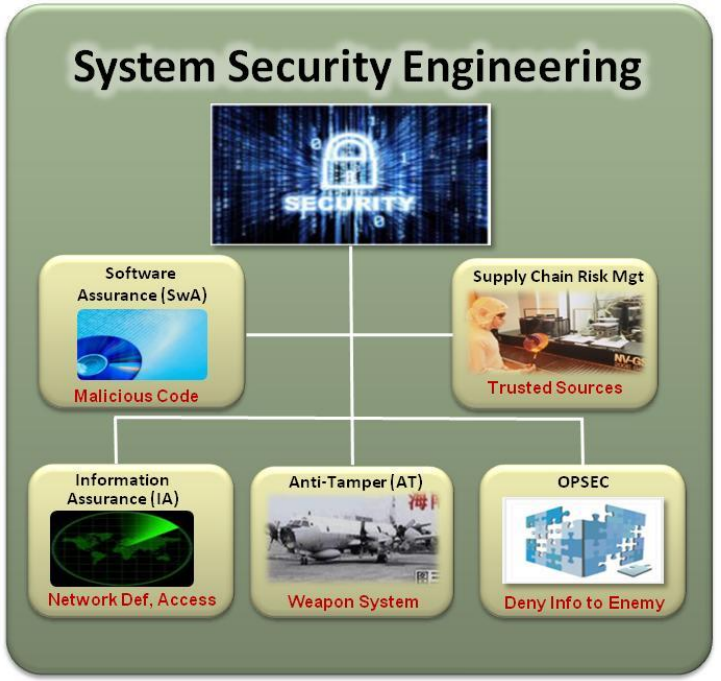
Joint SSWG/RWG Project



- **October 2022 Kickoff**
- **Anti-Patterns → Desired Pattern**
  - Anti-patterns for security
    (what we don't want because it isn't working)
  - Needs-oriented, loss-driven, capability-based analysis
    (what we want)
- **Domain-Specific Guide Format Experiments**
  1. Stand-alone security implementation of NRVV
  2. "Rosetta Stone" translation of NRVV to security
  3. Security focus for NRVV terms
- **August 2024 Publication**

“We Used a Security Expert”

Needs	Want a secure system
Requirements	NFRs created/reviewed by one security SME
Operational System	Not secure

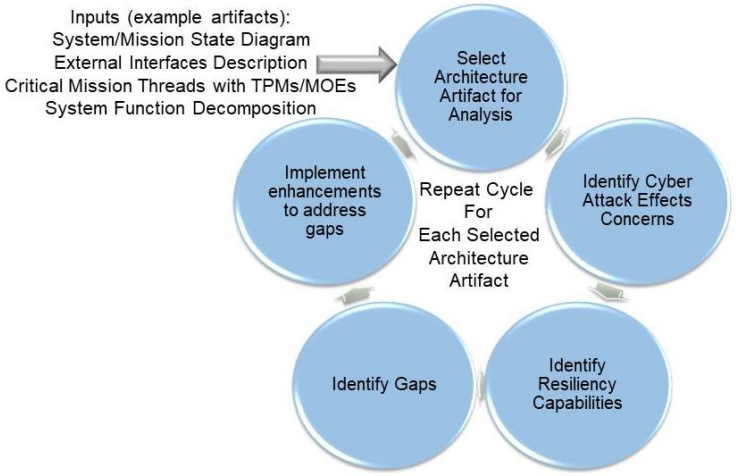


H. Dunlap, “NDIA SSE Engineering Committee,” NDIA SE Conference, 2013.

- **Anti-Pattern:** One security SME to cover all SSE disciplines:
  - Information Assurance expert with IT credentials looking at anti-tamper
  - Software Assurance expert reviewing a supply chain SOW
- **Mental model**: we had THE security expert look at it, we’re all set

“Security Review After Design”

Needs	Want a secure system
Requirements	“Shall be secure”
Collaboration	SS practitioner on review team
Operational System	Not secure



Hassell, S., B. Wilson, and P. Williams, “Cyber Secure and Resilient Techniques for Architecture.” INCOSE International Symposium 2020.

