31st Annual INCOSE international symposium
virtual event
July 17 - 22, 2021

STPA-Sec Analysis for DevSecOps Reference Design

2nd Lt Brynn Feighery
2nd Lt Ryyan Reule

About Us

RYYAN T REULE received a BS in Systems Engineering with a concentration in Electrical Engineering from the United States Air Force Academy, Colorado Springs, CO in 2021. He serves as a Commissioned Officer as a student pursuing his MS in Systems and Industrial Engineering in the United States Air Force. His research interests include model based systems engineering, human machine interactions, and systems security engineering.

BRYNN E. FEIGHERY received BS in Systems Engineering with a concentration in Human Factors Engineering from the United States Air Force Academy, Colorado Springs, CO in 2021. She serves as a Commissioned Officer as a project engineer in the United States Space Force. Her other research efforts include systems security engineering, model based systems engineering, and concept generation and preliminary design.

Additional Authors

WILLIAM J BARNUM received a BS in Computer Science from South-western College, Winfield, KS, and an ME in Engineering Management from University of Colorado, Boulder, CO. He served 5 years as a Commissioned Officer in the US Army Military Intelligence Branch. Will currently serves as group leader in the Systems Security Engineering Department in the MITRE Labs Center, where his research interests include enabling digital engineering, advancing emerging systems security engineering practices, and exploring data-driven analytics.

MARK WINSTEAD, The MITRE Corporation's Systems Security Engineering Department Chief Engineer, had over twenty-five years' STEM experience before joining MITRE in 2014, including stints as a crypto-mathematician, software engineer, systems engineer, systems architect and systems engineer as well as systems security engineer. He has worked for several defense contractors, an Environmental Protection Agency contractor, a Facebook-like start up, a fabless semiconductor manufacturer of commercial security protocol acceleration solutions, and a network performance management solutions company. Mark is a graduate of the University of Virginia (PhD, Mathematics) and Florida State University (BS & MS, Mathematics). He resides in Colorado Springs, CO.

DARYL R HILD received a BSEE from Washington University, St. Louis, MO and an MS and PhD in Electrical and Computer Engineering from University of Arizona, Tucson, AZ. He served nearly 6 years as a Commissioned Officer in the US Army Signal Corps. Daryl currently serves as the head of the Systems Security Engineering Department in the MITRE Labs Center, where his research interests include enabling digital engineering, modeling, and simulation for systems security. In the community, Daryl has served as a BSA Venturing advisor enabling coed youth to develop leadership skills through community service projects and high adventure experiences.

MARTIN "TRAE" SPAN received a BSSE from the United States Air Force Academy, Colorado Springs, CO in 2012, a M.S. in Systems Engineering in 2018 from the Air Force Institute of Technology, Dayton, OH, and holds an INCOSE CSEP certification. He serves as a Commissioned Officer in the United States Air Force. His research interests include model based systems engineering, systems security engineering, and conceptual system design.

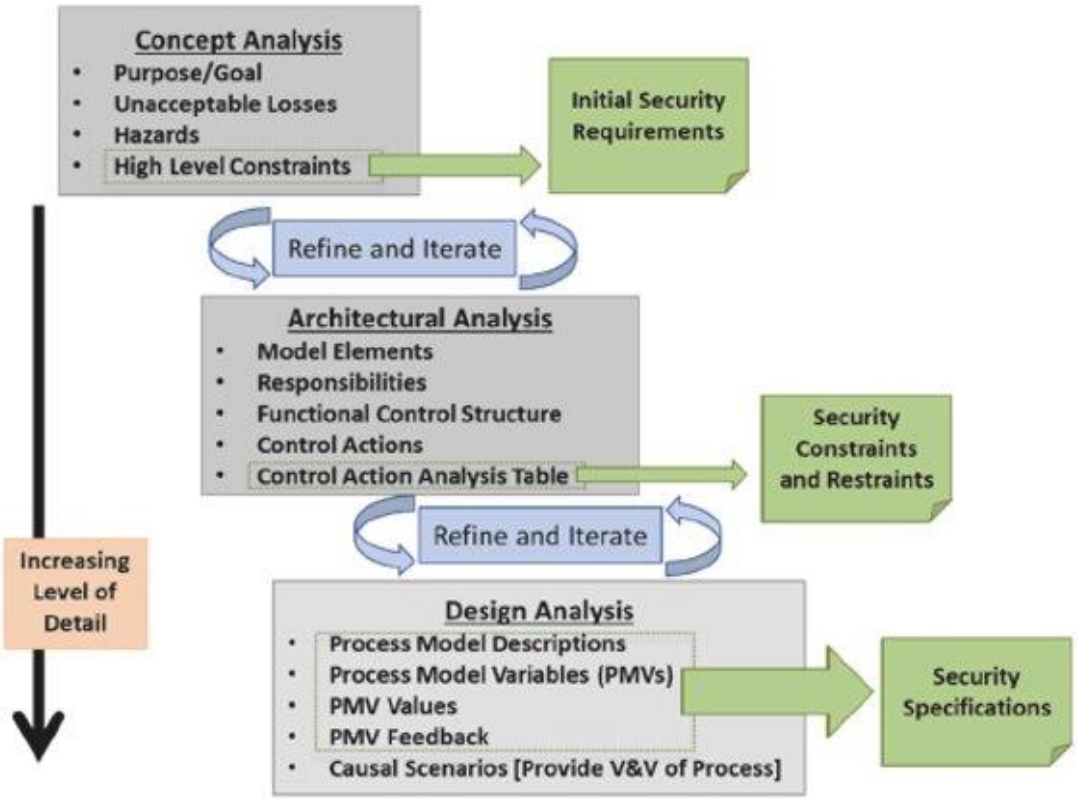
Overview

- STPA-Sec Overview
- Conceptual Analysis
  - Purpose
  - Loss/Hazard Mapping
  - Hazard/Constraint Mapping
- Architectural Analysis
  - Model Elements/Responsibilities
  - Functional Control Structures (FCS)
  - Control Action (Analysis)
- Design Analysis
  - Streamlined Methodology
  - Controller Constraints
  - Causal Scenario/Process
- STPA-Sec Value Added
- Future Work

