The Evolution Path to Version 0.75 of the Proposed INCOSE Competency Framework

Don S. Gelosh, Ph.D., CSEP-Acq

Director, Systems Engineering Programs

Worcester Polytechnic Institute

29 October 2015

Background

- The NDIA SE Division's Education and Training (E&T) Committee is conducting this project in collaboration with the INCOSE Competency Working Group (CWG) to develop a common approach to the definition of an overall SE Competency Framework.

- This presentation will describe the plan to evolve the Competency Framework to the next stage: Version 0.75.

E&T/CWG Leadership Team

John R. Snoderly

Defense Acquisition University

Ft. Belvoir, VA

Ken Nidiffer

Software Engineering Institute

Pittsburgh, PA

Mimi Heisey

Lockheed Martin Corporation

Manassas, VA

Outline of the Plan

- We plan to add a category called: **Enterprise**

- We plan to **align** the proposed framework with a number of other initiatives such as:

  - DoD Better Buying Power 3.0

  - Defense Acquisition University Competency Model and Acquisition Workforce Qualification Initiative

  - US Navy's Systems Engineering Competency Career Model (SECCM)

  - New INCOSE Systems Engineering Handbook V 4.0 and Systems Engineering Professional Program

- We plan to develop an initial draft **Role Definition Guide** that describes the typical roles that systems engineers may assume.

- We plan to develop **example competency models** for Systems Security Engineering, Power and Energy Systems, Transportation Systems, and Health Care Systems.

INCOSE SE Role-Based Competency Framework

INCOSE SE Role-Based Competency Framework Taxonomy

SE Role	A collection of interrelated and interdependent activities assigned to a person in a contextual environment such as Systems Engineering
Activity	A specified pursuit defined by a set of essential functions and desired outcomes that enable the successful accomplishment of one's role
Category	A grouping of closely related competencies considered essential to an individual's ability to successfully perform an activity
Competency	An observable and measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to successfully perform an activity
Description and Why It Matters	A depiction of the competency that clearly defines its essential function, desired outcomes and reasons for why the competency is needed
Knowledge Skills Abilities Behaviors	The measurable characteristics of proficiency that make up a competency

- Current Categories (Version 0.5):
  - Technical Processes
  - Technical Management
  - Analytical
  - Professional

- New Category (Version 0.75) – **Enterprise**
  - Innovation/Creativity
  - Systems Thinking & System Dynamics
  - Business Knowledge
  - Technical Basis for Cost
  - Portfolio Management
  - System of Systems Management
  - Strategy
  - Quality Management
  - Technical Workforce Development & Management

INCOSE SE Role-Based Competency Framework Architecture

- Knowledge, Skills, Abilities, and Behaviors can be acquired through Education, Training, Experiences, and Cultural Immersion.

- Five Levels of Proficiency:

  - Awareness

  - Supervised Practitioner

  - Practitioner

  - Senior Practitioner *(Proposed New Level)*

  - Expert

- This architecture approach allows us to map any SE Role into a set of clearly defined knowledge, skills, abilities and behaviors at the appropriate levels of proficiency.

Competency Framework Table

Systems Engineering Competency Framework				
Role – Title of the Role				
Role Description: explains the role and provides meaning to the role				
Why it matters: indicates the importance and value of the role and the problems that may be encountered in the absence of that role				
List of Activities	**Activity Description**	**Category**	**Competency**	**Recommended Proficiency Level**
Name of the activity	Explains the activity, the value of the activity and how it supports the role.	Technical Processes	Competency Title	Proficiency Level
			Competency Title	Proficiency Level
		Technical Management	Competency Title	Proficiency Level
			Competency Title	Proficiency Level
		Analytical	Competency Title	Proficiency Level
			Competency Title	Proficiency Level
		Professional	Competency Title	Proficiency Level
			Competency Title	Proficiency Level
Name of the activity	Explains the activity, the value of the activity and	Technical Processes	Competency Title	Proficiency Level