- **Anti-Pattern:** Allow systems security practitioners to review the design after it is complete
- **Mental model**: they identified some scary scenarios, but it is too late to change anything

“Security Controls”

Needs	Want a secure system
Requirements	NIST SP 800-53 controls
Verification	Checklist of controls
Operational System	Not secure

- **Anti-Pattern:** Open the controls closet and pull everything out
- **Mental model**: if we want to get the security certification, we need to make sure we include ALL the controls!

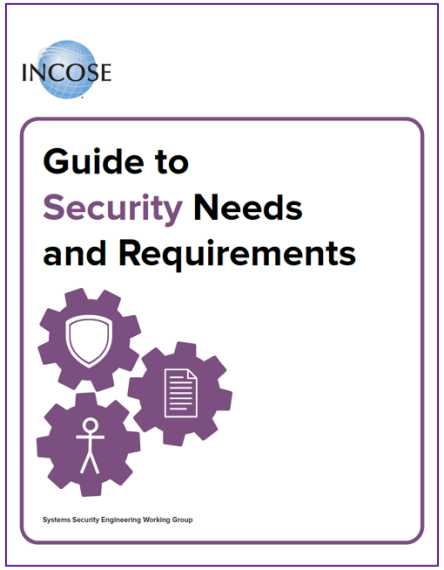
“Non-Functional Requirements”

Needs	Want a secure system
Requirements	Shall do XYZ securely
Design	Basic security measures
Verification	Confirm basic security measures are in place
Operational System	Not secure

- **Anti-Pattern:** Security is a non-functional requirement
- **Mental model**: just add a firewall and require passwords

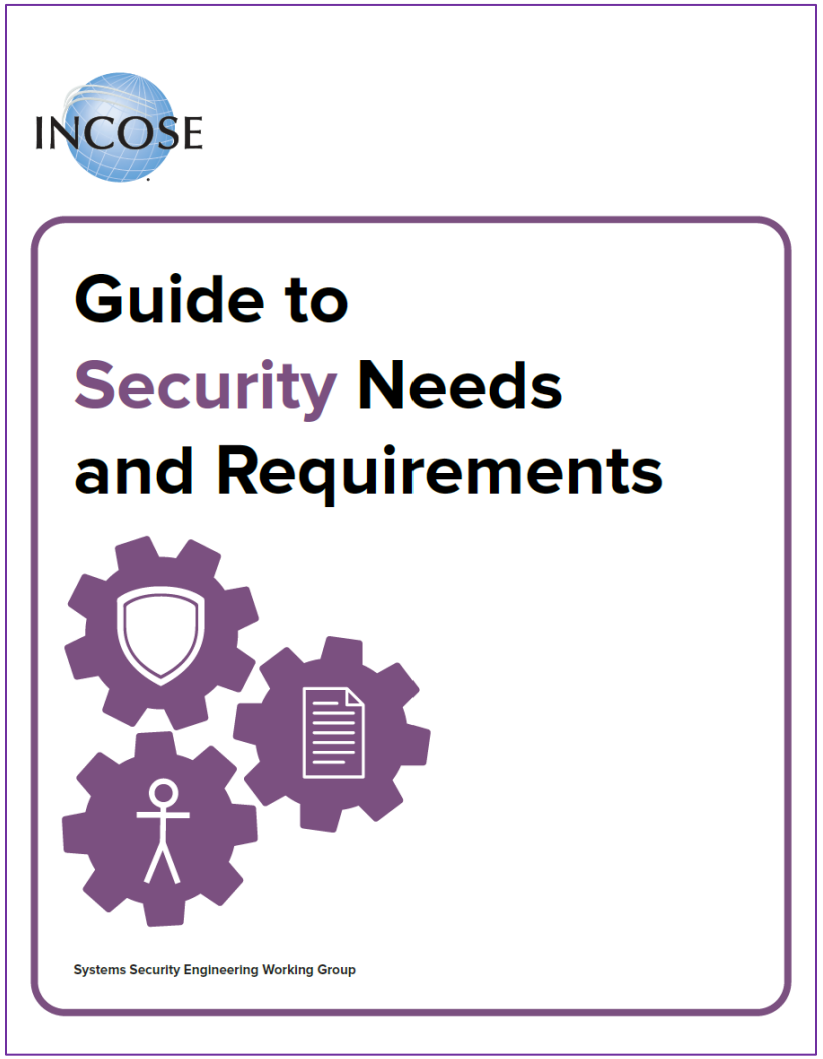
Desired Pattern

Needs	Loss-driven analysis
Requirements	Security is a functional requirement
Design	Identify security gaps in mission threads
Verification	Confirm capabilities to mitigate loss scenarios
Operational System	Mission success