STPA-Sec Overview

- **Purpose:** "To understand and elicit systems security requirements from a holistic viewpoint during the conceptual stage of development" (Span)
- **Components**
  - Conceptual Analysis
  - Architectural Analysis
  - Design Analysis

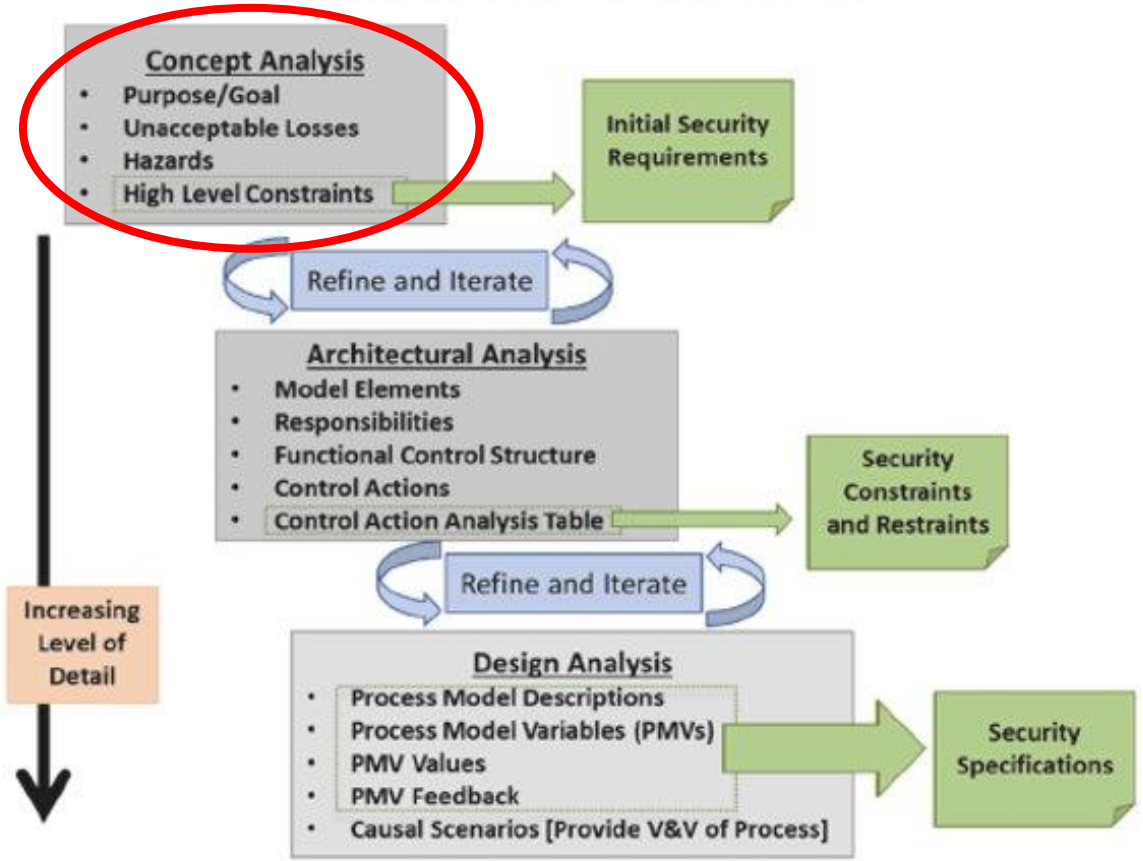
FIG 1. STPA-SEC TAILORED APPROACH.



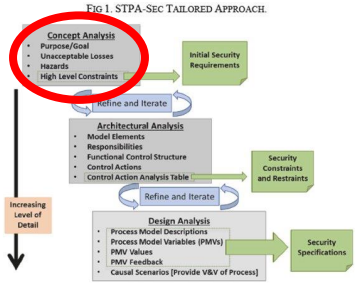
M. Span, L. Mailloux, R. Mills and W. Young, "Conceptual Systems Security Requirements Analysis: Aerial Refueling Case Study," IEEE Access, 2018.

Concept Analysis

FIG 1. STPA-SEC TAILORED APPROACH.



M. Span, L. Mailloux, R. Mills and W. Young, "Conceptual Systems Security Requirements Analysis: Aerial Refueling Case Study," IEEE Access, 2018.



Purpose/Goal Statement

A system to develop secure software **by means of** continuously integrating and delivering software while incorporating planning, developing, building, testing, releasing & delivering (deploying, operating, and monitoring) **in order to** provide secure operational software products.