Proficiency Level Table

Systems Engineering Competency Model - Proficiency Level Table				
COMPETENCY AREA – Category: Competency				
Description: explains the competency and provides meaning behind the title.				
Why it matters: indicates the importance of the competency and the problems that may be encountered in the absence of that competency.				
EFFECTIVE INDICATORS OF KNOWLEDGE, SKILLS, ABILITIES AND EXPERIENCE				
AWARENESS	**SUPERVISED PRACTITIONER**	**PRACTITIONER**	**SENIOR PRACTITIONER**	**EXPERT**
The person is able to understand the key issues and their implications. They are able to ask relevant and constructive questions on the subject.	The person displays an understanding of the subject but requires guidance and supervision.	The person displays detailed knowledge of the subject and is capable of providing guidance and advice to others.	The person displays both in-depth and broad knowledge of the subject based on practical experience. The person is capable of leading others to create and evaluate solutions to complex problems in the subject.	The person displays extensive and substantial practical experience and applied knowledge of the subject.

Seeking Alignments

Better Buying Power 3.0

Improve the Professionalism of the Total Acquisition Workforce

- Establish higher standards for key leadership positions
- **Establish stronger professional qualification requirements for all acquisition specialties**
- Strengthen organic engineering capabilities
- Ensure development program leadership is technically qualified to manage R&D activities
- Improve our leaders' ability to understand and mitigate technical risk
- Increase DoD support for STEM education

Acquisition Workforce Qualification Initiative

1. Establish higher standards for key leadership positions

2. **Establish increased professional qualification requirements for all acquisition specialties**

3. Increase the recognition and support of excellence in acquisition management

4. Continue to increase the cost consciousness of the acquisition workforce – change the culture

Defense Acquisition University Engineering Competency Model

Analytical:
- Mission-Level Assessment
- Stakeholder Requirements Definition
- Requirements Analysis
- Architecture Design
- Implementation
- Integration
- Verification
- Validation
- Transition
- Design Considerations
- Tools and Techniques
- Technical Management
- Decision Analysis
- Technical Planning
- Technical Assessment
- Configuration Management
- Requirements Management
- Risk Management
- Data Management
- Interface Management
- Software Engineering Management
- Acquisition

Business Acumen:
- Industry Landscape
- Organization
- Cost, Pricing, and Rates
- Cost Estimating
- Financial Reporting and Metrics
- Business Strategy
- Capture Planning and Proposal Process
- Supplier Management
- Industry Motivation, Incentives, Rewards
- Negotiations

Professional:
- Problem Solving
- Strategic Thinking
- Professional Ethics
- Leading High-Performance Teams
- Communication
- Coaching and Mentoring
- Managing Stakeholders
- Mission and Results Focus
- Personal Effectiveness/Peer Interaction
- Sound Judgment

US Navy's Systems Engineering Competency Career Model (SECCM)