- **Mental model:** Needs-oriented, loss-driven, capability-based analysis
- **Mental model**: Systems engineers work with systems security practitioners

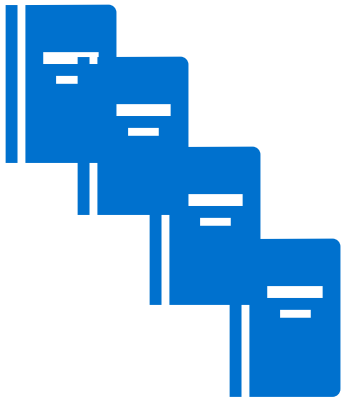
Joint SSWG/RWG Project



- **October 2022 Kickoff**
- **Anti-Patterns → Desired Pattern**
  - Anti-patterns for security
    (what we don't want because it isn't working)
  - Needs-oriented, loss-driven, capability-based analysis
    (what we want)
- **Domain-Specific Guide Format Experiments**
  1. Stand-alone security implementation of NRVV
  2. "Rosetta Stone" translation of NRVV to security
  3. Security focus for NRVV terms
- **August 2024 Publication**

Stand-Alone Guide

- **Approach:** Separate and standalone guides
  - Security (map NIST 800-160 to RWG products)
  - SoS (map ISO/IEC/IEEE 21840 to RWG products)
- **Rejected**
  - Would run hundreds of pages, duplicating RWG products and process standards
  - Target SS practitioners only (SE read RWG guides, SSE read SSWG guide)



Needs and Requirements Manual
Guide to Needs and Requirements
Guide to Writing Requirements
Guide to Verification and Validation

NIST SP 800-160

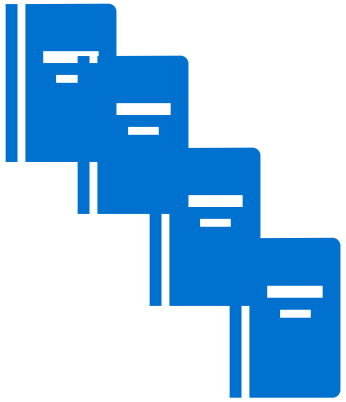
Boat Anchor

“Rosetta Stone” Translation

- **Approach:** Translate NRVV terms (help SSE see themselves in RWG guides)

NRVV Term	Security Term	SoS Term
Need Statement	Protection Need	Capability Objective

- **Rejected**
  - Still targets only SS practitioners (SE read RWG guide, SSE read guide and translator)
  - Would require a lot of work to “translate” and likely lead to more confusion



Needs and Requirements Manual
Guide to Needs and Requirements
Guide to Writing Requirements
Guide to Verification and Validation

