27th annual INCOSE international symposium

Adelaide, Australia

July 15 - 20, 2017

ENGINEERS AUSTRALIA SESA

Systems Security Engineering: What Every System Engineer Needs to Know

INCOSE IS 2017

Mr Ed Yakabovicz,
Northrop Grumman
Edward.yakabovicz@ngc.com

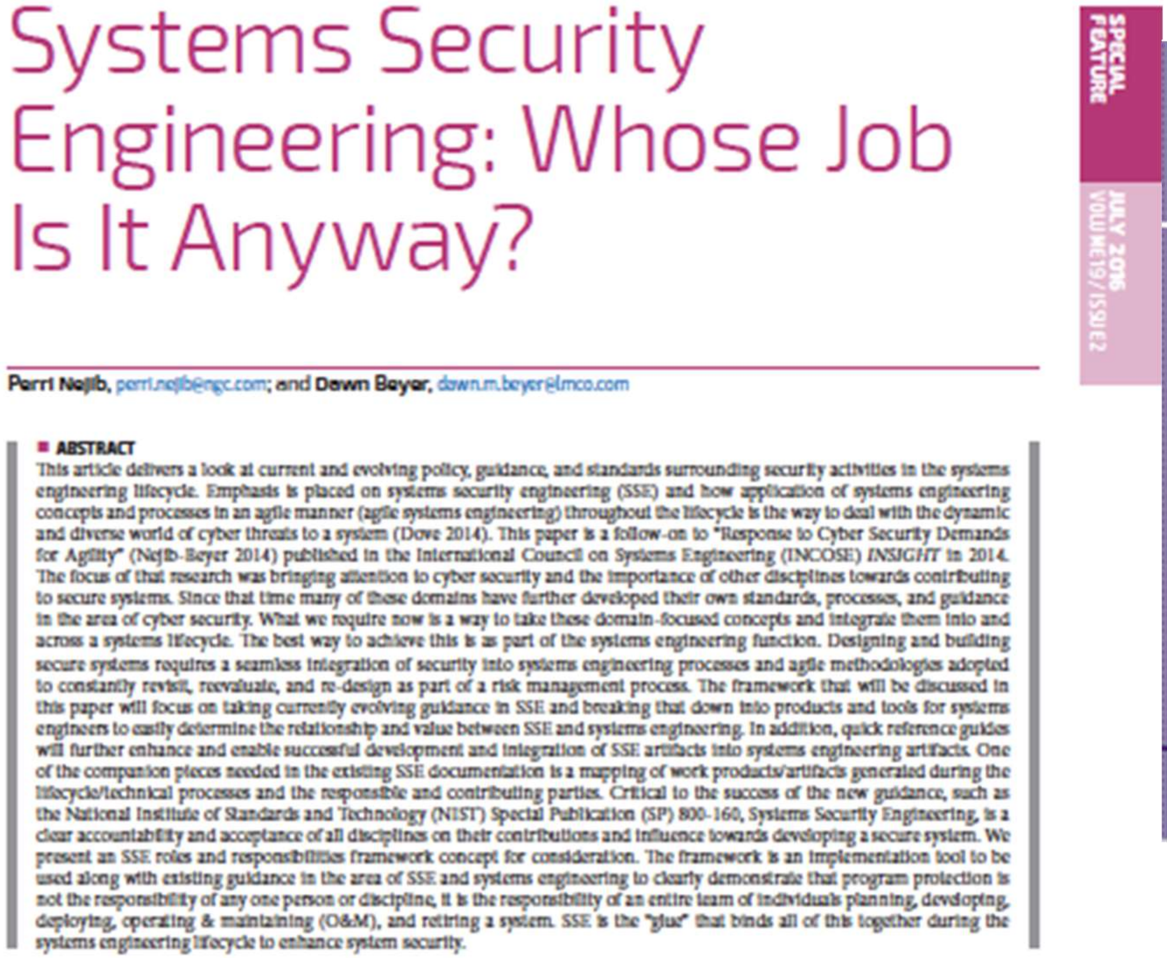
Ms Perri Nejib, Tech Fellow,
Northrop Grumman
perri.nejib@ngc.com