Technical Processes:
- Architecture Definition
- Implementation
- Integration
- Integration of Specialisms
- Systems Requirement Definition
- Transition
- Validation
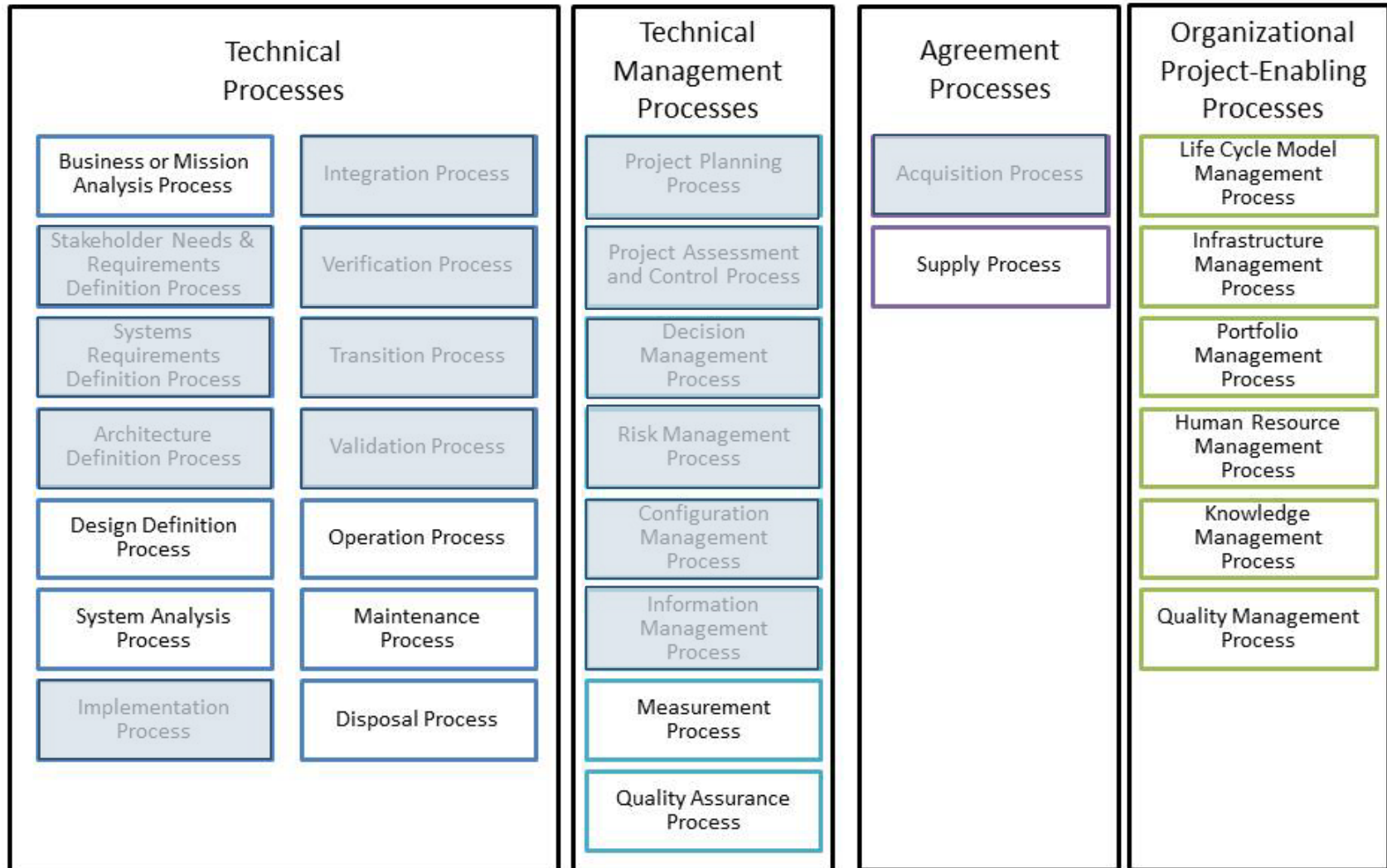- Verification