Translation Guide

A lot of work leading to confusion

Security Focus for NRVV Terms

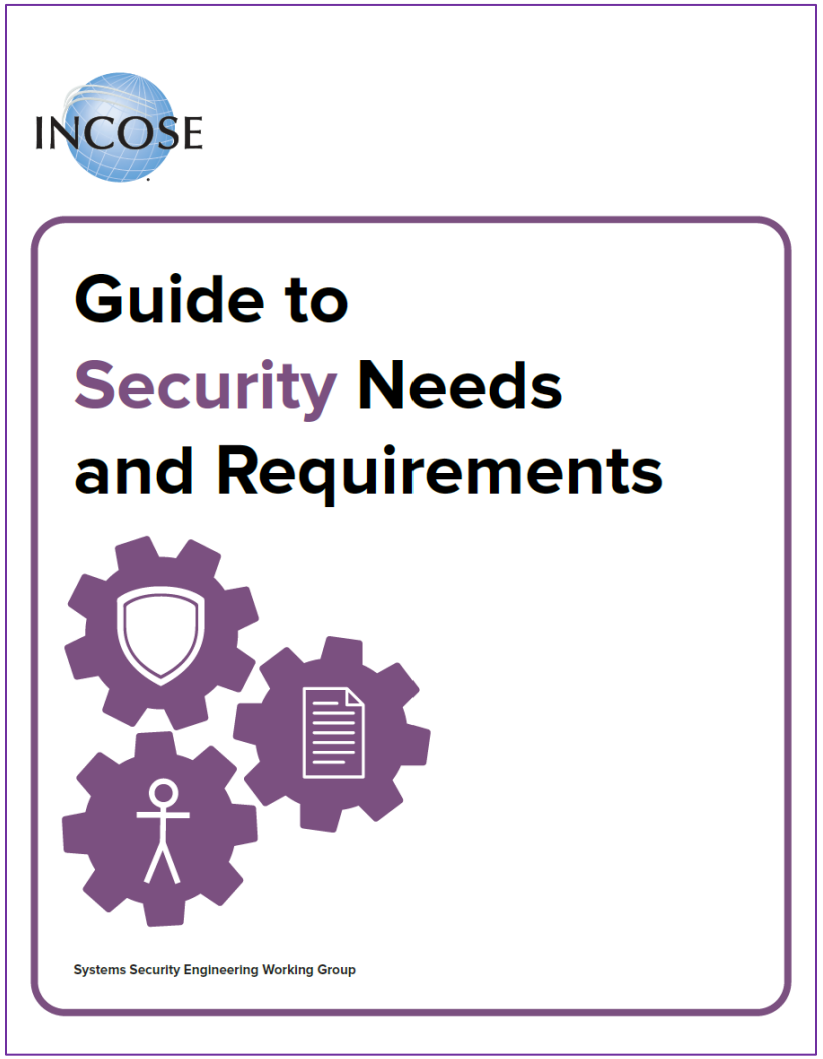
- **Approach:** Explain domain-specific focus of NRVV terms
- **Result**: 26-page document targeting both SE and SSE practitioners

NRVV Term: *Need Statements*
Formal textual statements of expectations for an entity stated in a structured, natural language from the perspective of what the stakeholders need a SOI to do, communicated at a level of abstraction appropriate to the level at which the entity exists.

Security Focus:
A protection need is an "informal statement or expression of the stakeholder security requirements focused on protection of information, systems, and services associated with mission and business functions through the system lifecycle." (Ross, McEvilley, & Winstead, 2022) Looking from a security perspective, soliciting needs for security capabilities, qualities, or attributes as early as possible in the engineering process presents the earliest opportunity to integrate security into the SOI's lifecycle, and best allows for the least costly integration of security requirements into the SOI.
The loss-driven lifecycle concepts and needs analysis to identify these protection needs and concepts for addressing those needs involves identifying the capabilities, features, and functionality required to fulfill system objectives and safeguard the assets necessary to achieve those objectives. One should also consider potential barriers to the SOI meeting its objectives. For instance, would the SOI fail to meet any of its objectives if it lost one or more of its functions or those functions failed to behave as intended? The loss-informed needs approach should extend beyond the scope of the system's purpose or mission. It should consider what the system needs to do today and, in the future, to help determine if any of the SOI's objectives would be negatively affected due to loss of certain assets or capabilities.

TABLE OF CONTENTS

Joint SSWG/RWG Project



- **October 2022 Kickoff**
- **Anti-Patterns → Desired Pattern**
  - Anti-patterns for security
    (what we don't want because it isn't working)
  - Needs-oriented, loss-driven, capability-based analysis
    (what we want)
- **Domain-Specific Guide Format Experiments**
  1. Stand-alone security implementation of NRVV
  2. "Rosetta Stone" translation of NRVV to security
  3. Security focus for NRVV terms
- **August 2024 Publication**

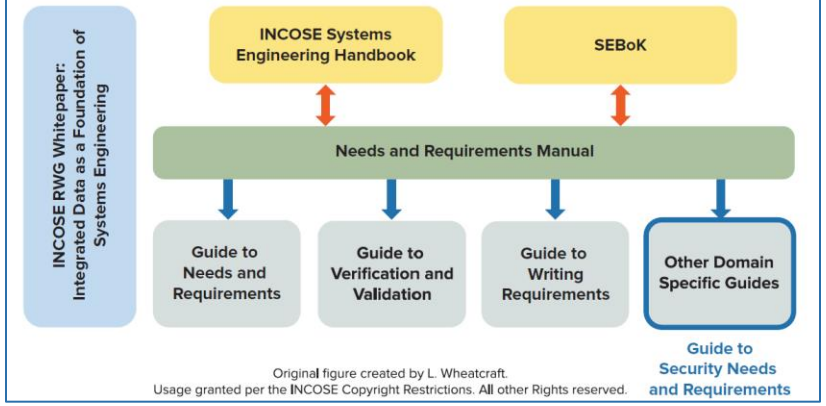
Introduction

1 INTRODUCTION

Needs and requirements form the backbone of the systems engineering information model of the System of Interest (SOI) being developed. The system security of the SOI results from a needs-oriented, loss-driven, capability-based set of need statements concerning the stakeholder expectations concerning security and a set of requirements statements about what the system must do to address those needs. Stakeholders often have difficulty describing their security needs and requirements.