Dr Dawn Beyer, Sr Fellow,
Lockheed Martin
dawn.m.beyer@lmco.com

www.incose.org/symp2017

Approved For Public Release #17-1081 Unlimited Distribution, Dated 5/22/17

Cybersecurity is *EVERYONE's* Job



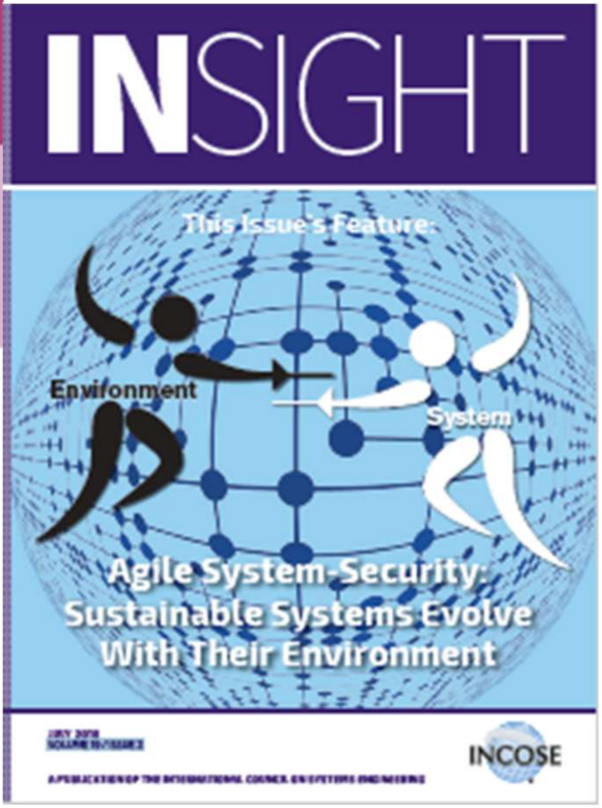
SPECIAL FEATURE

JULY 2016
VOLUME 19 / ISSUE 2

Systems Security Engineering: Whose Job Is It Anyway?

Perri Nejib, perri.nejib@ngc.com; and Dawn Beyer, dawn.m.beyer@lmco.com

■ **ABSTRACT**
This article delivers a look at current and evolving policy, guidance, and standards surrounding security activities in the systems engineering lifecycle. Emphasis is placed on systems security engineering (SSE) and how application of systems engineering concepts and processes in an agile manner (agile systems engineering) throughout the lifecycle is the way to deal with the dynamic and diverse world of cyber threats to a system (Dove 2014). This paper is a follow-on to "Response to Cyber Security Demands for Agility" (Nejib-Beyer 2014) published in the International Council on Systems Engineering (INCOSE) *INSIGHT* in 2014. The focus of that research was bringing attention to cyber security and the importance of other disciplines towards contributing to secure systems. Since that time many of these domains have further developed their own standards, processes, and guidance in the area of cyber security. What we require now is a way to take these domain-focused concepts and integrate them into and across a systems lifecycle. The best way to achieve this is as part of the systems engineering function. Designing and building secure systems requires a seamless integration of security into systems engineering processes and agile methodologies adopted to constantly revisit, reevaluate, and re-design as part of a risk management process. The framework that will be discussed in this paper will focus on taking currently evolving guidance in SSE and breaking that down into products and tools for systems engineers to easily determine the relationship and value between SSE and systems engineering. In addition, quick reference guides will further enhance and enable successful development and integration of SSE artifacts into systems engineering artifacts. One of the companion pieces needed in the existing SSE documentation is a mapping of work products/artifacts generated during the lifecycle/technical processes and the responsible and contributing parties. Critical to the success of the new guidance, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160, Systems Security Engineering, is a clear accountability and acceptance of all disciplines on their contributions and influence towards developing a secure system. We present an SSE roles and responsibilities framework concept for consideration. The framework is an implementation tool to be used along with existing guidance in the area of SSE and systems engineering to clearly demonstrate that program protection is not the responsibility of any one person or discipline, it is the responsibility of an entire team of individuals planning, developing, deploying, operating & maintaining (O&M), and retiring a system. SSE is the "glue" that binds all of this together during the systems engineering lifecycle to enhance system security.