Analytical:
- Design Considerations/Specialty Engineering
- Engineering & Scientific Fundamentals
- Mathematics/Logic/Quantitative Analysis
- Modeling and Simulation
- Reliability, Maintainability and Availability Analysis
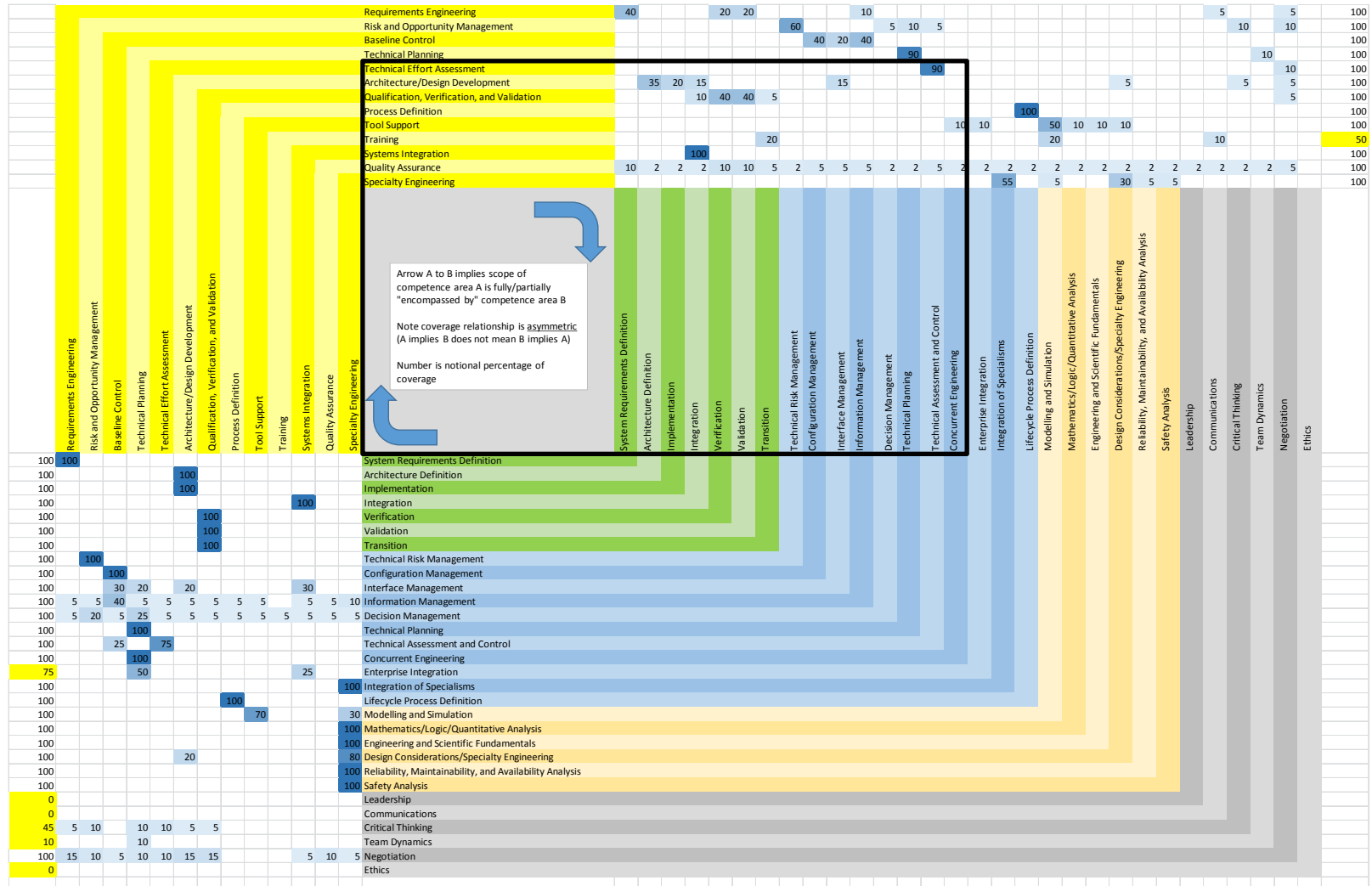
Technical Management:
- Concurrent Engineering
- Configuration Management
- Enterprise Integration
- Interface Management
- Information Management
- Lifecycle Process Definition
- Technical Assessment and Control
- Technical Planning
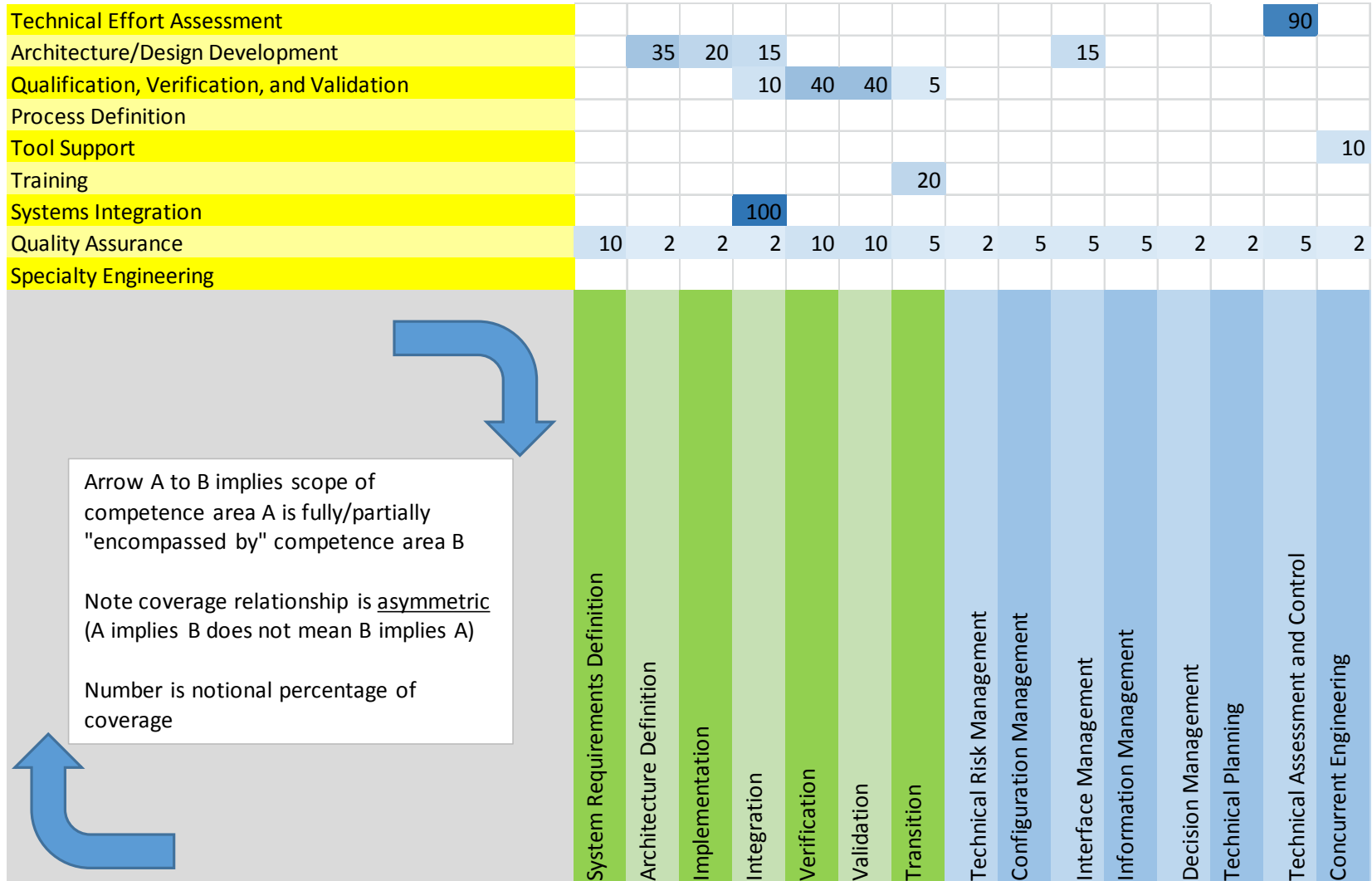- Technical Risk Management