The Requirements Working Group (RWG) has developed a portfolio of technical products that guide the development, articulation, verification, and validation of needs and requirements throughout the SOI lifecycle. The goal of this guide is to answer the question: "How can these products be used for the definition of systems security needs and requirements?"

As shown in Figure 1, this guide is one of the "Other Domain Specific Guides" that aligns, reinforces, and elaborates the concepts and activities defined within the other RWG products shown. This guide will provide a mapping of terms so that the System Security practitioner can relate to the RWG products and adapt the guidance in these products to security needs and requirements. The Systems Engineer (SE) practitioner working with the System Security practitioner can use this guide to better define security needs and requirements. This guide focuses on translating the Guide to Writing Requirements (GtWR) (INCOSE GtWR, 2023) which references the Needs and Requirements Manual (NRM) (INCOSE NRM, 2022) to apply to security needs and requirements.



- SSE practitioner can use the guide to better understand RWG products and adapt their guidance on security needs and requirements
- SE practitioner working with SSE can use the guide to better define security needs and requirements

Security View of NRVV

- Identifies shortfalls of defining security requirements as non-functional requirements
- Describes needs-oriented, loss-driven, capability-based approach
- Show example for NFR “system shall store data securely”

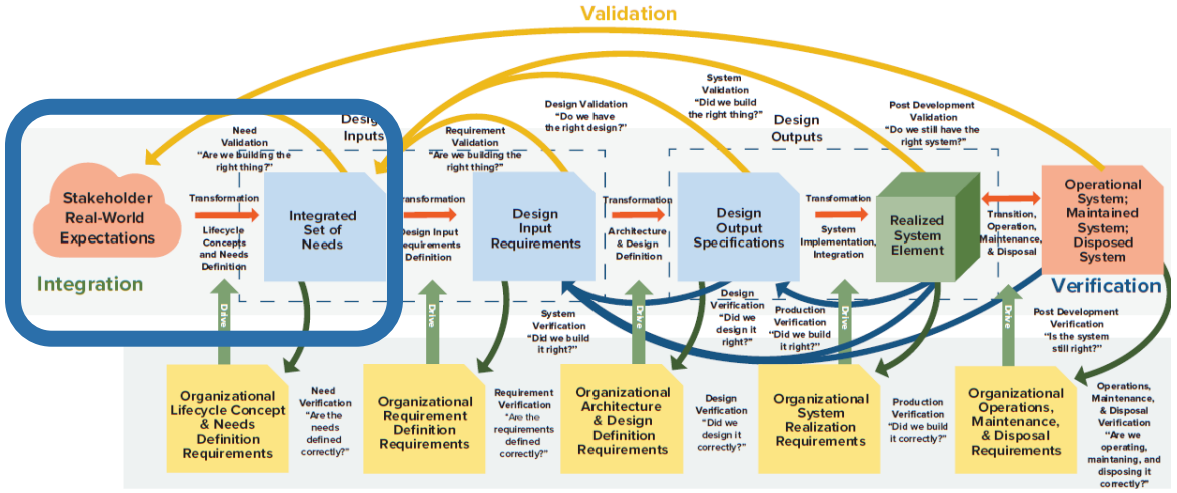
- **Example initial stakeholder security need:** *“The [stakeholders/users] need the SOI to protect Personally Identifiable Information (PII) data.”*
- **Example resulting need after lifecycle analysis and needs definition:** *“The [stakeholders/users] need the SOI to allow only Authorized Users access to Personally Identifiable Information (PII) data.”*
- **Example Resulting Design Input Requirements:** Two example design input requirements that may be elaborated from the above need statement: *“The [SOI] shall encrypt PII data stored within the SOI.” and “The [SOI] shall restrict access to PII data to Authorized Users only.”*

Lifecycle Concepts and Needs Analysis

- Relate need statements to protection needs
- Define security needs by developing loss scenarios, assurance cases, and misuse cases
- Define security focus for NRVV terms:
  - Lifecycle concepts and needs analysis
  - Need statements
  - Integrated set of needs
  - Needs (statement) verification
  - Needs (statement) validation

Need statement template:

[The SOI or stakeholders/users]
need [protection need]
to ensure [objective]
in the event of [potential loss scenario].