INSIGHT

This Issue's Feature:

Agile System-Security: Sustainable Systems Evolve With Their Environment

JULY 2016
VOLUME 19 / ISSUE 2

INCOSE

A PUBLICATION OF THE INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING

Integrating cybersecurity into the SE process is critical to ensuring a secure design

Recent paper published in INCOSE Insight Journal, July 2016 Volume 19 / ISSUE 2

INCOSE SSE/SE Roles & Responsibilities Framework - Origins

- Nejib/Beyer papers on agile security and SSE July 2014 and 2016, INCOSE Insight Journals
- Suggested project during INCOSE IS 2014 SSE working group session
- Timely with new SSE guidance and documents coming out from NIST and OSD (SE)
  - New specialty SSE section in INCOSE SE Handbook v4
- Need an easy reference responsibility framework to map out relationship between SSE/SE
  - Understandable by both SEs and SSEs

Approach

- Research applicable published Standards and Guidance
  - NIST 800-160
  - ISO 15288
  - INCOSE SE Handbook

These all had major updates mid 2015 and 2016

- Work focused on taking SSE activities, tasks and deliverables/artifacts and developing framework that can be used across domains and clearly defines critical artifact roles and & responsibilities within SSE and SE
- Make it clear to SEs how to integrate SSE products into related SE products and the value in doing so to manage overall program/system design and risk

The **systems security engineering** discipline provides the ***security perspective*** to the **systems engineering** processes, activities, tasks, products, and artifacts, with emphasis on system security risk management.

Project Goals

- Integrate artifact roles & responsibilities framework into current INCOSE specialty engineering section on SSE – Chapter 10
- Develop framework so that it can easily be adopted into NIST SP 800-160 and ISO 15288

Approved For Public Release #17-1081 Unlimited Distribution, Dated 5/22/17

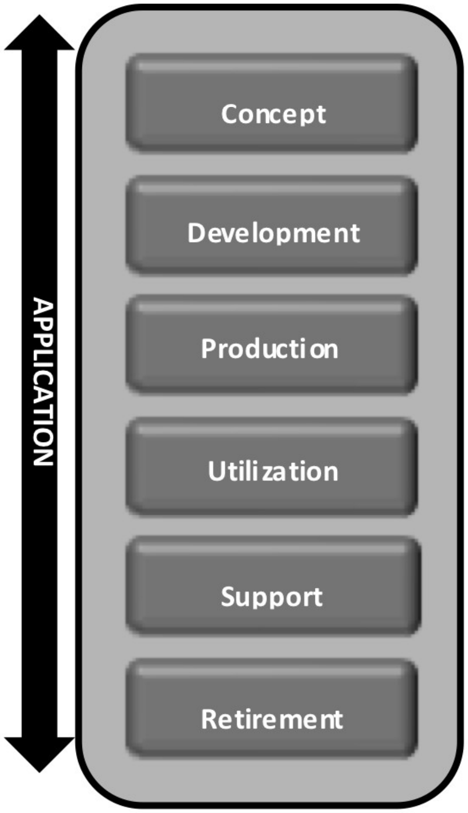
INCOSE SE Handbook & NIST SP 800-160 organized by Processes and associated Activities and Tasks

Systems Engineering Life Cycle Processes

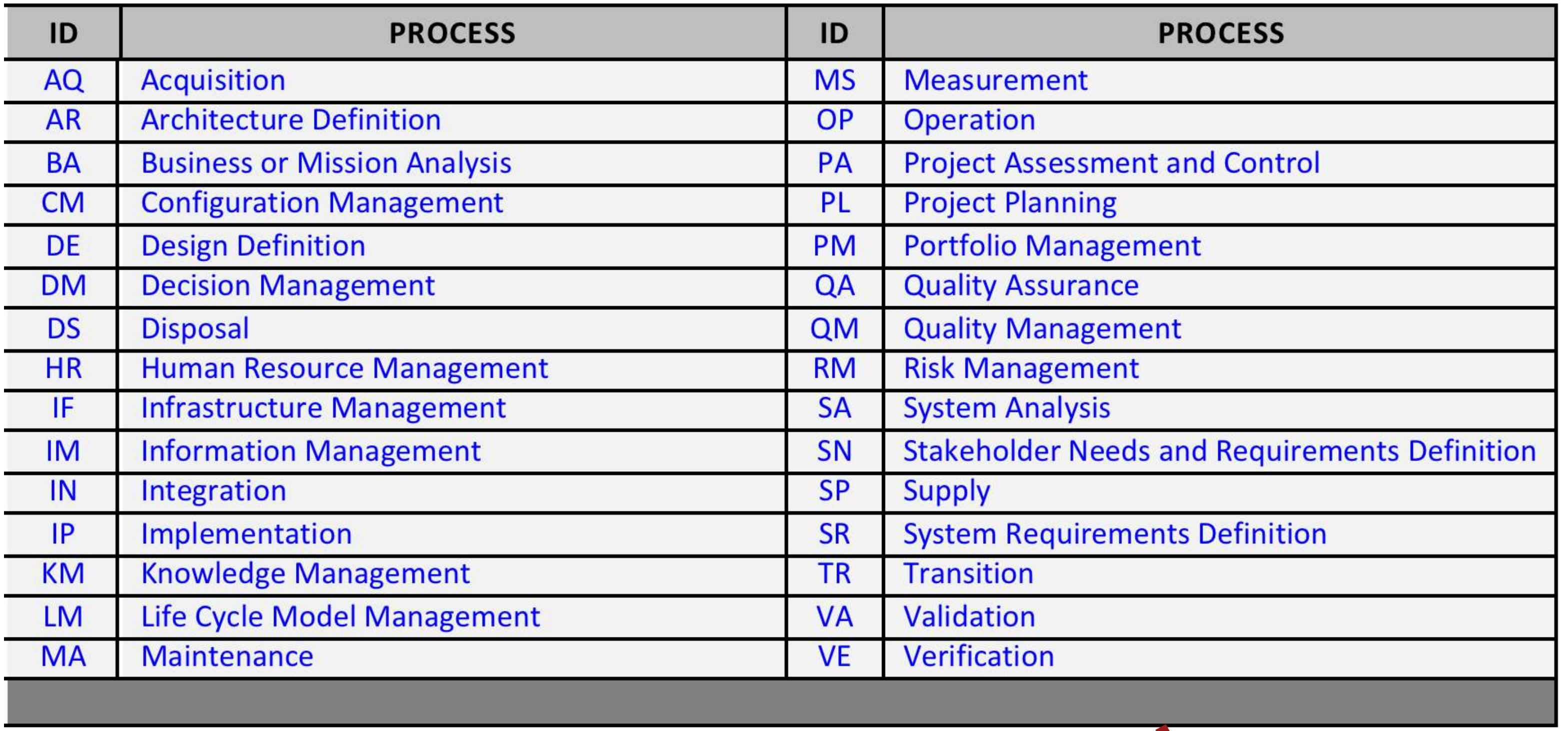
Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

Agreement Processes	Organization Project-Enabling Processes	Technical Management Processes	Technical Processes
• Acquisition • Supply	• Life Cycle Model Management • Infrastructure Management • Portfolio Management • Human Resource Management • Quality Management • Knowledge Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement • Quality Assurance	• Business or Mission Analysis • Stakeholder Needs and Requirements Definition • System Requirements Definition • Architecture Definition • Design Definition • System Analysis • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal

Life Cycle Stages

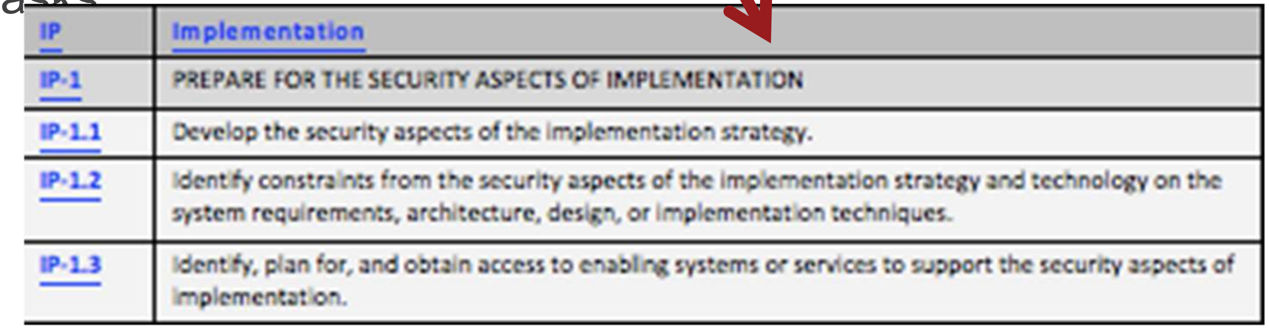


Source: *ISO/IEC/IEEE 15288: 2015*



ID	PROCESS	ID	PROCESS
AQ	Acquisition	MS	Measurement
AR	Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

NIST 800-160 broken down by ISO 15288:2015/INCOSE SE processes – expressed in security activities and tasks



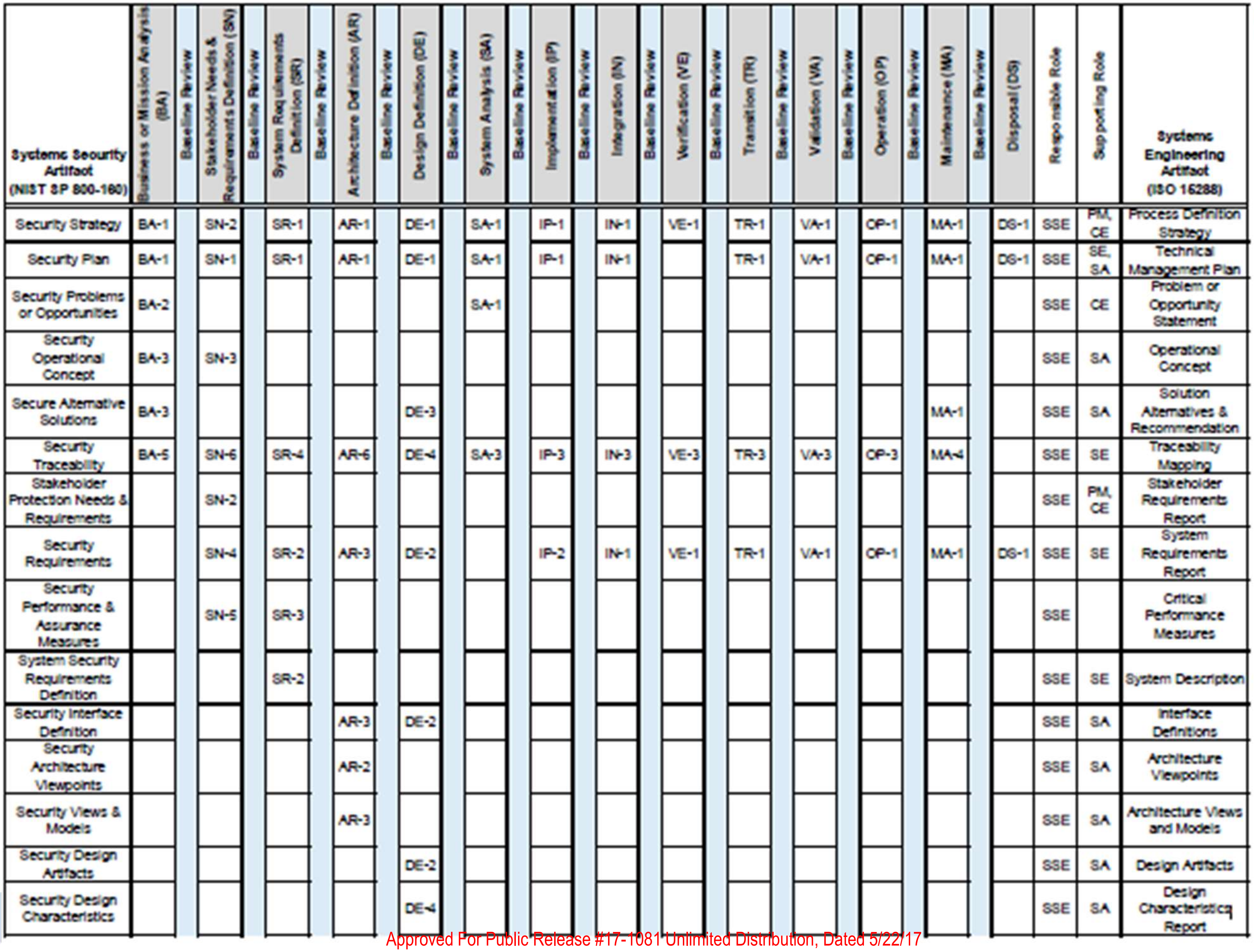
IP	Implementation
IP-1	PREPARE FOR THE SECURITY ASPECTS OF IMPLEMENTATION
IP-1.1	Develop the security aspects of the implementation strategy.
IP-1.2	Identify constraints from the security aspects of the implementation strategy and technology on the system requirements, architecture, design, or implementation techniques.
IP-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of implementation.

