NATO Resilience by Design:
Enhancing Resilience through Cyber Systems Engineering

June 26, 2017

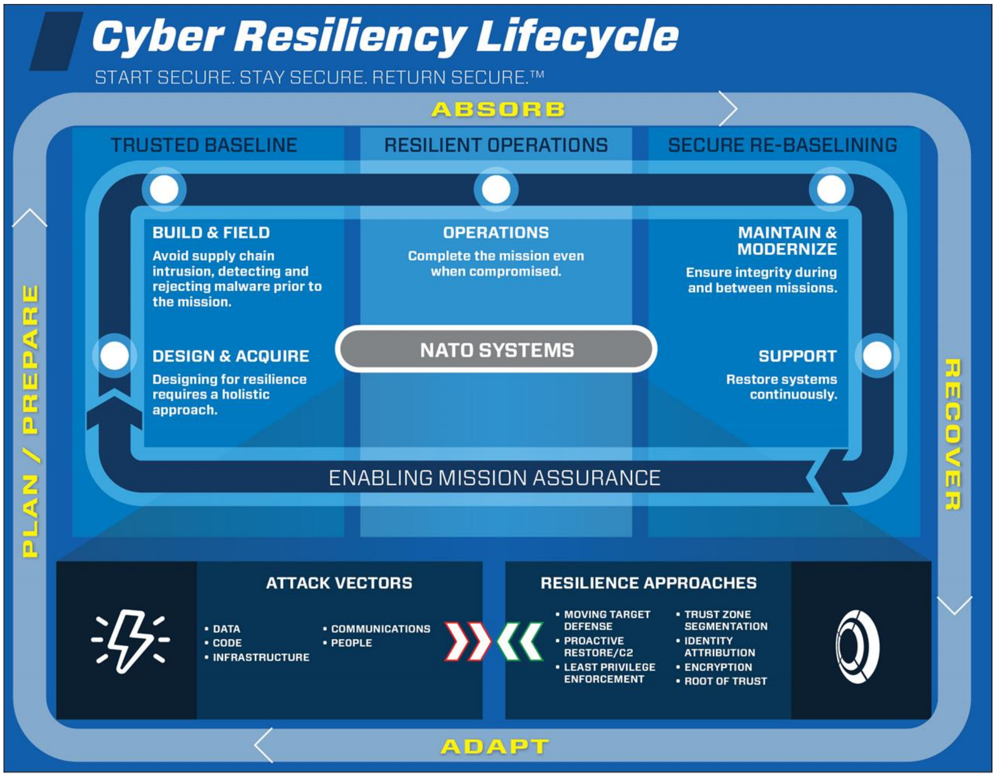
Northrop Grumman Corporation
Mission Systems Sector, Cyber and Intelligence Mission Solutions

Technical POCs/Authors:
Ms. Perri Nejib, Technical Fellow
Northrop Grumman Corporation
2691 Technology Drive
Annapolis Junction, MD 20701
Phone: (240) 755-9196
Perri.Nejib@ngc.com

Mr. Edward Yakabovicz, Cyber Architect
Northrop Grumman Corporation
2691 Technology Drive
Annapolis Junction, MD 20701
Phone: (410) 508-8294
Edward.Yakabovicz@ngc.com

Introduction

Cyber Resilience (as opposed to merely risk-based approaches) is an ever increasing topic of interest in literature and in practice with many nations expressing it in their cyber strategies to apply newer practices in providing system protection from the rapidly changing cyber threat environment. This paper addresses the engineering-driven actions necessary to develop more resilient systems by integrating Cyber Security/ Systems Security Engineering (SSE) to that of the well known Systems Engineering (SE) process. This concept, shown in Figure 1, infuses systems security engineering techniques, methods, and practices into typical systems and software engineering system development lifecycle activities, thus becoming part of the core solution/process rather than an isolated and expensive add-on, bolt-on, and separate task/process.



Cyber Resiliency Lifecycle

START SECURE. STAY SECURE. RETURN SECURE.™

ABSORB

TRUSTED BASELINE

RESILIENT OPERATIONS

SECURE RE-BASELINING

BUILD & FIELD

Avoid supply chain intrusion, detecting and rejecting malware prior to the mission.