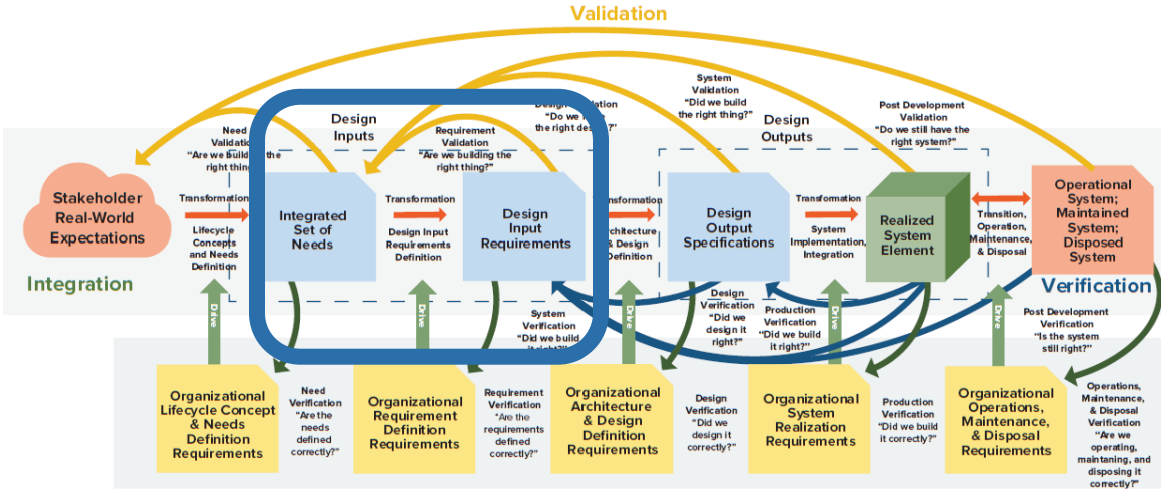


Needs to Requirements Transformation

- Translate protection needs into system capabilities to be provided by system to prevent loss scenarios
- Define security capabilities as functional requirements
- Define security focus for NRVV terms:
  - Design input requirements
  - Design input requirements definition
  - Requirements (statement) verification
  - Requirements (statement) validation

Requirements (statement) verification:
RWG Guide to Writing Requirements

Requirements (statement) validation:
Ensure that tactics support security strategies
Planned techniques will implement these tactics



Requirements Analysis

- Transform black (opaque) box to white (transparent) box including architecture definition
- Transition from *what* to protect to *how* to protect
- Define security focus for NRVV terms:
  - Architecture and design definition
  - Design output specification

Passive security functions

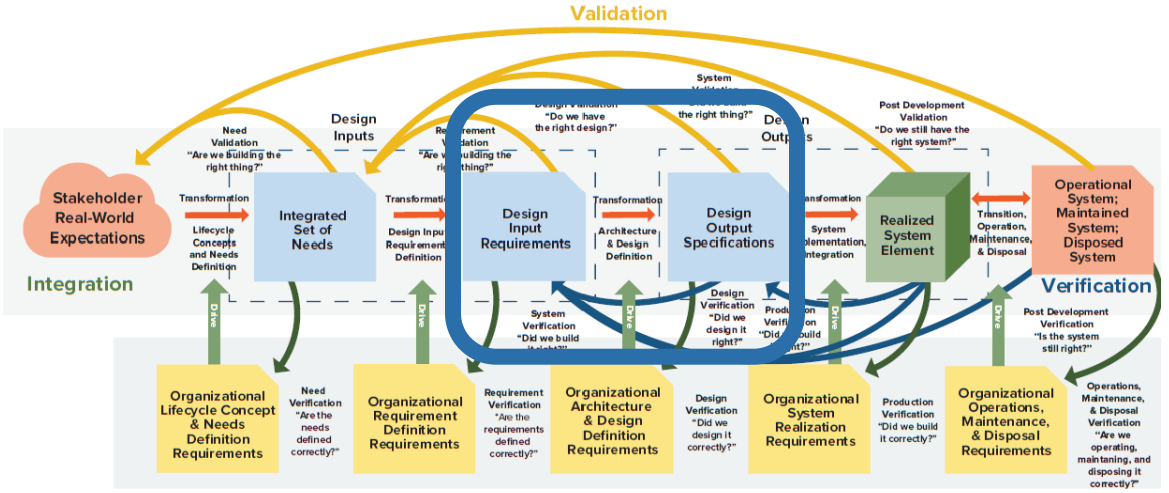
(do not exhibit behavior)

represented as structure constructs

Active security functions

(exhibit behavior)

represented by functional constructs

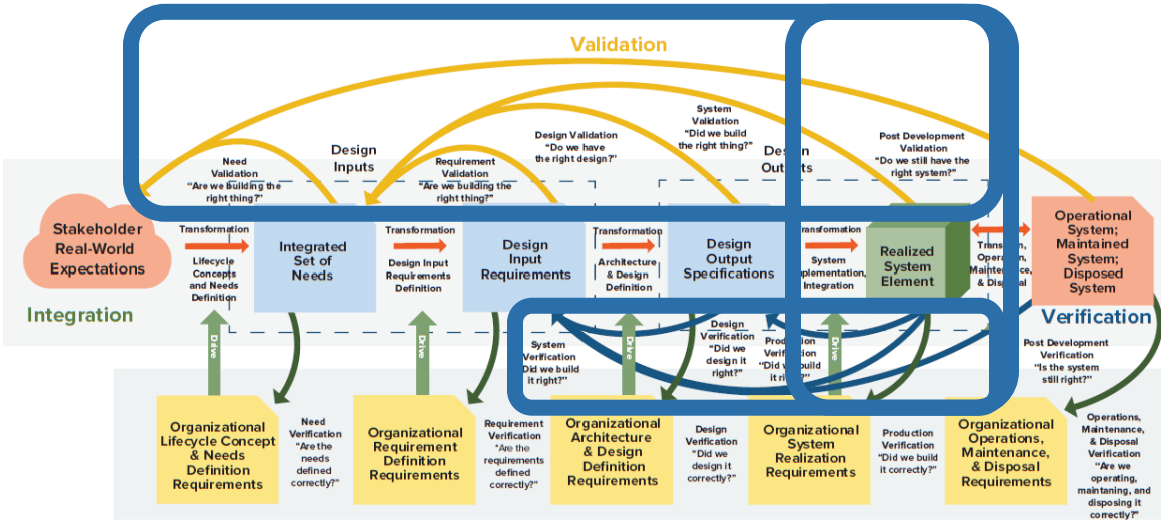


Design/System Verification/Validation

- Requirements Verification
- Needs Validation
- Define security focus for NRVV terms:
  - Design verification
  - Design validation
  - Production verification
  - System verification
  - System validation

Ensure that system test scenarios successfully accomplish loss scenarios

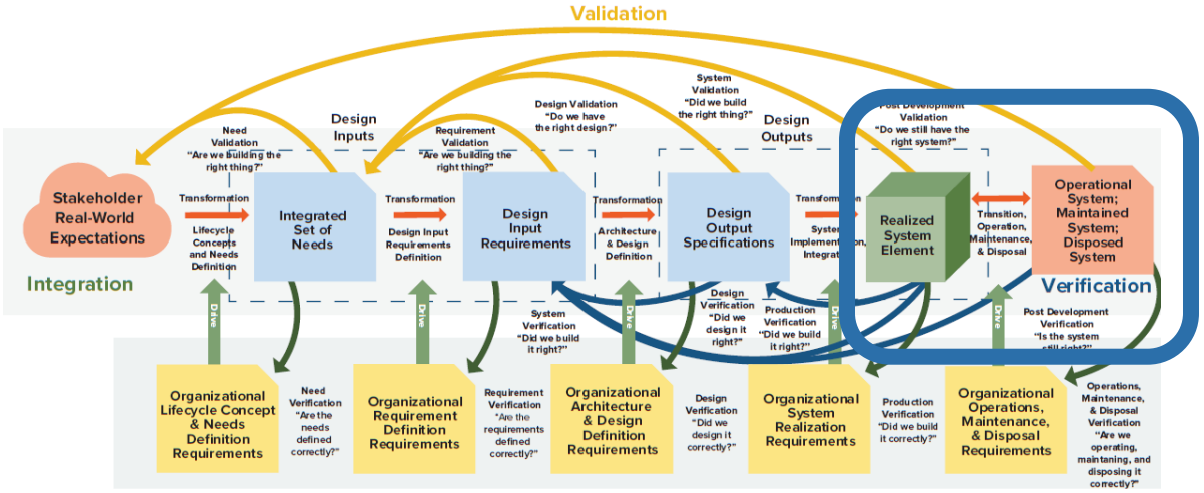
Ensure that security tactics satisfy security strategies



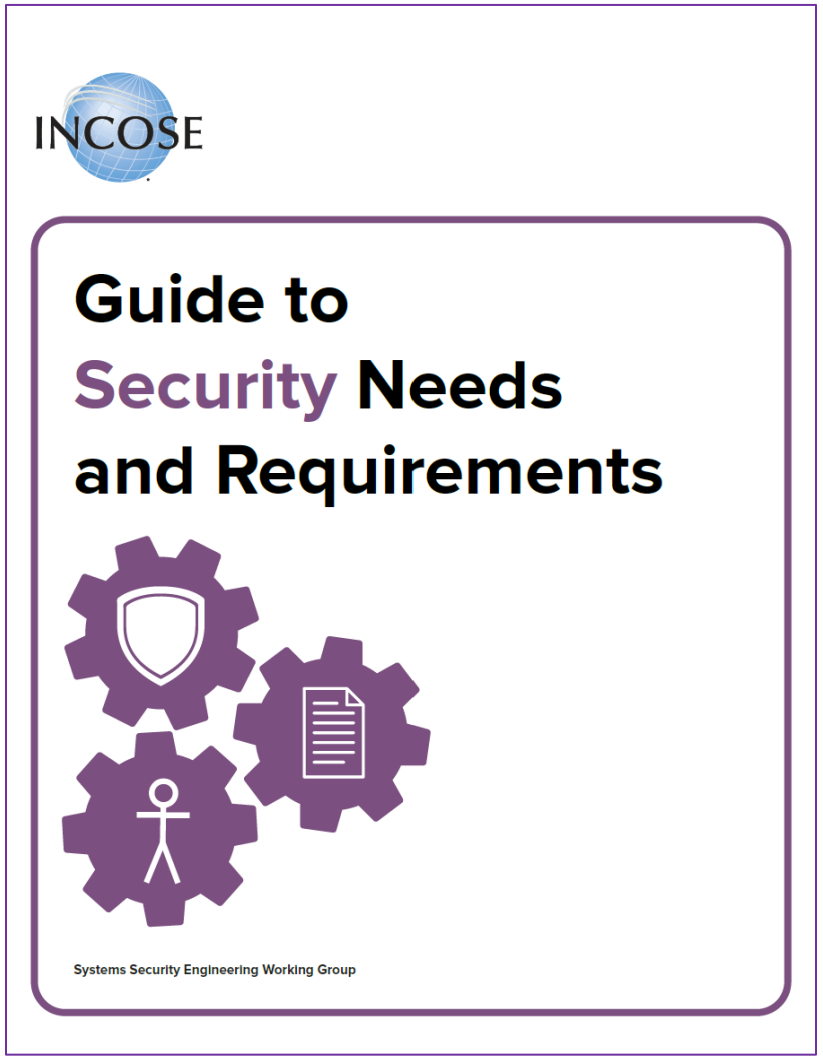
Post Development Verification/Validation

- Achieve sustainable security to enable continuous secure operation
- Confirm that loss-driven scenarios remain relevant
- Confirm that security strategy is sustainable

Use loss-driven,
capability-based analysis
to intentionally design systems that
achieve sustainable security



Summary



- GtSNR result of RWG/SSWG collaboration
- Perform needs-oriented, loss-driven, capability-based analysis across NRVV concept activities
- Define security as a functional requirement
- Format is basis for other domain-specific guides

Promote collaborative effort of SE and SSE
to design a system that can
protect from, react to, and recover from adversity
to achieve and sustain mission success