Professional:
- Communication
- Critical Thinking
- Ethics
- Leadership
- Negotiations
- Team Dynamics

New INCOSE Systems Engineering Handbook V 4.0

Technical Processes

- Business or Mission Analysis Process
- Stakeholder Needs & Requirements Definition Process
- Systems Requirements Definition Process
- Architecture Definition Process
- Design Definition Process
- System Analysis Process
- Implementation Process
- Integration Process
- Verification Process
- Transition Process
- Validation Process
- Operation Process
- Maintenance Process
- Disposal Process

Technical Management Processes

- Project Planning Process
- Project Assessment and Control Process
- Decision Management Process
- Risk Management Process
- Configuration Management Process
- Information Management Process
- Measurement Process
- Quality Assurance Process

Agreement Processes

- Acquisition Process
- Supply Process

Organizational Project-Enabling Processes

- Life Cycle Model Management Process
- Infrastructure Management Process
- Portfolio Management Process
- Human Resource Management Process
- Knowledge Management Process
- Quality Management Process

Source: ISO/IEC/IEEE 15288 & INCOSE SE Handbook, 4th Ed. 2015

	System Requirements Definition	Architecture Definition	Implementation	Integration	Verification	Validation	Transition	Technical Risk Management	Configuration Management	Interface Management	Information Management	Decision Management	Technical Planning	Technical Assessment and Control	Concurrent Engineering
Technical Effort Assessment														90	
Architecture/Design Development		35	20	15						15					
Qualification, Verification, and Validation				10	40	40	5								
Process Definition															
Tool Support															10
Training							20								
Systems Integration				100											
Quality Assurance	10	2	2	2	10	10	5	2	5	5	5	2	2	5	2
Specialty Engineering															

Arrow A to B implies scope of competence area A is fully/partially "encompassed by" competence area B

Note coverage relationship is asymmetric (A implies B does not mean B implies A)

Number is notional percentage of coverage

Initial Draft Role Definition Guide

- Purpose is to describe how to use the INCOSE Competency Framework to create generic role statements, thus embedding Systems Engineering competencies into the people that make up the enterprise.

- Role statements can be considered the "requirements" for the individuals (components) who make up the enterprise (the system).