OPERATIONS

Complete the mission even when compromised.

MAINTAIN & MODERNIZE

Ensure integrity during and between missions.

DESIGN & ACQUIRE

Designing for resilience requires a holistic approach.

NATO SYSTEMS

SUPPORT

Restore systems continuously.

ENABLING MISSION ASSURANCE

PLAN / PREPARE

RECOVER

ATTACK VECTORS

- DATA
- CODE
- INFRASTRUCTURE
- COMMUNICATIONS
- PEOPLE

RESILIENCE APPROACHES

- MOVING TARGET DEFENSE
- PROACTIVE RESTORE/C2
- LEAST PRIVILEGE ENFORCEMENT
- TRUST ZONE SEGMENTATION
- IDENTITY ATTRIBUTION
- ENCRYPTION
- ROOT OF TRUST

ADAPT

Figure 1 – Resilience by Design through Cyber System Engineering

In today's rapidly changing cyber threat environment with ever increasing attack surfaces, an integrated Cyber Security to Systems Engineering (SE) mindset, known as Systems Security Engineering (SSE) is required to properly design, test, deploy, operate and maintain secure systems in an affordability-constrained environment. Bringing together and integrating all security related expertise and disciplines with that of systems engineering at the beginning of any project would close the gap between engineering and systems security design considerations that are many times separate and discrete tasks. This would apply resilient practices found in cyber security solutions to secure and protect systems at the start of the system development life cycle for a seamless approach. Resilience by Design would then by default become part of the core management and technical plans from the start of any project and be considered through each step of the system development life cycle. What the authors have observed is while there are several separate international standards covering SE, cyber security and SSE, they lack a common basis and flow between them that would lend itself towards integration of each of these across a system lifecycle. What is needed is integrated processes that support the NATO Resilient approach- Plan/Prepare, Absorb, Recover and Adapt shown in Figure 1.

The primary focus of this position paper provides a discussion of the security engineering-driven actions necessary to develop a resilient process to enable NATO systems to Plan/Prepare, Absorb, Recover and Adapt to threats. The approach starts with and builds upon a set of well-established International Standards for systems and software engineering for the purpose of infusing systems security engineering techniques, methods, and practices into the systems and software engineering processes. The ultimate objective is to address security resiliency requirements and issues from stakeholder requirements and protection needs perspective and to use established engineering processes that include security to ensure that all requirements and needs are addressed together from the beginning with the appropriate fidelity and rigor across the entire life cycle of the system.

Current Efforts

Current efforts to align SE and SSE are seen across many well-established international standards for systems and software engineering as published by the International Organization for Standardization (ISO), International Council On System Engineering (INCOSE), and the National Institute of Standards and Technology (NIST). Each infuses systems security engineering techniques, methods, and practices into systems and software engineering processes with a purpose to enable and extend system resiliency with an ability to recover from or easily adjust to misfortune or change[1]. As NATO states " …resiliency refers to the system's ability to recover or regenerate its performance to a sufficient level after an unexpected impact produces a degradation of its performance"[2]. There are several separate standards covering SE, cyber security and SSE, but they lack a common basis and flow between them that would enable integration of each across a system lifecycle. The upper level guidance exists in these standards, but the ability to apply those principles and practices through process, roles responsibilities, and guidance is lacking.

For example, ISO 15288:2015 standard, Systems and software engineering – System life cycle processes, discusses and defines the various systems life cycle phases of a system/program and the associated SE processes that are utilized. ISO 15288 provides a common process framework for describing the life cycle of systems using a Systems Engineering approach with links to SE artifacts and processes. Beyond SE and SSE, the ISO 27000 series and specifically ISO 27001 Information Technology – Security Techniques – Information Security Management Systems (ISMS) –provides requirements for establishing, implementing, maintaining and continuously improving ISMS through systems security that protects the confidentiality, integrity and availability of information by applying a risk management process. In addition ISO 21827:2008, Information Technology – Security Techniques – System Security Engineering – Capability Maturity Model (SSE-CMM) describes the essential characteristics of an

[1] Ross, R., McEvilley, M., and Oren, J. (2016) Systems Security Engineering: Considerations for a multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. *NIST Special Publication*, 800(160),

vii.

[22] NATO, Workshop Announcement. Call For Contributions, Cyber Resilience, IST-153-RWS, p. 4 [PDF].

organization's security engineering process and focuses on practices observed in industry and is based in metrics.

Of these examples, only NIST SP 800-160 dated 2016 is the very first standard to link the System Engineering processes with System Security Engineering processes and define a common foundation/lexicon for integrating cyber security into all phases of the systems life cycle. This NIST standard is based on the same SE processes found in ISO 15288 and in the INCOSE System Engineering Handbook Fourth Edition 2015 in providing greater integration of security with SE artifacts and activities. Additionally, the INCOSE organization, through its System Security Engineering working group has several ongoing efforts that are focusing on building out additional frameworks further linking the SE and security processes and defining SSE. The authors of this position paper are actively involved in developing those frameworks.[3]

Gaps and Approaches

What the authors have observed is while there are several separate ISOs covering SE, security and SSE; they lack a common basis and flow between them that would lend itself towards integration of each of these across a system lifecycle. In contrast, both the INCOSE SE Handbook (Fourth Edition) and NIST SP 800-160 are based on and describe use of the technical processes presented in ISO 15288:2015. This has benefits that are two-fold, using the same terminology allows multiple disciplines to comprehend both SE and SSE processes and understand how one affects the other and why integration of the common artifacts and processes adds value. What the government, private industry, academia, and standards organizations are realizing is that integrating and implementing security using a SE approach is the most efficient and effective way to ensure that security is addressed at each and every stage of the life cycle and becomes part of the overall SE processes instead of being done separately and isolated from

[3] Beyer, D., Nejib, P and Yakabovicz, E., System Security Engineering: What Every System Engineer Needs to Know, INCOSE IS 2017 Proceedings, July 2017

other engineering activities. Typically, separate and isolated activities occurring at the end of the lifecycle, known as “bolting on cyber security”, cost more, and delay projects and schedules.

Summary

The resilience by design topic is still evolving and becoming accepted as a way to improve cyber security. By integrating the SSE practices to those of SE is a starting point to enable and effectivity enable cyber resilient engineering as part of the foundational elements of program management, system and software engineering, and supply chain early within the system development life cycle. Although there are only two efforts to link SSE to SE processes and components, there are still many gaps in the lower level details that explain the granular engineering functions, tasks and artifacts. As mentioned previously both NIST and INCOSE are currently developing companion documents and frameworks to supplement the standards. While these evolve, organizations such as NATO should consider some initial first steps or best practices to prepare themselves to integrating the SSE to SE-based engineering practices as a starting point to the cyber resilient discussion and planning.

With INCOSE and US NIST standards already moving to address the gap between Security Engineering and Systems Engineering through integrating key engineering aspects throughout the system development life cycle, the positon of this paper is NATO should evaluate these changes and plan next steps in the adoption of these SSE into SE practices now. NATO should consider adoption since these standards have based themselves on the ISO 15288 terminology/processes. Since change is difficult regardless of the process, this paper recommends NATO take initial steps to accept SSE-based thinking by adopting a few of these practices early to allow fast acceptance later on as standards and framework mature and as the industry as a whole embraces these concepts. NATO could accommodate Cyber Security as a key delivery practice; specifically find ways to better link the various ISO standards in individual domains (SE, Security, and SSE) to each other and to NATO/Country specific standards. In doing so, NATO would also start the process of adopting resiliency aspects found in each of these documents, thereby making resilient solutions as a common process that would become part of the core NATO system delivery process.

NATO can reference and even adopt US SSE processes found in US NIST SP 800-160, which based itself on ISO and INCOSE Handbook that are internationally recognized SE processes and built a system security standard from those origins so a wide audience would be able to implement and benefit. Adding cyber security throughout the SE lifecycle stages will only strengthen and ensure resiliency of those deliveries by ensuring cyber security is thought of first (as well as resilient standards), along with and in addition to the stakeholder, business and technical needs. The end goal being reduced cyber security risk and improved system performance for assured delivery of secure and resilient systems for the NATO mission.