Approved For Public Release #17-1081 Unlimited Distribution, Dated 5/22/17

Example Process Breakout

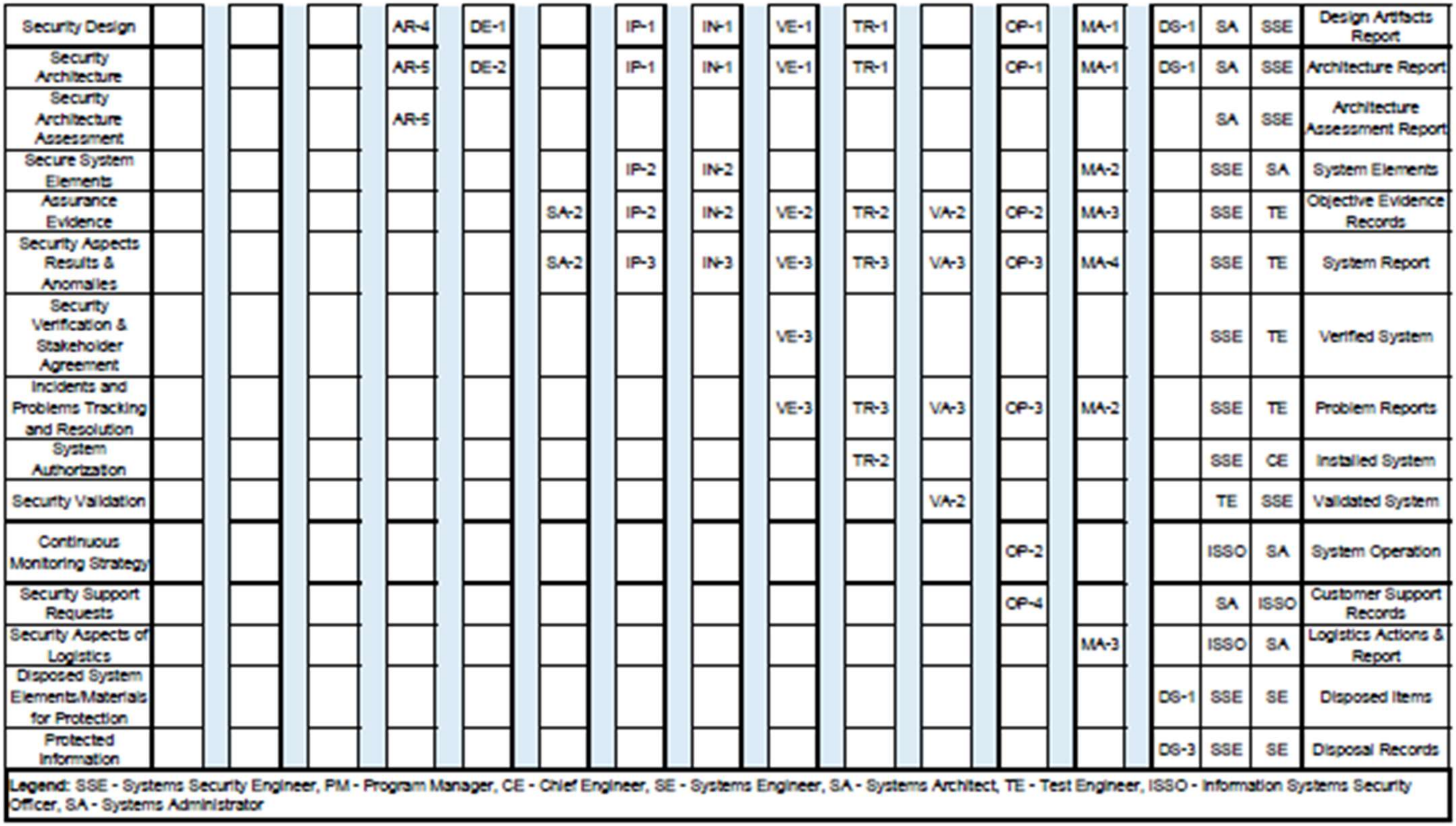
Implementation (IP) Process Breakout	
Purpose	• Realize the security aspects of all system element • Results in a system element that satisfies specified system security requirements, architecture, and design
Outcomes	• Security aspects of the implementation strategy are developed • Security aspects of implementation that constrain the requirements, architecture, or design are identified • Security system element • System elements securely packaged and stored • Enabling systems or services needed for security aspects of implantation • Traceability of security aspects of implemented system elements
Activities and Tasks	• IP-1 Prepare for the security aspects of implementation ○ IP 1.1 – 1.3 • IP-2 Perform the security aspects of implementation ○ IP 2.1 – 2.4 • IP-3 Manage results of the security aspects of implementation ○ IP 3.1 – 3.3
Inputs	Security strategy, plan, traceability, requirements, design, architecture, secure system elements, assurance evidence, assurance results and anomalies report
Responsible and Supporting Roles	Responsible: Systems Security Engineer (SSE) Supporting: Program Manager (PM), Chief Engineer (CE), Systems Engineer (SE), Systems Architect (SA), and Test Engineer (TE)

Roles & Responsibilities Framework



Systems Security Artifact (NIST SP 800-160)	Business or Mission Analysis (BA)	Baseline Review	Stakeholder Needs & Requirements Definition (SN)	Baseline Review	System Requirements Definition (SR)	Baseline Review	Architecture Definition (AR)	Baseline Review	Design Definition (DE)	Baseline Review	System Analysis (SA)	Baseline Review	Implementation (IP)	Baseline Review	Integration (IN)	Baseline Review	Verification (VE)	Baseline Review	Transition (TR)	Baseline Review	Validation (VA)	Baseline Review	Operation (OP)	Baseline Review	Maintenance (MA)	Baseline Review	Disposal (DS)	Responsible Role	Supporting Role	Systems Engineering Artifact (ISO 15288)
Security Strategy	BA-1		SN-2		SR-1		AR-1		DE-1		SA-1		IP-1		IN-1		VE-1		TR-1		VA-1		OP-1		MA-1		DS-1	SSE	PM, CE	Process Definition Strategy
Security Plan	BA-1		SN-1		SR-1		AR-1		DE-1		SA-1		IP-1		IN-1				TR-1		VA-1		OP-1		MA-1		DS-1	SSE	SE, SA	Technical Management Plan
Security Problems or Opportunities	BA-2										SA-1																	SSE	CE	Problem or Opportunity Statement
Security Operational Concept	BA-3		SN-3																									SSE	SA	Operational Concept
Secure Alternative Solutions	BA-3								DE-3																MA-1			SSE	SA	Solution Alternatives & Recommendation
Security Traceability	BA-5		SN-6		SR-4		AR-6		DE-4		SA-3		IP-3		IN-3		VE-3		TR-3		VA-3		OP-3		MA-4			SSE	SE	Traceability Mapping
Stakeholder Protection Needs & Requirements			SN-2																									SSE	PM, CE	Stakeholder Requirements Report
Security Requirements			SN-4		SR-2		AR-3		DE-2				IP-2		IN-1		VE-1		TR-1		VA-1		OP-1		MA-1		DS-1	SSE	SE	System Requirements Report
Security Performance & Assurance Measures			SN-5		SR-3																							SSE		Critical Performance Measures
System Security Requirements Definition					SR-2																							SSE	SE	System Description
Security Interface Definition							AR-3		DE-2																			SSE	SA	Interface Definitions
Security Architecture Viewpoints							AR-2																					SSE	SA	Architecture Viewpoints
Security Views & Models							AR-3																					SSE	SA	Architecture Views and Models
Security Design Artifacts									DE-2																			SSE	SA	Design Artifacts
Security Design Characteristics									DE-4																			SSE	SA	Design Characteristics Report

Roles & Responsibilities Framework



Security Design				AR-4	DE-1		IP-1	IN-1	VE-1	TR-1		OP-1	MA-1	DS-1	SA	SSE	Design Artifacts Report
Security Architecture				AR-5	DE-2		IP-1	IN-1	VE-1	TR-1		OP-1	MA-1	DS-1	SA	SSE	Architecture Report
Security Architecture Assessment				AR-5											SA	SSE	Architecture Assessment Report
Secure System Elements							IP-2	IN-2					MA-2		SSE	SA	System Elements
Assurance Evidence						SA-2	IP-2	IN-2	VE-2	TR-2	VA-2	OP-2	MA-3		SSE	TE	Objective Evidence Records
Security Aspects Results & Anomalies						SA-2	IP-3	IN-3	VE-3	TR-3	VA-3	OP-3	MA-4		SSE	TE	System Report
Security Verification & Stakeholder Agreement									VE-3						SSE	TE	Verified System
Incidents and Problems Tracking and Resolution									VE-3	TR-3	VA-3	OP-3	MA-2		SSE	TE	Problem Reports
System Authorization										TR-2					SSE	CE	Installed System
Security Validation											VA-2				TE	SSE	Validated System
Continuous Monitoring Strategy												OP-2			ISSO	SA	System Operation
Security Support Requests												OP-4			SA	ISSO	Customer Support Records
Security Aspects of Logistics													MA-3		ISSO	SA	Logistics Actions & Report
Disposed System Elements/Materials for Protection														DS-1	SSE	SE	Disposed Items
Protected Information														DS-3	SSE	SE	Disposal Records

Legend: SSE - Systems Security Engineer, PM - Program Manager, CE - Chief Engineer, SE - Systems Engineer, SA - Systems Architect, TE - Test Engineer, ISSO - Information Systems Security Officer, SA - Systems Administrator

References

- Slides 6,7 – NIST Special Publication 800-160, Systems Security Engineering - *Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Final, November 2016* *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf*

27th annual INCOSE international symposium

Adelaide, Australia

July 15 - 20, 2017

ENGINEERS
AUSTRALIA

SESA

www.incose.org/symp2017