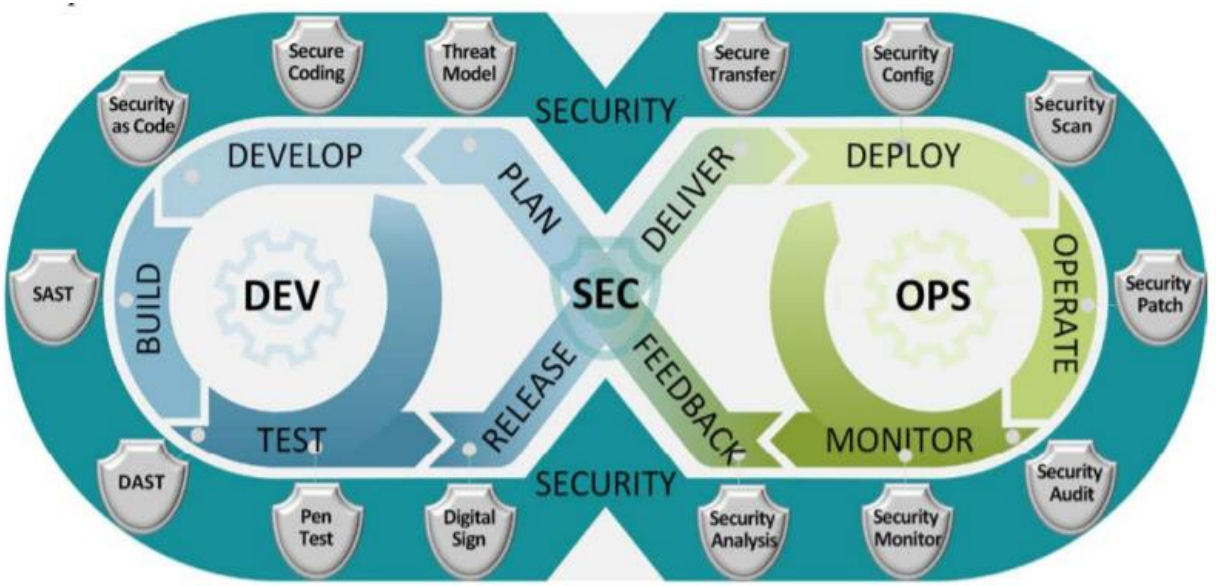


Figure 3: DevSecOps Software Lifecycle

Lam, Thomas. "DoD Enterprise DevSecOps Reference Design." Department of Defense, 2019.

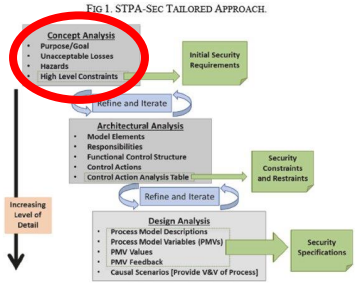
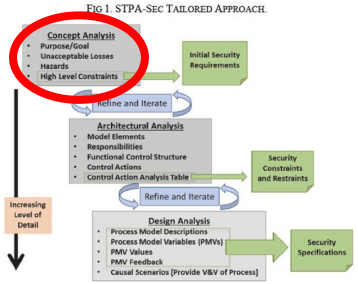


FIG 1. STPA-SEC TAILORED APPROACH.

Loss/Hazards Mapping

		Losses		
		L1: Loss of reputation/trust with stakeholders	**L2: Does not meet operational needs**	**L3: Compromise of critical data**
Hazards	**H1: Lack of availability to information and/or pipeline**	**X**	**X**	**X**
	H2: Lack of control of sensitive information	**X**	**X**	**X**
	H3: Software gets incorrectly passed through the pipeline	**X**	**X**	
	H4: Inability to continuously integrate software	**X**	**X**	**X**
	H5: Inability to deliver functional software	**X**	**X**	

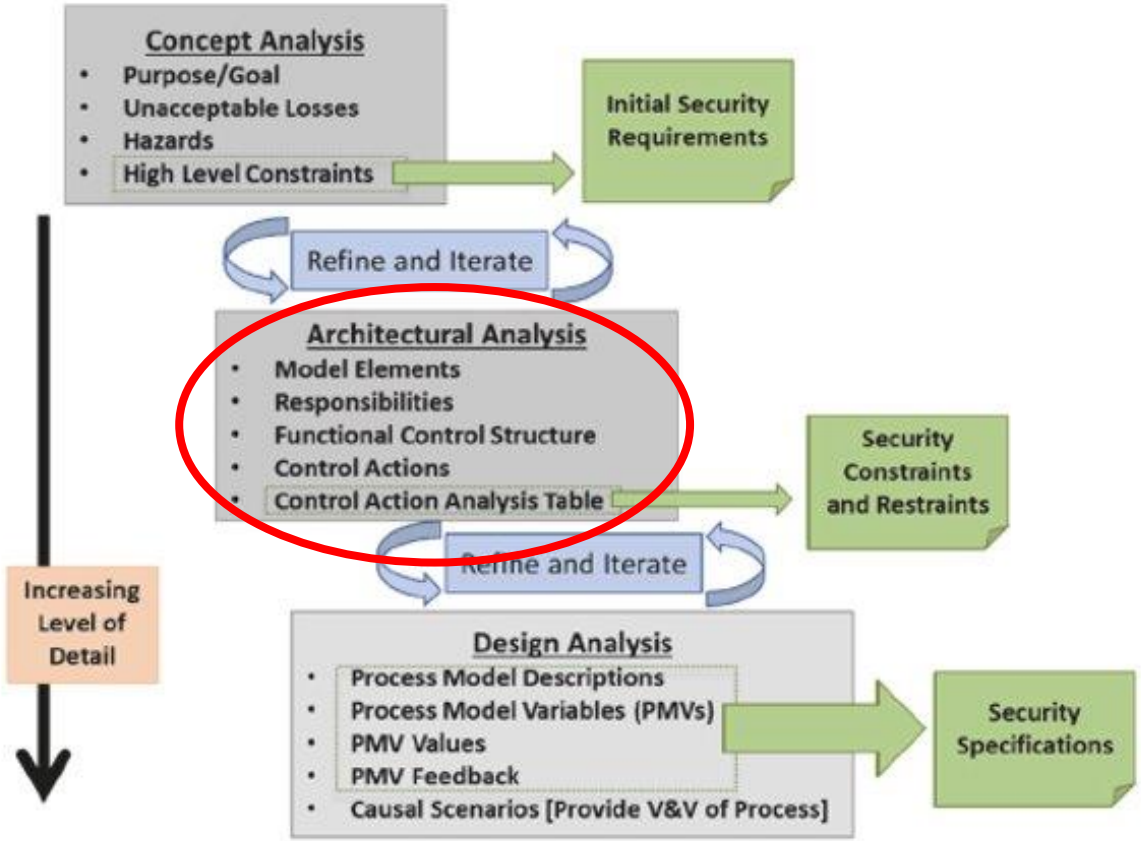


Hazards/Constraints Mapping

Hazards	Constraints
Lack of access to information and/or pipeline	The system shall ensure that precautions and redundancy measures are in place to reduce probability of lack of access.
Lack of control of sensitive information	The system shall be designed to minimize exposure and/or loss of information to unauthorized entities.
Software gets incorrectly passed through the pipeline	The system shall actively enforce processes that allow software passage through the DevSecOps lifecycle.
Inability to continuously integrate software	The system shall incorporate practices that provide integration mechanisms.
Inability to deliver functional software	The system shall execute validity tests to ensure functional software is being delivered.

Architectural Analysis

FIG 1. STPA-SEC TAILORED APPROACH.



M. Span, L. Mailloux, R. Mills and W. Young, "Conceptual Systems Security Requirements Analysis: Aerial Refueling Case Study," IEEE Access, 2018.

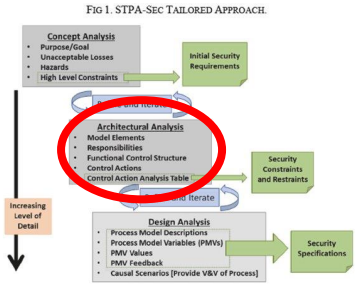
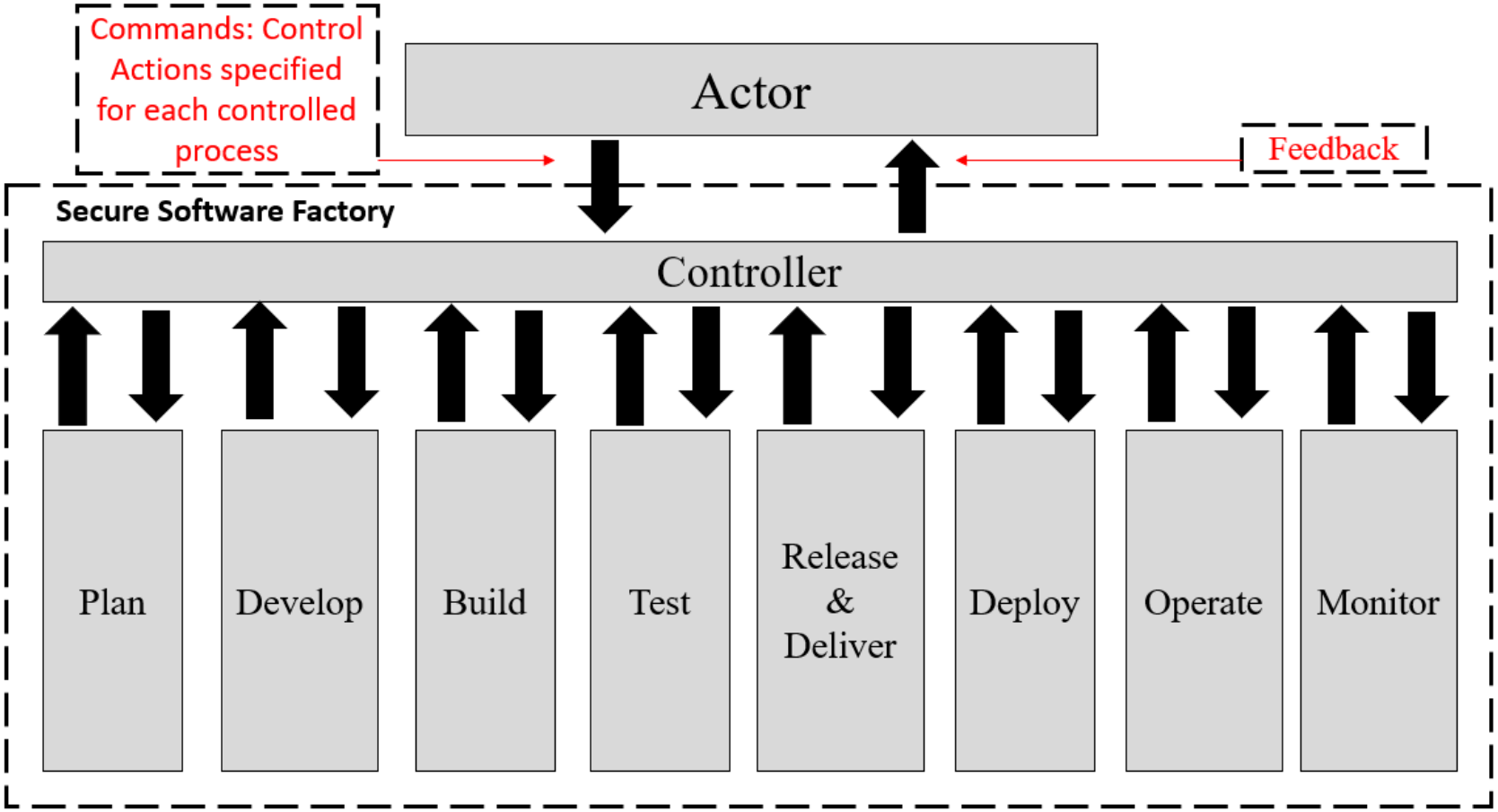
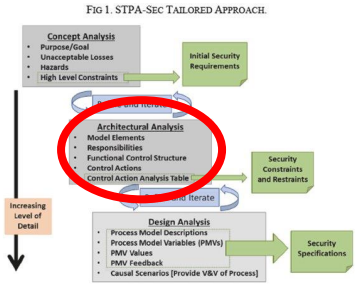


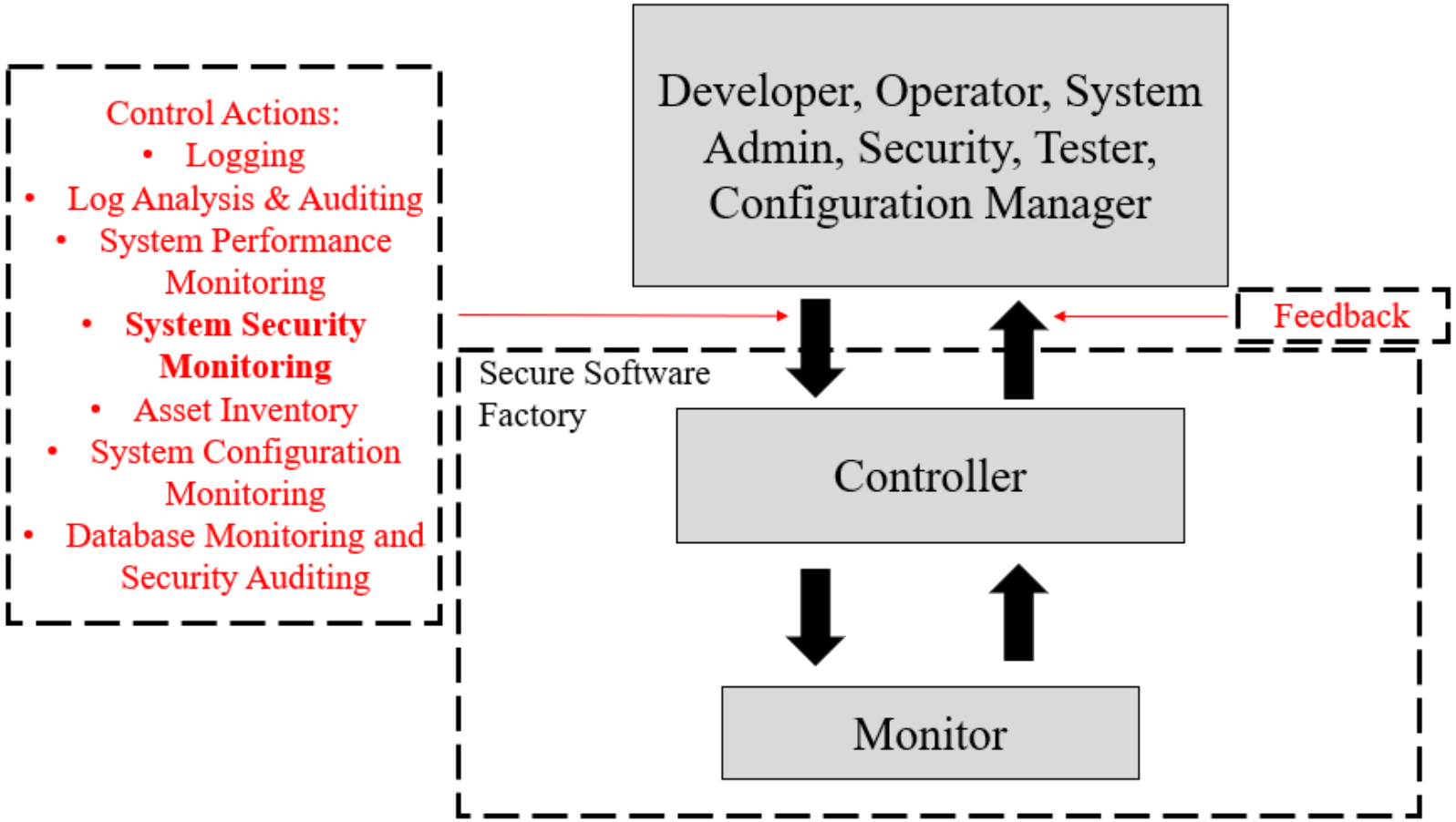
Fig 1. STPA-Sec Tailored Approach

Functional Control Structures





Functional Control Structures



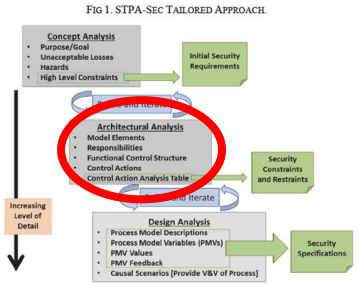
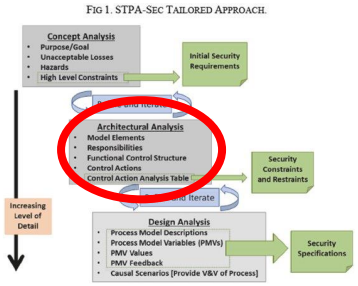


FIG 1. STPA-SEC TAILORED APPROACH.

Control Actions Table

- **67 Control Actions analyzed**
- **9 Phases**
- **8 Performers**

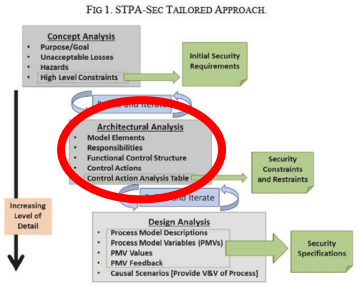
Control Action	Activity (Phase)	Performer	Description
System Security Monitoring	Monitor	Operator, Security, System Admin	Monitor security of all system components; Security vulnerability assessment; System security compliance scan



Control Actions Table

Focus on System Security Monitoring

Control Action (CA)	Activity (Phase)	Actor	Description
Logging	Monitor	Developer, Security, System Admin	Log system events
Log Analysis and Auditing	Monitor	Developer (only for analysis), Operator, Security, System Admin, Tester (only for analysis)	Filter or aggregate logs; Analyze and correlate logs
System Performance Monitoring	Monitor	Operator, Security, System Admin	Monitor system hardware, software, database, and network performance; Baselining system performance; Detect anomalies
System Security Monitoring	Monitor	Operator, Security, System Admin	Monitor security of all system components; Security vulnerability assessment; System security compliance scan
Asset Inventory	Monitor	Configuration Manager, Operator, Security, System Admin	Inventory system IT assets
System Configuration Monitoring	Monitor	Configuration Manager, Operator, Security, System Admin	System configuration (infrastructure components and software) compliance checking, analysis, and reporting
Database Monitoring and Security Auditing	Monitor	Operator (only for Database Monitoring), Security, System Admin	Database performance and activities monitoring and auditing



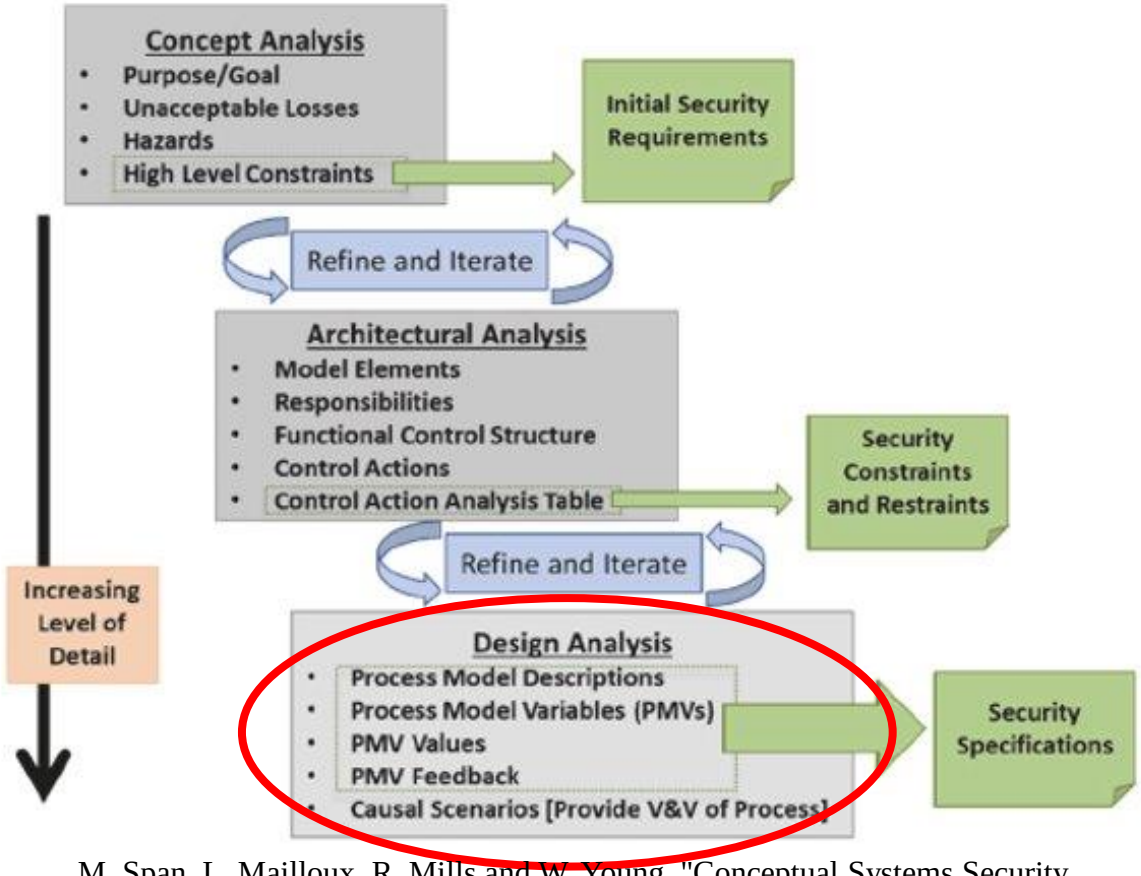
Control Actions Analysis

Hazards				
H1: Lack of availability to information and/or pipeline	H2: Lack of control of sensitive information	H3: Software gets incorrectly passed through the pipeline	H4: Inability to continuously integrate software	H5: Inability to deliver functional software

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong	Stopping too soon/applying too long
System Security Monitoring (33)	Not providing system security monitoring is hazardous if unauthorized activities go undetected. [H1, H2, H3, H4]	Providing system security monitoring is hazardous if exposed or manipulated. [H2, H5] ; if it exhaust system resources [H1, H4, H5]	Providing system security monitoring is hazardous if too late unauthorized activities go undetected. [H1, H2, H3, H4]	Providing system security monitoring is hazardous if stopped too soon if unauthorized activities go undetected. [H1, H2, H3, H4] or applied too long if it exhaust system resources [H1, H4, H5]

Design Analysis

FIG 1. STPA-SEC TAILORED APPROACH.



M. Span, L. Mailloux, R. Mills and W. Young, "Conceptual Systems Security Requirements Analysis: Aerial Refueling Case Study," IEEE Access, 2018.

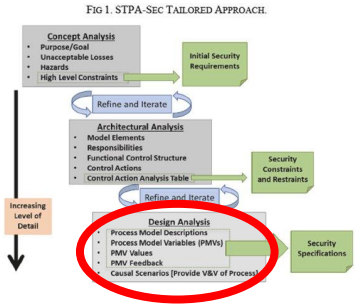


FIG 1. STPA-SEC TAILORED APPROACH.

Design Analysis

- **Due to the extensive nature of the DevSecOps system, we adapted a streamlined methodology (STPA Handbook)**
- **Revisit specific application to be able to identify meaningful PMVs**

- **Based on the CA Analysis:**
  - **System Constraints:** Derive specific system behaviors that must be satisfied to prevent UCAs
  - **Causal Scenarios:** Describes the causal factors that may lead to the UCAs and to hazards

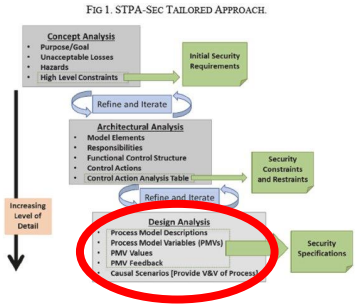


Fig 1. STPA-Sec Tailored Approach

Control Action Analysis

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong	Stopping too soon/applying too long
System Security Monitoring (33)	Not providing system security monitoring is hazardous if unauthorized activities go undetected. [H1, H2, H3, H4]	Providing system security monitoring is hazardous if exposed or manipulated. [H2, H5] ; if it exhaust system resources [H1, H4, H5]	Providing system security monitoring is hazardous if too late unauthorized activities go undetected. [H1, H2, H3, H4]	Providing system security monitoring is hazardous if stopped too soon if unauthorized activities go undetected. [H1, H2, H3, H4] or applied too long if it exhaust system resources [H1, H4, H5]

	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong	Stopping too soon/applying too long
Security Constraints	SC-33.1 System Security monitoring must occur on an uninterrupted basis. SC-33.2 Critical assets and information must be determined before System security monitoring. SC-33.3 Authorized and unauthorized actions must be determined prior to the configuration of the system security monitoring system.	SC-33.4 System Security monitoring information and resources that must be protected from unauthorized tampering and exposure must be determined before the system is deployed. SC-33.5 The system must prevent the unauthorized tampering or modification of system security monitoring. SC-33.6 System security monitoring must detect the exposure of resources needing to be kept private. SC-33.7 System Security Monitoring must abide by a resource utilization threshold to avoid exhausting system resources and facilitate timely progress.	SC-33.8 Monitoring Capabilities must be in place before the development phase begins. SC-33.9 Monitoring Capabilities must be evolve as the system design changes. SC-33.10 System changes are evaluated for security impacts prior to release.	See SC33.1 and SC-33.7.

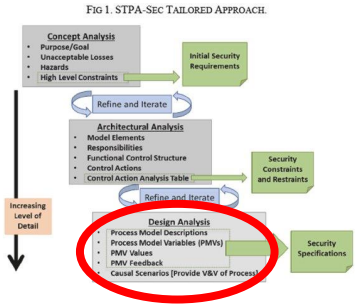
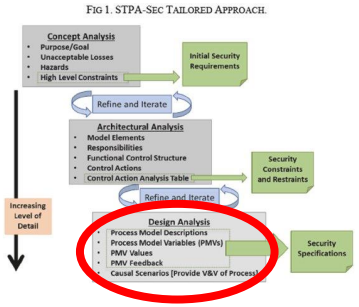


FIG 1. STPA-SEC TAILORED APPROACH.

Security Constraints and Causal Scenarios

Security Constraints: System Security Monitoring (Control Action 33)			
Not Providing Causes Hazard	**Providing Causes Hazard**	**Too Early/Too Late, Wrong**	**Stopping Too Soon/Applying Too Long**
SC-33.1 System security monitoring must occur on an uninterrupted basis.	**SC-33.4** System security monitoring information and resources that must be protected from unauthorized tampering and exposure must be determined before the system is deployed.	**SC-33.8** Monitoring capabilities must be in place before the development phase begins.	See **SC-33.1**
SC-33.2 Critical assets and information must be determined before system security monitoring.	**SC-33.5** The system must prevent the unauthorized tampering or modification of system security monitoring.	**SC-33.9** Monitoring capabilities must evolve as the system design changes.	See **SC-33.7**
SC-33.3 Authorized and unauthorized actions must be determined prior to the configuration of the system security monitoring system.	**SC-33.6** System security monitoring must detect the exposure of resources needing to be kept private.	**SC-33.10** System changes are evaluated for security impacts prior to release.	
	SC-33.7 System security monitoring must abide by a resource utilization threshold to avoid exhausting system resources and facilitate timely progress.		

Causal Scenarios
Contextual background/environmental conditions that would result in a loss
Adversary gains knowledge of monitoring through information exposure and can manipulate monitoring procedures to gain undetected access to a system, allowing them to disrupt operations by triggering hazards.



STPA-Sec Value Added

Control Action 33: System Security Monitoring

Causal Scenario: Adversary gains knowledge of monitoring through information exposure and is able to manipulate monitoring procedures to gain undetected access to a system, allowing them to disrupt operations by triggering hazards.

System Security Monitoring (Control Action 33)

Unacceptable Losses	Hazards	Hazardous Control Action	Security Requirement
L1: Loss of reputation/ trust with stakeholders	H1: Lack of availability to information and/or pipeline	Providing system security monitoring is hazardous if exposed or manipulated. [H2] ; if it exhaust system resources [H1, H4]	SC-33.7 System Security Monitoring must abide by a resource utilization threshold to avoid exhausting system resources and facilitate timely progress.
L2: Does not meet operational needs	H2: Lack of control of sensitive information		
L3: Compromise of critical data	H4: Inability to continuously integrate and deliver software		

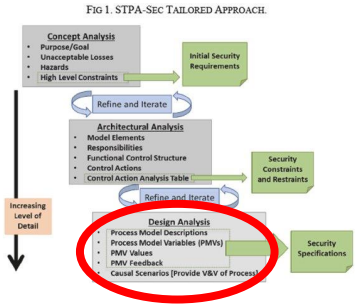


FIG 1. STPA-SEC TAILORED APPROACH.

Additional Examples

Dynamic Application Security Test and Scan (Control Action 35)

Unacceptable Losses	Hazards	Hazardous Control Action	Security Requirement
L1: Loss of reputation/ trust with stakeholders	H1: Lack of availability to information and/or pipeline	Providing dynamic application security test and scan is hazardous if unwarranted assurance is provided. [H1, H2]	SC 35.5 All security test results should be holisticallly reviewed to create a complete picture of the system's security stature.
L2: Does not meet operational needs	H2: Lack of control of sensitive information		
L3: Compromise of critical data			

Threat Modeling (Control Action 37)

Unacceptable Losses	Hazards	Hazardous Control Action	Security Requirement
L1: Loss of reputation/ trust with stakeholders	H1: Lack of availability to information and/or pipeline	Providing threat modeling is hazardous if too late if threats are already realized in the system before identification and model. [H1, H2, H3, H4]	SC 37.6 Threat modeling should be completed alongside the design documents in the plan phase.
L2: Does not meet operational needs	H2: Lack of control of sensitive information		
L3: Compromise of critical data	H3: Software gets incorrectly passed through the pipeline		
	H4: Inability to continuously integrate and deliver software		

Future Work

- Applicable to more specific systems
  - Produce actual, meaningful requirements
  - Derive concrete variables/values

Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the U. S. Air Force, the Department of Defense, or the U.S. Government.

Acknowledgements

We would like to thank all the members of the USAFA and MITRE team and for the various program sponsors for their review and support.

Questions?

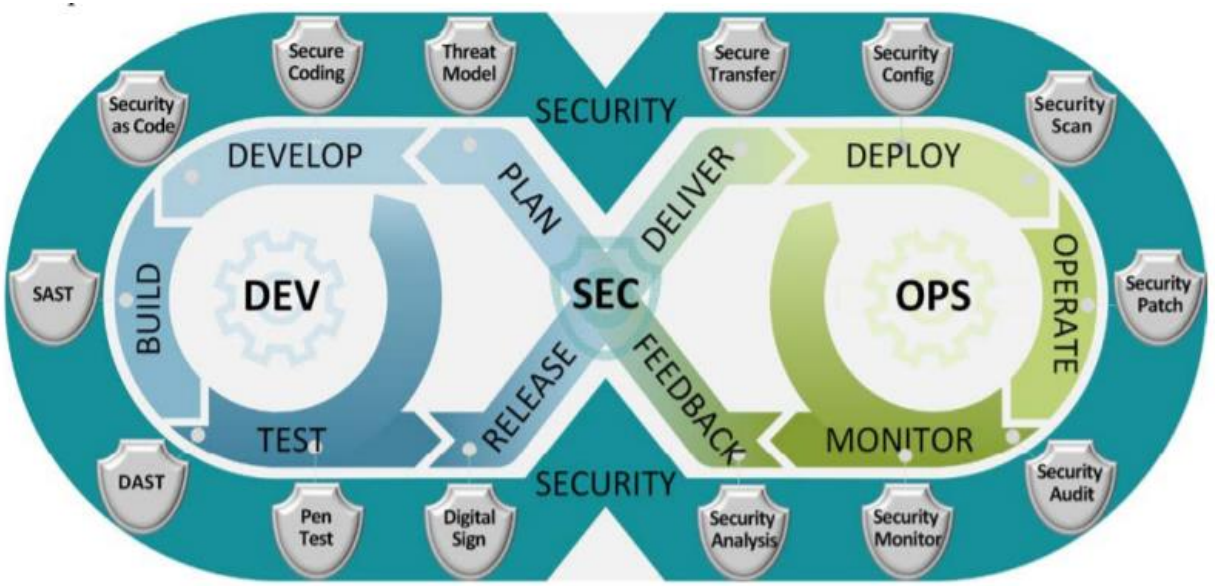
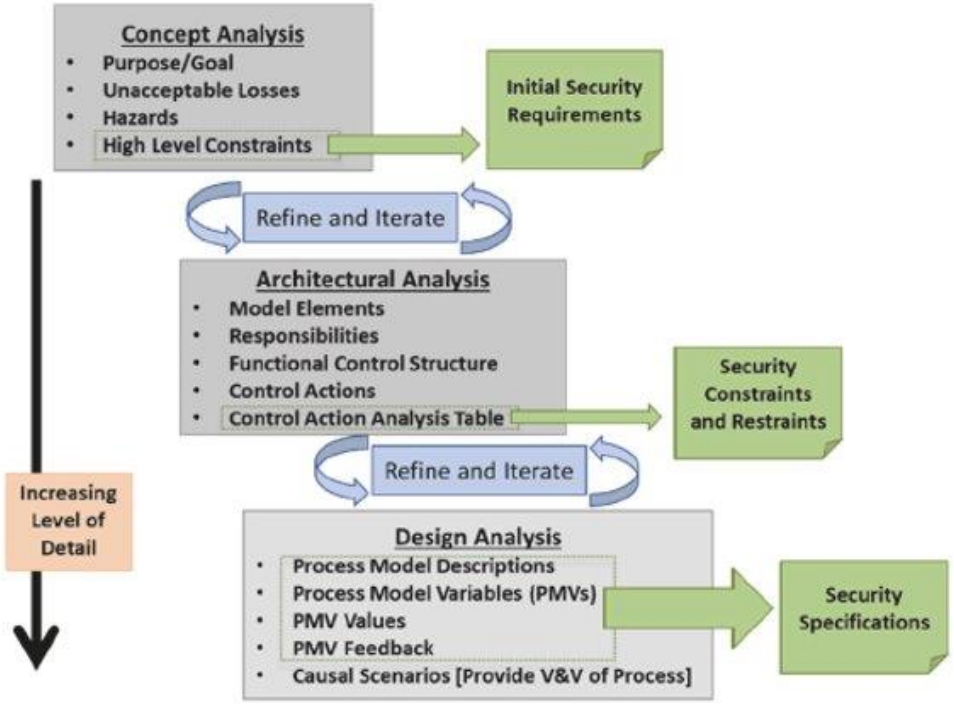


Figure 3: DevSecOps Software Lifecycle

Lam, Thomas. "DoD Enterprise DevSecOps Reference Design." Department of Defense, 2019.

FIG 1. STPA-SEC TAILORED APPROACH.



M. Span, L. Mailloux, R. Mills and W. Young, "Conceptual Systems Security Requirements Analysis: Aerial Refueling Case Study," IEEE Access, 2018.

31st Annual INCOSE
international symposium

virtual event

July 17 - 22, 2021

www.incose.org/symp2021