- A role statement must be a combination of describing what the role does (activities) and the competencies (knowledge, skills, abilities & behaviors) that the individual needs to perform the activities.

- This document is only a guide – the definitions of Systems Engineering roles must be consistent with the HR policies of the organization.

Example Competency Models

- Systems Security Engineering – In Progress

- Power and Energy Systems

- Transportation Systems

- Health Care Systems

Next Steps

More Work to V0.75

- Need to Coordinate and Align with:

    - INCOSE Professional Development Initiative

    - Systems Engineering Research Center's Helix Study

    - INCOSE Vision 2025 Roles and Competencies

    - Systems Engineering Body of Knowledge (SEBoK Part 5)

    - Information Technology Body of Knowledge (ITBoK)

Future Work to V1.0

- Need to Coordinate and Align with:
  - INCOSE PMI Working Group
  - Other models (i.e., CMMI, etc.) and how they may impact the framework

- Develop Use Cases

- Develop an Assessment Methodology
  - Consider how to support an Individual / Supervisor Assessment of Competence

- Examine competencies outside traditional SE to provide breadth

- Include foundational systems principles

Questions?

Don's Contact Info

Don S. Gelosh, Ph.D., CSEP-Acq
Director, Systems Engineering Programs
Worcester Polytechnic Institute

Corporate and Professional Education

540-349-3949

dsgelosh@wpi.edu

cpe.wpi.edu

Back Up Slides

Systems Security Engineering Competency Model Examples

Systems Engineering Role-Based Competency Model

Role – System Security Engineering

Role Description: System Security Engineering (SSE) is a specialty engineering discipline within Systems Engineering (SE) focused on ensuring a system can function under disruptive conditions associated with misuse and malicious behavior. SSE involves a disciplined application of SE principles in analyzing threats and vulnerabilities to systems and assessing and mitigating risk to the information assets of the system during its lifecycle. It applies a blend of technology, management principles and practices, and operational rules to ensure sufficient protections are available to the system at all times.[1]

Why it matters: Appropriate SSE activities are needed because an adversary may attempt to sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

Activity	Activity Description	Class	Competency	Recommended Proficiency Level
Cybersecurity	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.[2]	Technical Processes	Security Requirements	Senior Practitioner
			Secure Architecture Design	Expert
		Technical Management	Technical Risk Management	Senior Practitioner
			Enterprise Integration	Senior Practitioner
		Analytical	Mathematics/Logic/Quantitative Analysis	Senior Practitioner
			Reliability, Maintainability, and Availability Analysis	Senior Practitioner
		Professional	Leadership	Senior Practitioner
			Critical Thinking	Expert

---

[1] Dove, R, Popick, P, and Wilson, E. 2013. The Buck Stops Here: Systems Engineering is Responsible for System Security. Insight Theme Issue Essay Collection 16 (2). International Council on Systems Engineering, July 2013.
[2] Recommendation ITU-T X.1205 (2008), *Overview of Cybersecurity*

Systems Security Engineering Competency Model – Proficiency Level Table

COMPETENCY AREA – Security Requirements[1]

Description: Security Requirements define the *measurable* active and passive protection capability, behavior, performance, and parameters that constitute a system deemed "secure" in specific operational environments for a given set of use-cases, given the mission/business system requirements and associated constraints. Security requirements enable a balanced, secure and optimum result that considers all stakeholder requirements and the means and methods to verify and validate the system implementation.

Why it matters: Security is the "enduring state" of an operational system and is achieved by employment of protection mechanism and procedures allocated to the combination of technical, physical/environmental, and human system elements. Security requirements define the "enduring state" and how it is achieved and maintained across all system elements throughout the entire system life cycle. Security requirements are the basis for secure architecture and design, drive implementation and integration, and are the basis for continual verification and validation.

EFFECTIVE INDICATORS OF KNOWLEDGE AND EXPERIENCE

AWARENESS	SUPERVISED PRACTITIONER	PRACTITIONER	SENIOR PRACTITIONER	EXPERT
• Understands the principles, methods, and practices of stakeholder requirements definition and requirements analysis processes. • Understand the difference in stakeholder (design independent capability requirements) and system (design dependent requirements) and their relationship. • Understands the various attributes/properties that underlie protection and security across the system lifecycle. • Aware of the difference in security requirement, security policy, and	• Able to use requirements elicitation techniques to gather information to ascertain the need for protection and what constitutes being secure. • Able to transform stakeholder requirements into system design security requirements. • Able to support security requirements analysis and security requirements trade-offs. • Able to perform security requirements traceability and coverage analysis.	• Able to generate alternative sets of security requirements that satisfy the protection need using different technologies and methods. • Able to assess a range of security requirements oriented to a protection need and justify the selection of the optimum solution. • Able to define a process and appropriate tools and techniques for developing security requirements. • Able to choose appropriate requirements elicitation, analysis, and selection techniques.	• Able to help others understand security requirements development techniques, their relationship with other system quality requirements, and their appropriateness at different levels of complexity and levels of assurance. • Able to evaluate appropriate processes, tools and techniques for developing security requirements. • Has contributed to novel techniques and ideas in this field. • Able to supervise and guide practitioners.	• Can demonstrate a full understanding of security requirements, their relationship with other system quality properties, and their appropriateness, given the levels of complexity and assurance of the system of interest. • Reviews and judges the necessity, completeness, coverage, and effectiveness of the security requirements in providing protection at the level of assurance required for the system of interest. • Has coached new practitioners and senior practitioners in this field.

---

[1] Courtesy of Michael A. McEvilley.

Systems Security Engineering Competency Model – Proficiency Level Table

COMPETENCY AREA – Secure Architecture Design[1,2]

Description: Secure Architecture Design is the definition of the system architecture and derived requirements to produce a solution that is secure and can be implemented to enable a balanced, secure and optimum result that considers all stakeholder requirements. Systems security engineering, as part of the Architectural Design Process: (i) identifies and examines one or more security architectural design and implementation strategies; and (ii) identifies, minimizes, and contains the impact of vulnerabilities, taking into account susceptibility to threats and stakeholder risk tolerance.

Why it matters: Effective secure architectural design enables systems to be partitioned into realizable system elements which can be brought together to meet the requirements. A security architectural design solution that provides a sufficient level of trustworthiness is defined in terms of the security requirements for the security-relevant system elements. The protections specified by the security design requirements are iteratively refined into security specifications and security procedures from which the system is implemented, configured, operated, and maintained.

EFFECTIVE INDICATORS OF KNOWLEDGE AND EXPERIENCE

AWARENESS	SUPERVISED PRACTITIONER	PRACTITIONER	SENIOR PRACTITIONER	EXPERT
• Understands the principles of secure architectural design and its role within the lifecycle. • Aware of the different types of secure architectures. • Aware that secure architectural decisions can constrain and limit future use and evolution.	• Able to use techniques to support secure architectural design process. • Able to support secure architectural design trade-offs. • Able to contribute to alternative secure architectural designs that are traceable to the requirements. • Able to interpret a secure architectural design.	• Able to generate alternative secure architectural designs that are traceable to the requirements. • Able to assess a range of secure architectural designs and justify the selection of the optimum solution. • Able to define a process and appropriate tools and techniques for secure architectural design. • Able to choose appropriate analysis and selection techniques.	• Able to help others understand secure architectural design techniques and their appropriateness at different levels of complexity. • Able to evaluate appropriate processes, tools and techniques for secure architectural design. • Has contributed to novel techniques and ideas in this field. • Able to supervise and guide practitioners.	• Can demonstrate a full understanding of secure architectural design techniques and their appropriateness, given the levels of complexity of the system of interest. • Reviews and judges the security and suitability of security architecture designs. • Has coached new practitioners and senior practitioners in this field. • Has championed the introduction of novel techniques and ideas in this

---

[1] Derived from INCOSE UK Competency Framework, 2010.
[2] NIST Special Publication 800-160, Initial Public Draft, Systems Security Engineering: *An Integrated Approach to Building Trustworthy Resilient Systems*, May 2014.

Systems Security Engineering Competencies Model – Proficiency Level Table

COMPETENCY AREA – Software Assurance Assessment

Description: Software Assurance Assessment provides a level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner.

Why it matters: Most critical functions that support systems developed for national defense to banking to healthcare to telecommunications to aviation to control of hazardous materials depend on the correct, predictable operation of software. It is crucial to assess the software systems and determine the resultant levels of confidence. If these functions do not have the necessary level of assurance, they could be seriously disrupted and may result in loss of mission or life if the underlying software-intensive systems fail. [1]

EFFECTIVE INDICATORS OF KNOWLEDGE AND EXPERIENCE[1]

AWARENESS	SUPERVISED PRACTITIONER	PRACTITIONER	SENIOR PRACTITIONER	EXPERT
• Possesses technical knowledge and skills, typically gained through a certificate or an associate degree program, or equivalent knowledge and experience. • May be employed in a system operator, implementer, tester, or maintenance position with specific individual tasks assigned by someone at a higher level.	• Possesses application-based knowledge and skills and entry-level professional effectiveness, typically gained through a bachelor's degree in computing or through equivalent professional experience. • May manage a small internal project; supervise and assign sub-tasks; supervise and assess system operations; and implement commonly accepted assurance practices.	• Possesses breadth and depth of knowledge, skills, and effectiveness beyond Supervised Practitioner level. • Typically has two to five years of professional experience. • May set plans, tasks, and schedules for in-house projects; define and manage such projects and supervise teams on the enterprise level; report to management; assess the assurance quality of a system; implement and promote commonly accepted software assurance assessment practices.	• Possesses breadth and depth of knowledge, skills, and effectiveness and a variety of work experiences with 5 to 10 years of professional experience and advanced professional development at the master's level or with equivalent education and training. • May identify and explore effective software assurance assessment practices for implementation, manage large projects, interact with external agencies, and so forth.	• Possesses breadth and depth of knowledge, skills, and effectiveness beyond Senior Practitioner. • Advances the field by developing, modifying, and creating methods, practices, and principles at the organizational level or higher. • Has peer/industry recognition indicated by a nice paperweight. • Typically includes a low percentage of an organization's workforce within the SwA profession (e.g., 2 % or less).

[1] Derived from Karen Mercedes, Theodore Winograd, "Enhancing The Development Life Cycle To Produce Secure Software", Data & Analysis Center for Software, October 2008.

Proposed Evolution

We propose a evolution of the current INCOSE UK Competencies Framework along four paths of development and growth:

1. Evolve to an SE role-based competency framework that is extensible, scalable, and tailorable by the customer organization.

2. Evolve by adding the concept of classes. This is where the competencies achieve their interdependence with each other.

3. Evolve by ensuring there is a Professional Class that covers leadership and soft skill competencies.

4. Evolve by adding a new level of proficiency called the Senior Practitioner to the existing four levels in the INCOSE UK Competencies Framework.

Category Definitions (V 0.5 & 0.75)

- **Technical Processes** – competencies required to perform fundamental SE activities

- **Technical Management** – competencies required to plan, assess and control the technical effort

- **Analytical** – competencies required to develop inputs for decisions or to inform fundamental SE activities

- **Professional** – non-technical competencies required to enable systems engineers to effectively and efficiently achieve objectives in the organizational context

- **Enterprise** – high level competencies that impact all aspects of SE

Current Proficiency Levels

- **Awareness Level:**

  - *The person is able to understand the key issues and their implications. They are able to ask relevant and constructive questions on the subject.*

- **Supervised Practitioner Level:**

  - *The person displays an understanding of the subject but requires guidance and supervision.*

- **Practitioner Level:**

  - *The person displays detailed knowledge of the subject and is capable of providing guidance and advice to others.*

Source: INCOSE UK Competencies Framework (INCOSE UK, 2010)

Current Proficiency Levels

- **Senior Practitioner Level *(Proposed New Level):***

  - *The person displays both in-depth and broad knowledge of the subject based on practical experience and is capable of leading others to create and evaluate solutions to complex problems in the subject.*

- **Expert Level:**

  - *The person displays extensive and substantial practical experience and applied knowledge of the subject.*

Source: INCOSE UK Competencies Framework (INCOSE UK, 2010)

Senior Practitioner Proficiency Level

- **Those who achieve Senior Practitioner Level would have:**

  - An in-depth and broad knowledge of the particular SE competency

  - Ability to lead others in solving complex problems utilizing the competency

- **Senior Practitioner Level provides a bridge that makes it easier to transition from the Practitioner level to the Expert level.**

Source: INCOSE UK Competencies Framework (INCOSE UK, 2010)