THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

# Secure Systems Engineering

## Achieving cyber resiliency in an Australian context

1 May 2019

Michael McGarity

Chief Engineer
Northrop Grumman Australia Mission Systems

# Systems Security Engineering
# What Every System Engineer Needs to Know

NORTHROP GRUMMAN


- Security: Whose job is it anyway?
  - The tired answer is everyone.
  - But System Engineering has a particular role.
- System Engineering manages complexity
  - Robustness: The ability to withstand adverse conditions or rigorous testing.
  - Resilience: The ability of a system to continue to operate at an acceptable level within all likely adverse environments
- A different “Ility”
  - Most non-functional requirements or quality factors (stability, portability, safety, usability, maintainability, extensibility, scalability) combat error, the unknown, or entropy.
  - Security is a quality factor which must also combat deliberate, active and malicious action.

# An Approach

NORTHROP GRUMMAN

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

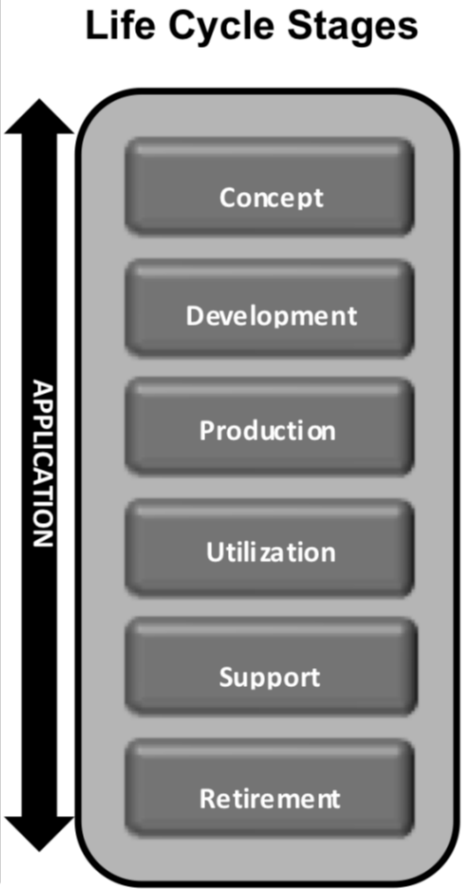
# INCOSE Processes vs NIST 800-160

NORTHROP GRUMMAN

## Systems Engineering Life Cycle Processes

*Recursive, Iterative, Concurrent, Parallel, Sequenced Execution*

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




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

Goal

To integrate artefact roles & responsibilities framework into current INCOSE specialty engineering section

To present framework for easy adoption by practitioners of ISO15288

# Roles & Responsibilities Framework (extract)

NORTHROP GRUMMAN

| 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 Design Characteristics | | | | | | | | | DE-4 | | | | | | | | | | | | | | | | | | | SSE | SA | Design Characteristics Report |
| 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 | | | | | | | | | | | | | | | | | VE-3 | | | | | | | | | | | SSE | TE | Verified System |

**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

# Roles & Responsibilities Framework (extract)

NORTHROP GRUMMAN

| 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 Design Characteristics | | | | | | | | | DE-4 | | | | | | | | | | | | | | | | | | | SSE | SA | Design Characteristics Report |
| 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 | | | | | | | | | | | | | | | | | VE-3 | | | | | | | | | | | SSE | TE | Verified System |

**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

# Roles & Responsibilities Framework (extract)

NORTHROP GRUMMAN

| 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 Design Characteristics | | | | | | | | | DE-4 | | | | | | | | | | | | | | | | | | | SSE | SA | Design Characteristics Report |
| 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 | | | | | | | | | | | | | | | | | VE-3 | | | | | | | | | | | SSE | TE | Verified System |

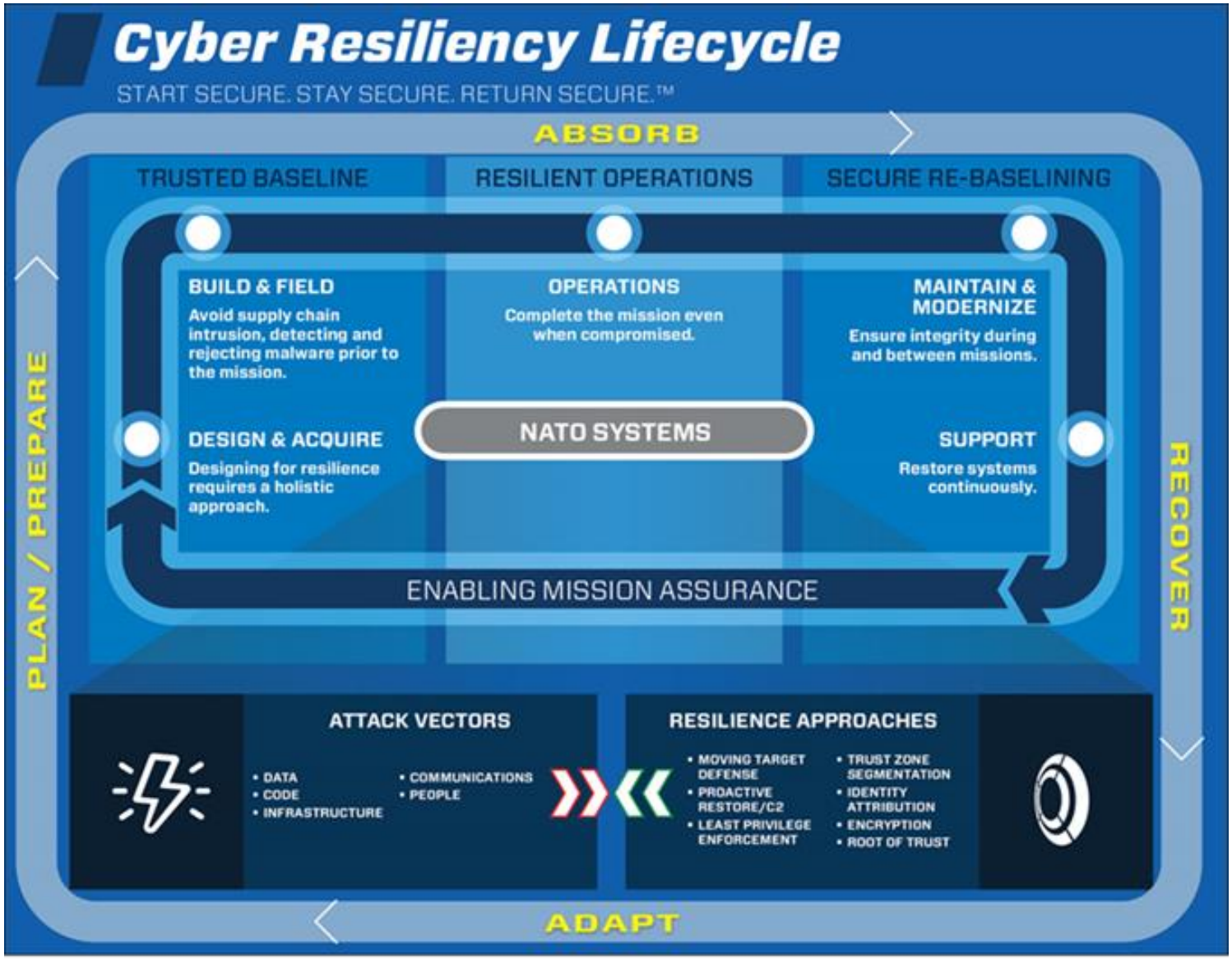
**Legend:** SSE - Systems Security Engineer, PM - Program Manager, CE - Chief Engineer, SE - Systems Engineer, SA - Systems Architect, TE - Test Engineer, ISSO - Information Systems Security Officer, SA - Systems Administrator

# Example Process Breakout

NORTHROP GRUMMAN

| Implementation (IP) Process Breakout | |
|---|---|
| Purpose | • Realize the security aspects of all system element<br>• Results in a system element that satisfies specified system security requirements, architecture, and design |
| Outcomes | • Security aspects of the implementation strategy are developed<br>• Security aspects of implementation that constrain the requirements, architecture, or design are identified<br>• Security system element<br>• System elements securely packaged and stored<br>• Enabling systems or services needed for security aspects of implantation<br>• 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)<br>IP-2 Perform the security aspects of implementation (IP 2.1 – 2.4)<br>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 |
| PSPF Artefacts | System Security Plan (Secure System Elements, Security Architecture)<br>Statement of Applicability (Assurance Evidence)<br>Security Testing (Security Testing Results and Anomolies) |
| Roles | Responsible: Systems Security Engineer (SSE)<br>Supporting: Program Manager (PM), Chief Engineer (CE), Systems Engineer (SE), Systems Architect (SA), and Test Engineer (TE) |

# Going further - Resiliency




The Start Secure, Stay Secure, and Return Secure concept shown here mapped to the NATO Plan, Prepare, Absorb, Recover and Adapt concept for cyber resiliency.

NATO Cyber Resilience Capabilities across the system lifecycle concept based on Start Secure, Stay Secure and Return Secure Concept

# Takeaways

NORTHROP GRUMMAN

- The role of systems engineering in systems security
- The commonalities – and differences – between system security and other quality factors
- Ways in which systems engineering practitioners can access security thinking
- Next steps towards cyber-resilient systems

# Acknowledgments

INCOSE (International Council on System Engineering). 2015. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities.* Version 4. Revised by D. Walden, G. Roedler, K. Forsberg, R. D. Hamelin, and T. Shortell. San Diego, US-CA: INCOSE.

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

Nejib, P., Yakabovicz, E., and Beyer, D. 2014. “Systems Security Engineering: What Every System Engineer Needs to Know”. Proceedings of the 27th Annual INCOSE International Symposium.


THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN