



SURFACE VEHICLE RECOMMENDED PRACTICE

J3061®

DEC2021

Issued 2016-01
Stabilized 2021-12

Superseded by ISO/SAE 21434

Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

RATIONALE

This SAE Recommended Practice is being stabilized because the technical committee has determined that the using community is moving towards newer technology, processes, and information that are called out in ISO/SAE 21434 and would like to alert users that this new technology exists which may want to be considered for new design. SAE J3061 is being superseded by ISO/SAE 21434.

STABILIZED NOTICE

This document has been declared "Stabilized" by the SAE Vehicle Cybersecurity Systems Engineering Committee and will no longer be subjected to periodic reviews for currency. Users are responsible for verifying references and continued suitability of technical requirements. Newer technology may exist.

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2021 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
<http://www.sae.org>

SAE WEB ADDRESS:

Full document details: SAE J3061_202112

For more information on this standard, visit
https://www.sae.org/standards/content/J3061_202112

Documents

Document Sharing Hub

TABLE OF CONTENTS

1.	SCOPE.....	5
1.1	Purpose.....	6
1.2	When to Apply a Cybersecurity Process.....	6
2.	REFERENCES.....	6
3.	DEFINITIONS AND ACRONYMS.....	8
4.	RELATIONSHIP BETWEEN SYSTEM SAFETY AND SYSTEM CYBERSECURITY	17
4.1	Analogies between System Safety and System Cybersecurity Engineering.....	18
4.2	Unique Aspects of System Safety and System Cybersecurity	18
5.	GUIDING PRINCIPLES ON CYBERSECURITY FOR CYBER-PHYSICAL VEHICLE SYSTEMS (CPS).....	20
5.1	Know Your System's Cybersecurity Potential.....	20
5.2	Understand Key Cybersecurity Principles.....	20
5.3	Consider the Vehicle Owners' Use of the System	21
5.4	Implement Cybersecurity in Concept and Design Phases.....	21
5.5	Implement Cybersecurity in Development & Validation.....	21
5.6	Implement Cybersecurity in Incident Response	22
5.7	Cybersecurity Considerations When the Vehicle Owner Changes	22

6.	CYBERSECURITY PROCESS OVERVIEW	22
6.1	Motivation for a Well-Defined and Well-Structured Process	22
6.2	Process Framework	23
6.2.1	Overall Management of Cybersecurity	23
6.2.2	Concept Phase	25
6.2.3	Product Development	26
6.2.3.1	Product Development: System Level	27
6.2.3.2	Product Development: Hardware Level	28
6.2.3.3	Product Development: Software Level	30
6.2.4	Production, Operation & Service	33
6.2.5	Supporting Processes	33
6.3	Milestone and Gate Reviews	33
7.	OVERALL MANAGEMENT OF CYBERSECURITY	36
7.1	Cybersecurity Culture	37
7.2	Measuring Conformance to a Cybersecurity Process	37
7.3	Identifying and Establishing Communication Channels	38
7.4	Developing and Implementing Training and Mentoring	38
7.5	Operation and Maintenance Activities	39
7.5.1	Incident Response Process	39
7.5.2	Field Monitoring Process	39
8.	PROCESS IMPLEMENTATION	39
8.1	Applying a Cybersecurity Process Separately with Integrated Communication Points to a Safety Process	40
8.2	Applying a Cybersecurity Process in Conjunction with a Safety Process Tailored after ISO 26262	43
8.3	Concept Phase	44
8.3.1	Feature Definition	44
8.3.2	Initiation of Cybersecurity Lifecycle	44
8.3.3	Threat Analysis and Risk Assessment	44
8.3.3.1	Identifying Cybersecurity Goals	45
8.3.4	Cybersecurity Concept	45
8.3.5	Identify Functional Cybersecurity Requirements	45
8.3.6	Initial Cybersecurity Assessment	46
8.3.7	Concept Phase Review	47
8.4	Product Development: System Level	47
8.4.1	Initiation of Product Development at the System Level (Planning)	48
8.4.2	System Level Vulnerability Analysis	48
8.4.3	Refine Functional Cybersecurity Concept into Technical Cybersecurity Concept	48
8.4.4	Specify Technical Cybersecurity Requirements	48
8.4.5	System Design	49
8.4.6	Feature Integration and Testing	49
8.4.7	Verification / Validation of Cybersecurity Technical Requirements	49
8.4.8	Final Cybersecurity Assessment / Cybersecurity Case	50
8.4.9	Final Cybersecurity Review	50
8.4.10	Release for Production	51
8.5	Product Development at the Hardware Level	52
8.5.1	Background	52
8.5.2	Initiation of Product Development at the Hardware Level	52
8.5.3	Hardware Level Vulnerability Analysis	52
8.5.4	Specification of Hardware Cybersecurity Requirements	53
8.5.5	Hardware Cybersecurity Design	53
8.5.6	Hardware Level Integration and Testing	53
8.5.7	Hardware Level Vulnerability Testing and Penetration Testing	54
8.5.8	Verification / Validation of Hardware Cybersecurity Requirements	54
8.5.9	Refine Cybersecurity Assessment	54

8.6	Product Development at the Software Level	55
8.6.1	Initiation of Product Development at the Software Level (Planning)	55
8.6.2	Specification of Software Cybersecurity Requirements	56
8.6.3	Software Architectural Design	56
8.6.4	Software Vulnerability Analysis	57
8.6.5	Software Unit Design and Implementation	58
8.6.6	Software Implementation Code Reviews	58
8.6.7	Software Unit Testing	59
8.6.8	Software Integration and Testing	60
8.6.9	Verification/Validation to Software Cybersecurity Requirements	60
8.6.10	Software Vulnerability Testing and Penetration Testing	60
8.6.11	Refine Cybersecurity Assessment	60
8.7	Production, Operation and Service	61
8.7.1	Production	61
8.7.1.1	Planning	61
8.7.2	Operation, Service (Maintenance and Repair)	61
8.7.2.1	Field Monitoring	61
8.7.2.2	Incident Response	62
8.7.2.3	Execution and Maintenance of an Incident Response Process (15)	64
8.8	Supporting Processes (16)	65
8.8.1	Configuration Management	65
8.8.2	Requirements Management	66
8.8.3	Change Management	66
8.8.4	Documentation Management	67
8.8.5	Quality Management	68
8.8.6	Requirements for Distributed Development (with suppliers)	68
9.	NOTES	69
9.1	Revision Indicator	69
APPENDIX A	Description of Cybersecurity Analysis Techniques	70
APPENDIX B	Example Templates for Work Products	90
APPENDIX C	Examples Using Identified Analyses	92
APPENDIX D	Security & Privacy Controls Description and Application	102
APPENDIX E	Vulnerability Databases and Vulnerability Classification Schemes	108
APPENDIX F	Vehicle Level Considerations	112
APPENDIX G	Current Cybersecurity Standards and Guidelines that may be useful to the Vehicle Industry	115
APPENDIX H	Vehicle Project Awareness	122
APPENDIX I	Security Test Tools of Potential use to the Vehicle Industry	127
Figure 1	Relationship between safety-critical and Cybersecurity-critical systems	17
Figure 2	Relationship between system safety and system Cybersecurity engineering elements	17
Figure 3	Overall Cybersecurity process framework	24
Figure 4	Concept phase activities	25
Figure 5	Relationships between product development at the system, hardware, and software levels	26
Figure 6	V diagram for product development at the system level	27
Figure 7	Product development: system level	28
Figure 8	V diagram showing product development at the HW level and its relationship to product development at the system level	29
Figure 9	Product development: hardware level	30
Figure 10	V diagram for product development at the software level in relation to product development at the system level	31
Figure 11	Product development: software level	32
Figure 12	Possible milestones and gate reviews	34
Figure 13	Gate review activities	36

Figure 14	Concept phase activities with potential communications paths between Cybersecurity and safety activities.....	40
Figure 15	Product development at the system level activities with potential communications paths between Cybersecurity and safety activities.....	41
Figure 16	Product development at the hardware level activities with potential communications paths between Cybersecurity and safety activities.....	42
Figure 17	Product development at the software level activities with potential communications paths between Cybersecurity and safety activities.....	43
Figure 18	Determining functional Cybersecurity requirements.....	46
Figure 19	Example incident response team data sources (15).....	62
Figure 20	Example incident response process.....	64
Figure 21	Phases of the OCTAVE method (21).....	76
Figure 22	OCTAVE allegro roadmap (22).....	76
Figure 23	Workflow of the HEAVENS security model.....	78
Figure 24	Generic attack tree.....	88
Figure 25	Attack tree.....	98
Figure 26	Data flow diagram of on-board diagnostics (OBD) use case.....	99
Figure 27	Relationships between faults, weaknesses, vulnerabilities and exploits.....	109
Table 1	Example incident handling checklist (15).....	65
Table 2	EVITA severity classes.....	71
Table 3	Rating of attack potential and attack probability.....	72
Table 4	Cybersecurity risk graph for privacy, financial, and operational Cybersecurity threats.....	72
Table 5	Controllability classifications of safety-related threats.....	73
Table 6	Portion of risk graph for safety-related threats.....	73
Table 7	Column headings for EVITA method applied at feature level using THROP.....	74
Table 8	Correlation of OCTAVE phases (21) and process steps to NIST SP 800-30 (16).....	77
Table 9	Mapping between STRIDE threats and security attributes.....	79
Table 10	Applying the TL parameters to estimate threat level.....	81
Table 11	Estimating the threat level (TL).....	82
Table 12	Impact level parameter – safety.....	83
Table 13	Impact level parameter – financial.....	83
Table 14	Impact level parameter – operational.....	84
Table 15	Impact level parameter – privacy and legislation.....	85
Table 16	Estimating impact level (IL).....	85
Table 17	Security level based on threat level and impact level.....	86
Table 18	Examples of deriving Cybersecurity requirements.....	86
Table 19	OCTAVE's allegro worksheet 10, information asset risk worksheet.....	90
Table 20	OCTAVE's allegro worksheet 10, risk mitigation section.....	91
Table 21	Example spreadsheet of EVITA risk assessment at feature level.....	93
Table 22	Example of OCTAVE's allegro worksheet 10, information asset risk worksheet - ECU firmware.....	94
Table 23	Example of OCTAVE's allegro worksheet 10, risk mitigation section – ECU firmware.....	95
Table 24	Example of attack tree structure for “malicious intentional vehicle disable”.....	97
Table 25	Threats associated with the OBD use case.....	100
Table 26	Risk rating of the OBD use case based on the HEAVENS methodology.....	100
Table 27	Asset, threat, security attribute and security level for the OBD use case.....	101
Table 28	Sample list of potential security control families & controls for vehicle industry.....	103
Table 29	Sample list of potential privacy control families & controls for vehicle industry.....	107
Table 30	Example on abstraction levels concerning software security issues.....	109
Table 31	Examples of dictionary and terminology sources for vulnerability databases.....	110
Table 32	Examples of Vulnerability Databases.....	110
Table 33	Examples of Vulnerability Classification Schemes.....	111
Table 34	Cybersecurity standards and guidelines that may be useful to the vehicle industry.....	115
Table 35	Vehicle Cybersecurity-relative research projects (2004 to present).....	122
Table 36	Sample categories of security test tools.....	127

1. SCOPE

This recommended practice provides guidance on vehicle Cybersecurity and was created based off of, and expanded on from, existing practices which are being implemented or reported in industry, government and conference papers. The best practices are intended to be flexible, pragmatic, and adaptable in their further application to the vehicle industry as well as to other cyber-physical vehicle systems (e.g., commercial and military vehicles, trucks, busses). Other proprietary Cybersecurity development processes and standards may have been established to support a specific manufacturer's development processes, and may not be comprehensively represented in this document, however, information contained in this document may help refine existing in-house processes, methods, etc.

This recommended practice establishes a set of high-level guiding principles for **Cybersecurity** as it relates to **cyber-physical vehicle systems**. This includes:

- Defining a complete lifecycle process framework that can be tailored and utilized within each organization's development processes to incorporate Cybersecurity into cyber-physical vehicle systems from concept phase through production, operation, service, and decommissioning.
- Providing information on some common existing tools and methods used when designing, verifying and validating **cyber-physical vehicle systems**.
- Providing basic guiding principles on Cybersecurity for vehicle systems.
- Providing the foundation for further standards development activities in vehicle Cybersecurity.

The appendices provide additional information to be aware of and may be used in helping improve Cybersecurity of feature designs. Much of the information identified in the appendices is available but some experts may not be aware of all of the available information. Therefore, the appendices provide an overview of some of this information to provide further guidance on building Cybersecurity into cyber-physical vehicle systems. The objective of the overviews is to encourage research to help improve designs and identify methods and tools for applying a company's internal Cybersecurity process.

Appendices A-C - Describe some techniques for Threat Analysis and Risk Assessment, Threat Modeling and Vulnerability Analysis (e.g., Attack Trees) and when to use them.

Appendices D-I - Provide awareness of information that is available to the Vehicle Industry.

Appendix D - Provides an overview of sample Cybersecurity and privacy controls derived from NIST SP 800-53 that may be considered in design phases.

Appendix E - Provides references to some available vulnerability databases and vulnerability classification schemes.

Appendix F - Describes vehicle-level considerations, including some good design practices for electrical architecture.

Appendix G -Lists current Cybersecurity standards and guidelines of potential interest to the vehicle industry.

Appendix H - Provides an overview of vehicle Cybersecurity-related research projects starting from 2004.

Appendix I - Describes some existing security test tools of potential interest to the vehicle industry.

Refer to the definitions section to understand the terminology used throughout the document.

1.1 Purpose

Just as with system safety, Cybersecurity should be built in to the design rather than added on at the end of development. Building Cybersecurity into the design requires an appropriate lifecycle process from the concept phase through production, operation, service, and decommissioning. This document provides a complete lifecycle process framework that may be tailored to a company-specific process. The process framework described in this document is analogous to the process framework described in ISO 26262 Functional Safety Road Vehicles (1). These two processes are different, but are related and require integrated communications in order to maintain consistency and completeness between an organizations safety process outputs and their Cybersecurity process outputs. An organization is free to maintain separate processes with appropriate levels of interaction between the two processes, or to attempt to directly integrate the two processes. The Cybersecurity process framework described in this document can be tailored to either application (integrated or separate) by individual organizations.

1.2 When to Apply a Cybersecurity Process

For systems that may be considered Cybersecurity-critical cyber-physical vehicle systems, an initial short assessment of potential threats related to, for example, operation, privacy (e.g., PII, eavesdropping), financial, reputation, and an initial estimate of risks can be made to determine if the system being considered should follow a Cybersecurity process. The quick assessment version of a threat analysis and risk assessment to determine applicability of a Cybersecurity process may consist of a short brainstorming and discussion meeting to consider potential threats associated with the feature, and to consider whether the potential risks of the threats may be high enough to warrant following a Cybersecurity process. The risk assessment portion of the initial assessment may be based on experience or expert judgment rather than on a rigorous assessment process. Potential brainstorming could come from knowledge gained by hacker chatter and conferences, previous experiences, checklists, etc. Examples of issues that might be considered in determining the risk include an estimate of the magnitude of the impact, from financial, safety, privacy, or operational aspects, and whether an attack may involve a fleet of vehicles or a single vehicle.

For potential safety-related vehicle features, it is recommended that an initial short assessment of potential safety-related threats be performed to determine if there are any potential high-risk safety-related threats. If the initial assessment indicates that high risk safety-related threats may exist, then a Cybersecurity process should be applied. If the initial assessment does not identify any high risk potential safety-related threats, the Cybersecurity process may not need to be applied with respect to the low-risk safety-related threats; it is up to an organization to determine what is considered low risk and whether low risk safety-related threats need to be addressed. To help ensure that all potential safety-related threats are considered, the Cybersecurity experts should communicate with the safety experts. Note that the basis of decision for following the process is on the identified potential risk of the identified safety-related threats rather than on whether a corresponding potential hazard is ASIL rated (A, B, C, or D). This is because the threat risk for a safety-related threat may be low, while the corresponding hazard may be assessed a high ASIL; there is no direct correspondence between an ASIL rating and the potential risk associated with a safety-related threat.

2. REFERENCES

1. ISO 26262 Part 8 First Edition, "Supporting Processes, Road Vehicles – Functional Safety", 11-15-2011.
2. Barbara J. Czerny. "System Security and System Safety Engineering: Differences and Similarities and a System Security Engineering Process Based on the ISO 26262 Process Framework", SAE Technical Paper 2013-01-1419, SAE World Congress and Exhibition, 2013.
3. B. Potter. 'Microsoft SDL Threat Modelling Tool'. In: *Network Security* 2009.1 (2009), pp. 15–18. ISSN: 1353-4858. DOI:[http://dx.doi.org/10.1016/S1353-4858\(09\)70008-X](http://dx.doi.org/10.1016/S1353-4858(09)70008-X). URL: <http://www.sciencedirect.com/science/article/pii/S135348580970008X> (cit. on p. 37).
4. Iván Arce, Kathleen Clark-Fisher, Neil Daswani, Jim DelGrosso, Danny Dhillon, Christoph Kern, Tadayoshi Kohno, Carl Landwehr, Gary McGraw, Brook Schoenfeld, Margo Seltzer, Diomidis Spinellis, Izar Tarandach, and Jacob West. "Avoiding the Top 10 Software Security Design Flaws", IEEE Computer Society, 2014.

5. Global Alliance, Global Automakers, "Consumer Privacy Protection Principles for Vehicle Technologies and Services", November 12, 2014.
6. NIST, SP 800-88, Revision 1, "Guidelines for Media Sanitization", December, 2014.
7. ISO/IEC 15408 "Information Technology – Security Techniques – Evaluation Criteria for IT Security", (3 Parts).
8. NIST, Version 1, "Framework for Improving Critical Infrastructure Cybersecurity", February 12, 2014.
9. NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations", April 2014.
10. FIPS Pub 199. "Standards for Security Categorization of Federal Information and Information Systems", February 2004.
11. ISO (International Organization for Standardization). "ISO 12207 - Systems and Software Engineering - Software LifeCycle Processes", 2008.
12. ISO (International Organization for Standardization). "ISO/IEC 27001: - Information technology - Security techniques - Information security management systems - Requirements". International Organization for Standardization. 27 January 2015.
13. ISO (International Organization for Standardization). "ISO/IEC 27002: Information Technology - Security Techniques. Code of Practice for Information Security Controls" 2008.
14. ISO (International Organization for Standardization). "ISO/IEC 29119: The International Software Testing Standard", September 10, 2014.
15. NIST 800-61 Revision 2, "Computer Security Incident Handling Guide", August 2012.
16. NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments", September 2012.
17. Chrysler Corporation, Ford Motor Company, General Motors Corporation, QS 9000 Third Edition, "Quality System Requirements", October 1998.
18. ISO/TS 16949:2009 "Quality Management Systems" December 2008.
19. Ruddle, Alastair, Ward, David, *et al*, EVITA Project Deliverable D2.3: "Security requirements for automotive on-board networks based on dark-side scenarios" Version 1.1, 30 December 2009.
20. EVITA deliverable D2.1: "Specification and evaluation of e-security relevant use cases", 2009.
21. Woody, Carol. "Applying OCTAVE: Practitioners Report." Software Engineering Institute, May 2006.
22. Caralli, Richard, James Stevens, Lisa Young, and William Wilson. "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process." Software Engineering Institute, May 2007.
23. M. Islam *et al.*, *Deliverable D2 Security models*. HEAVENS Project, Deliverable D2, Release 1. Dec. 2014.
24. ISO (International Organization for Standardization). *Road vehicles - Functional safety* ISO 26262:2011. (cit. on pp. 17, 30, 40, 42, 44).
25. BSI-Standard 100-4, Version 1.0, 2009, Federal Office for Information Security (BSI), Germany.
26. Automotive Industry Action Group (AIAG), "Potential Failure Mode and Effects Analysis (FMEA)", 2008.
27. "Privacy Impact Assessment Guideline", 2011, Federal Office for Information Security (BSI), Germany.

28. ISO (International Organization for Standardization). *Road vehicles - Functional safety - Part 3: Concept phase (ISO 26262-3:2011)*. ISO 26262-3:2011. 2011 (cit. on p. 18).
29. Schneier, Bruce, "Secrets and Lies – Digital Security in a Networked World", Wiley, ISBN 978-0-471-45380-2.
30. Amer Aijaz¹, Bernd Bochow², Florian D'otzer³, Andreas Festag⁴, Matthias Gerlach², Rainer Kroh⁵ and Tim Leinmüller⁵, "Attacks on Inter Vehicle Communication Systems – an Analysis".
31. http://www7.informatik.uni-erlangen.de/~dulz/fkom/06/Material/11/Security/NOW_TechReport_Attacks_on_Inter_Vehicle_Communications.pdf.
32. Avizienis A, Laprie J-C, Randell B, Lanwehr C, "Basic Concepts and taxonomy of Dependable and Secure Computing", IEEE Transactions on independent and Secure Computing". January-March 2004.
33. MITRE Corporation, "Common Weakness Enumeration, A Community Developed Dictionary for Software Weakness Types ", 2006 -2014, <http://cwe.mitre.org/>.
34. MITRE Corporation, "Common Vulnerabilities and Exposures ", 1999-2014, <https://cve.mitre.org/cve/index.html>.
35. Security Focus, 'BugTraQ', 2010, <http://www.securityfocus.com/archive>.
36. NIST, 'National Vulnerability Database', <http://nvd.nist.gov/>.
37. MITRE Corporation, 'Common Weakness Scoring System', 2006-2014, http://cwe.mitre.org/cwss/cwss_v1.0.1.html.
38. NIST, 'Common Vulnerability Scoring System', <http://nvd.nist.gov/cvss.cfm>.

3. DEFINITIONS AND ACRONYMS

3.1 API

Application Programming Interface

3.2 ASF - Application Security Frame

Threat categorization tool that determines threats based on system break down methodology.

3.3 ASIL - Automotive Safety Integrity Level

A means of classifying hazards in ISO 26262.

3.4 ATTACK POTENTIAL

The likelihood that a potential attack can be successfully carried out.

3.5 ATTACK SURFACE

The different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.

3.6 ATTACK TREE ANALYSIS (ATA)

An analysis method to determine the potential paths that an attacker could take through the system to lead to the top level threat.

3.7 BLACK BOX TESTING

Testing where nothing formal is known about the system being tested. No specifications, hardware information, software code, etc. are provided during the testing.

3.8 CAN - Controller Area Network

A serial communication network. The following standards provide the specifics associated with the CAN protocol and some of its automotive variants: SAE J1939, SAE J2411, ISO 11898, ISO 15765-2.

3.9 CERT C

Secure coding standard for C, C++, Java and Pearl. Developed by the CERT coding initiative team.

3.10 CPU - Central Processing Unit

The part of a computer system (a microcontroller) that performs the computer's main functions and controls parts of the system.

3.11 COMMON VULNERABILITY ENUMERATION (CVE™)

CVE is designed to allow vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services.

3.12 COMMON VULNERABILITY SCORING SYSTEM (CVSS)

Scoring system for vulnerabilities.

3.13 COMMON WEAKNESS ENUMERATION (CWE™)

The CWE is a "formal list of software weakness types" hosted by MITRE cooperation.

3.14 COMMON WEAKNESS SCORING SYSTEM (CWSS™)

Is a scoring system that may help stakeholders concerned with software security - to assess and - where applicable - prioritize reported software weakness.

3.15 CYBER-ATTACK

An assault on system Cybersecurity that derives from an intelligent act, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade Cybersecurity services and violate the Cybersecurity policy of a system.

3.16 CYBER-PHYSICAL SYSTEM (CPS)

A system of collaborating computational elements controlling physical entities.

3.17 CYBER-PHYSICAL VEHICLE SYSTEM (CPAS)

Vehicle embedded control systems where there exists a tight coupling between the computational elements and the physical elements of the system and the environment around the system.

3.18 CYBERSECURITY

Measures taken to protect a cyber-physical system against unauthorized access or attack.

3.19 CYBERSECURITY ASSESSMENT

An assessment of the level of Cybersecurity of a feature that will be refined throughout the development process and provides appropriate arguments and evidence to support Cybersecurity claims at each stage of development. The Cybersecurity assessment is reviewed at each of the major milestones.

3.20 CYBERSECURITY CASE

The final Cybersecurity Assessment after all milestone reviews have been completed and before the feature can be released for production. The Cybersecurity case provides the final argumentation and evidence that the feature as designed and developed satisfies its Cybersecurity goals.

3.21 CYBERSECURITY CONCEPT

Developed in the concept phase to describe the high-level Cybersecurity strategy for the feature. The Cybersecurity concept will be refined to a technical Cybersecurity concept during product development at the system level.

3.22 CYBERSECURITY CONTROLS

The management, operational, and technical controls (e.g., safeguards or countermeasures) prescribed for a feature to eliminate potential vulnerabilities or to reduce the likelihood that a vulnerability will be exploited.

3.23 CYBERSECURITY-CRITICAL

A system where losses could occur in cyber-physical systems due to vulnerabilities in the system that could be exploited either directly or indirectly by an outside entity.

3.24 CYBERSECURITY GOALS

The goals for achieving Cybersecurity for the feature determined from the threat analysis and risk assessment results. These are the highest level Cybersecurity requirements that will drive the development and refinement of functional and technical Cybersecurity requirements.

3.25 CYBERSECURITY MECHANISM

Technical Cybersecurity control added to the feature to eliminate potential vulnerabilities or to reduce the likelihood that a vulnerability will be exploited.

3.26 CYBERSECURITY POTENTIAL

The level of risk or likelihood that something may happen.

3.27 CYBERSECURITY PROGRAM PLAN

Defines responsibilities for planning and overseeing the Cybersecurity activities.

3.28 CYBERSECURITY REVIEW

A review, possibly conducted by a small team of technical reviewers, to assess the technical aspects of the work products during the various stages of the development process.

3.29 DIS

Draft International Standard

3.30 DOD

Department of Defense

3.31 DREAD - Damage Reproducibility Exploitability Affected users and Discoverability

Threat categorization tool that determines threats based on system break down methodology.

3.32 DVD - Digital Video Disc

A device with high storage capacity of information.

3.33 ECU - Electronic Control Unit

A module that provides a function to the vehicle.

3.34 ETHERNET

A serial communication network.

3.35 ETSI

European Telecommunications Standards Institute

3.36 EVITA - E-safety Vehicle Intrusion protected Applications

A project initiated by the European Community from 2007 through 2013. Primarily to design, verify and prototype Cybersecurity building blocks for vehicle on-board networks.

3.37 FEATURE

System or an array of systems to implement a function at the vehicle level to which a Cybersecurity process for cyber-physical vehicle systems is applied.

3.38 FAULT TREE ANALYSIS (FTA)

A deductive analysis technique that starts with a top-level hazard and works down to identify potential single and multi-point failure combinations that can cause the hazard to occur.

3.39 FLEXRAY

A serial communication network.

3.40 FUZZ TESTING

A software testing technique that can be used to find potential security flaws.

3.41 GREY BOX TESTING

Testing where partial information is known about the feature being tested. For example, some feature specifications are provided but the product source code was not provided. Thus, some ad hoc methods are still required to try to determine the vulnerabilities.

3.42 GPS

Global Positioning System, used for navigation.

3.43 HACKER

A person who illegally attempts to gain access to or gains access to a system with the intent to gain something or to cause losses from a stakeholder perspective; e.g., fame, financial, terrorist attack.

3.44 HACKER CHATTER

On line blogs or conventions, etc. where hackers hold conversations about what they try to do.

3.45 HACKER INTRUSION

An unauthorized access.

3.46 HAZOP

Hazard and Operability Analysis, in the context of functional safety, is a structured and systematic technique for identifying potential hazards of a feature; the method uses guidewords and brainstorming to attempt to identify potential hazards.

3.47 HEAVENS

HEAling Vulnerabilities to ENhance Software Security and Safety

3.48 HMI

Human Machine Interface

3.49 HSM - Hardware Security Module

A physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.

3.50 HM

Hardware Module

3.51 IEC - International Electrotechnical Commission

Group authoring industry standards.

3.52 INCIDENT

An attack on the system that may have or may not have been successful.

3.53 ISAC - Information Sharing and Analysis Centers

A central repository for security-related information. The group's purpose is to share each organization's information about Cybersecurity attacks and vulnerabilities among all the members.

3.54 ISO/TS

International Organization for Standardization / Technical Specifications

3.55 I/O

Input / Output

3.56 IT - Information Technology

Resource management activity.

3.57 ITS

Intelligent Transportation System

3.58 JTAG

Port on a microprocessor used to extract data or code from an ECU.

3.59 LIN - Local Interconnect Network

A serial communication network.

3.60 MALICIOUS ACTORS

A person or persons with the intent to identify and exploit vulnerabilities within a feature to achieve access to the feature for personal or group gain; the gains may be for fame, financial, malicious intent, etc.

3.61 MISRA C

A software development standard for the C programming language developed by Motor Industry Software Reliability Association (MISRA). It aims to facilitate code safety, portability, and reliability in the context of embedded systems.

3.62 MOST - Media Oriented Systems Transport

A serial communication network (fiber optic or electrical).

3.63 NIST - National Institute of Standards and Technology

The U.S. Department of Commerce pulls groups of people together to draft standards in various areas of technology.

3.64 NVD - National Vulnerability Database

Contains more than 57000 vulnerabilities entered by NIST.

3.65 OBD-II - On Board Diagnostics Connector

Access point in vehicle to be able to communicate to modules and pull diagnostic information.

3.66 OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation

A threat analysis and risk assessment method for assessing risk in existing enterprise information systems.

3.67 OEM - Original Equipment Manufacturer

A large vehicle manufacturer corporation.

3.68 PENETRATION TESTING

A testing method with the intent to penetrate a feature in order to identify unknown vulnerabilities and to determine vulnerabilities that are not adequately protected. Penetration testing uncovers critical issues and demonstrates how well the feature is protected. Combined with a comprehensive Cybersecurity program, penetration tests can help you reduce the risk of a breach.

3.69 PII - Personally Identifiable Information

Is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

3.70 QS

Quality System. (e.g., QS 9000)

3.71 RAM

Read Access Memory

3.72 ROM

Read Only Memory

3.73 RISK ANALYSIS METHOD

A process for analyzing the potential risk of identified threats with respect to the severity of the possible outcome of an attack and the likelihood that a potential attack can be successfully carried out (the attack potential).

3.74 SAE

Society of Automotive Engineers

3.75 SAFETY-CRITICAL SYSTEMS

A system that may cause harm to life, property, or the environment if the system does not behave as intended or desired.

3.76 SCADA

Supervisory Control and Data Acquisition is a system operating with coded signals over communication channels so as to provide control of remote equipment.

3.77 SDL - Security Development Lifecycle

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.

3.78 SEI

Software Engineering Institute at Carnegie Mellon.

3.79 STAKEHOLDER

A group, organization or member that can affect or can be affected by an organizations actions.

3.80 SQL

Structured Query Language is a special-purpose programming language designed for managing data held in a relational database management system (RDBMS).

3.81 STRIDE

Threat modeling technique by Microsoft. Stands for Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

3.82 SW

Shorthand for Software.

3.83 SYSTEM

A collection of hardware and software to perform a function or functions in a vehicle.

3.84 SYSTEM CONTEXT

To define the interfaces between the system's hardware and software, the key data flows, storage and processing within the system.

3.85 TECHNICAL PHASE REVIEW

A technical phase review is used at the end of a development phase to review the technical activities performed and the technical documents created during the development phase; for example, a Concept Phase Technical Review would be performed at the completion of the concept phase of development to help ensure that the technical activities and documents generated during the concept phase are correct, consistent, complete, etc. The technical phase review is best performed by a technical review board consisting of a small team of technical experts (3-4). The work products being reviewed should be provided to the review board members at least 2-3 weeks prior to the review board meeting.

3.86 TECHNICAL CYBERSECURITY CONCEPT

The high-level Cybersecurity strategy defined into engineering terms.

3.87 TECHNICAL REVIEW

A review of the technical correctness, technical completeness, and technical consistency of the work products developed as part of a Cybersecurity process. A technical review may be performed as each individual analysis activity or work product is completed, or at set gate review points throughout the development lifecycle. This review may be done by a technical review board of a small number of (e.g., 3-4) technical experts and the work product or analysis activity being reviewed should be provided to the review board members enough in advance (e.g., two to three weeks) of the technical review to allow the review board ample time to review the work products.

3.88 TARA - Threat Analysis and Risk Assessment

An analysis technique that is applied in the concept phase to help identify potential threats to a feature and to assess the risk associated with the identified threats. Identifying the potential threats and assessing the risk associated with these threats, allows an organization to prioritize follow-on Cybersecurity activities associated with the threats so efforts and resources can be focused on the highest priority threats.

3.89 TATRC

Telemedicine and Advanced Technology Research Center.

3.90 TIER 1

A supplier sourced directly by a vehicle manufacturer for a given product. The supplier has a direct business agreement with the vehicle manufacturer.

3.91 THREATS

A circumstance or event with the potential to cause harm, where harm may be with respect to financial, reputation, privacy, safety, or operational.

3.92 THROP - Threat and Operability Analysis

An analysis technique that applies guidewords to identified primary functionality of a feature to identify potential threats associated with the feature. A THROP parallels a HAZOP except that it considers potential threats rather than potential hazards.

3.93 TRUST BOUNDARY

A boundary where program data or execution changes its level of "trust". An example of an execution trust boundary would be where an application attains an increased privilege level (such as root). A data trust boundary is a point where data comes from an untrusted source.

3.94 TVRA

Threats, Vulnerabilities and Risks (TVR) of a system to be analyzed. A TARA method.

3.95 Unauthorized Access

If a user attempts to access an area of a system they should not be accessing. When attempting to access that area, they would be denied access.

3.96 USB - Universal Serial Bus

A means to store and communicate information to others.

3.97 VALIDATION

The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers. Contrast with verification.

3.98 VERIFICATION

The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process. Contrast with validation.

3.99 VULNERABILITY ANALYSIS

Vulnerability analysis techniques attempt to identify and classify potential Cybersecurity vulnerabilities or holes in the software and hardware of the feature being developed that may be exploited by an attacker.

3.100 WELL DEFINED AND WELL STRUCTURED (WDWS) PROCESS

Establishes a repeatable, structured method to systematically identify and assess threats, and vulnerabilities that could be exploited to achieve a threat, and appropriate Cybersecurity Controls to design in to the system during development to protect against the identified vulnerabilities.

3.101 WHITE BOX TESTING

Testing where full information is known about the feature being tested. Detailed specifications and source code is available during the testing.

4. RELATIONSHIP BETWEEN SYSTEM SAFETY AND SYSTEM CYBERSECURITY¹

System safety (beyond regulatory requirements) is the state of a system that does not cause harm to life, property, or the environment. System Cybersecurity is the state of a system that does not allow exploitation of vulnerabilities to lead to losses, such as financial, operational, privacy, or safety losses. A safety-critical system is a system that may cause harm to life, property, or the environment if the system does not behave as intended or desired. A Cybersecurity-critical system is a system that may lead to financial, operational, privacy, or safety losses if the system is compromised through a vulnerability that may exist in the system. All safety-critical systems are Cybersecurity-critical since a cyber-attack either directly or indirectly on a safety-critical system could lead to potential safety losses (Figure 1). Not all Cybersecurity-critical systems are safety-critical since cyber-attacks on Cybersecurity-critical systems can result in losses other than safety losses; namely, privacy, operational, or financial.

The two domains are also related in that there is some overlap between the elements of system safety engineering and the elements of system Cybersecurity engineering, but the elements are not identical between the two engineering disciplines (Figure 2). An example of a Cybersecurity-critical system that is not safety-critical is an entertainment system that obtains personal information from the driver. If this system is compromised, it may lead to financial or privacy losses to the driver, however, it most likely would not cause physical harm to the driver; thus, the system is Cybersecurity-critical, but not safety-critical. An example of a system that is both Cybersecurity-critical and safety-critical is a steering assist system. A steering assist system is safety-critical since if it exhibits malfunctioning behavior it could lead to potential harm to the vehicle occupants. The steering assist system is also Cybersecurity-critical since if the system is compromised by an attacker and a malicious intentional steering maneuver is injected, this could also lead to potential harm to the vehicle occupants; in Cybersecurity, this would be analyzed as a potential safety loss.

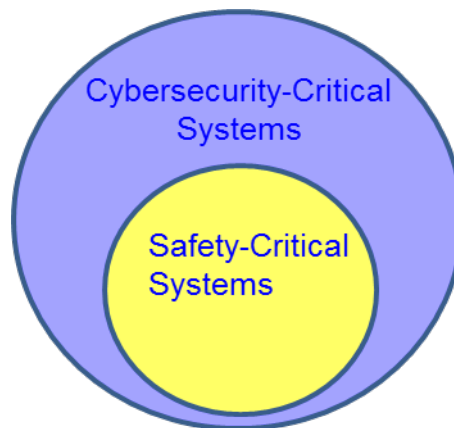


Figure 1 - Relationship between safety-critical and Cybersecurity-critical systems

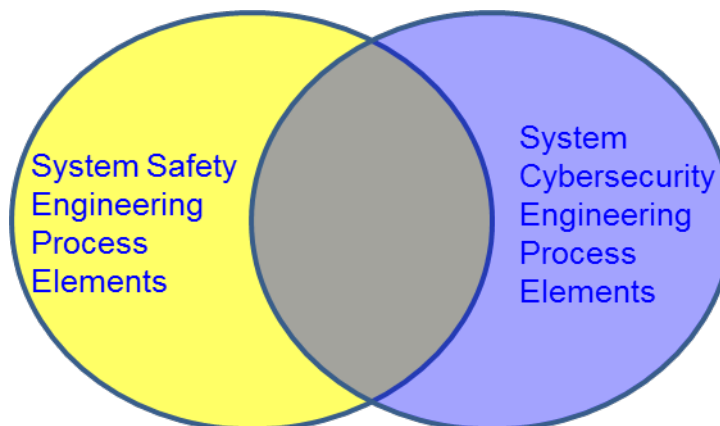


Figure 2 - Relationship between system safety and system Cybersecurity engineering elements

1. The information in this chapter was taken from: SAE Technical Paper 2013-01-1419 – System Security and System Safety Engineering: Differences and Similarities and a System Security Engineering Process Based on the ISO 26262 Process Framework (2).

4.1 Analogies between System Safety and System Cybersecurity Engineering

The objectives of system safety and system Cybersecurity engineering are analogous to each other. The goal of both engineering activities is, if possible, to build safety into the design, or to build Cybersecurity into the design, rather than attempting to add safety and Cybersecurity on to an existing design. The systems engineering aspect is important in both system Cybersecurity and system safety. However, in Cybersecurity, there can be a tendency to only consider the problem to be one of simply adhering to best practices (e.g., authentication and cryptography), and ignoring the system engineering aspects. This section uses the term “system” in front of Cybersecurity to stress a systems approach to Cybersecurity as described in this Recommended Practice.

The process elements of system safety and system Cybersecurity engineering are also analogous to each other. In the concept phase of a system safety engineering process, a hazard analysis and risk assessment is performed. Analogous to this in a system Cybersecurity engineering process, a threat analysis and risk assessment is performed during the concept phase. In the requirements phase of a system safety engineering process, safety requirements are derived and refined from the safety goals identified in the hazard analysis and risk assessment. Likewise, in the requirements phase of a system Cybersecurity engineering process, Cybersecurity requirements are derived and refined from the Cybersecurity goals identified in the threat analysis and risk assessment. In the design phase of a system safety engineering process, detailed hazard analysis is performed on the highest risk hazards to help identify controls or safety mechanisms to help eliminate the potential hazards, or to help mitigate the consequences should a potential hazard occur. Likewise, in the design phase of a system Cybersecurity engineering process, detailed vulnerability analysis is performed on high risk identified threats to help identify Cybersecurity controls to apply to help reduce the likelihood of a successful attack. Analogies between process elements continue through product development and verification/validation. Though there are many similarities among the process elements between system safety and system Cybersecurity engineering, the underlying application of the process elements may be unique between the two engineering disciplines.

Suggestions for maintaining consistency between safety & Cybersecurity include:

- Build appropriate checkpoints into the product lifecycle of both processes.
- Use a **Risk Analysis Method** to help guide the corporation to address the threats of highest riskBuild Cybersecurity awareness and interface or communication points into existing processes and forums.
- Identify, establish and distribute the various communication paths between safety and Cybersecurity.

4.2 Unique Aspects of System Safety and System Cybersecurity

System safety and system Cybersecurity are unique from each other. Whilst system safety focuses on analyzing the system for potential hazards so that safety mechanisms can be identified and integrated into the design to address the causes of the potential hazards and to reduce the risk associated with those potential hazards, system Cybersecurity considers potential threats posed by an attacker whose goal is to cause harm, wreak havoc, gain financial or other benefits, or simply to gain notoriety.

Though there are analogies between “hazard analysis and risk assessment” and “threat analysis and risk assessment,” the response to identified hazards is different from the response to identified threats. Since potential threats involve intentional, malicious, and planned actions, they are more difficult to address than potential hazards. Addressing potential threats fully, requires the analysts to think like the attackers, but it can be difficult to anticipate the exact moves an attacker may make. Predicting an attacker’s moves, however, helps the analysts to know what Cybersecurity controls are appropriate for protecting against the attacker’s possible actions. In system safety, analysts can more readily identify the potential hazards, identify the potential causes and take appropriate action to mitigate the potential consequences, or to eliminate the potential hazards all together. The reason is that causes of potential hazards can be determined based on experience, knowledge of the system, components, and interactions, etc., and potential causes may be unique for particular systems, but are not unknown. In addition, with respect to safety, statistics may be used for claiming an acceptable level of risk. However, this may not be the case for Cybersecurity. For Cybersecurity, statistics or statistical analysis techniques may need to be employed in some manner due to the large amount of unknown information likely to be part of a Cybersecurity analysis, however, these techniques are likely fundamentally different than the empirical techniques that can be used based on experience in safety-related systems.

A further difference between hazard analysis and risk assessment and threat analysis and risk assessment is that additional factors are considered with respect to threats and the risks associated with threats, that need not be considered with respect to hazards and the risks associated with hazards. These additional factors to consider in assessing the risks of potential threats include the knowledge required by an attacker (proprietary or publically available), the experience level of an attacker, the access to the system that is required by an attacker, an attacker's need for special equipment, etc. None of these factors need be considered in assessing the risks of potential hazards.

Another unique aspect with respect to system Cybersecurity and system safety is that with system Cybersecurity a broader focus is considered. In system safety the focus is on safety-critical systems, whereas in system Cybersecurity, both safety-critical and non-safety-critical systems are considered. System Cybersecurity considers both safety-critical and non-safety-critical systems since threats may be non-safety-related (e.g., financial, privacy, operational), it may be possible to access a safety-critical vehicle system from non-safety-critical vehicle systems (e.g., in-vehicle entertainment systems). In addition, any safe state identified as part of the system safety engineering analyses needs to be considered with respect to Cybersecurity to assess whether that safe state could be exploited by an attacker. Even if exploiting safe states seems acceptable and would not lead to a safety threat, it should also be evaluated to determine if it could result in denial of service of another feature. It is possible that a safe state may have some potential risk associated with it; these safe states could be exploited by an attacker and may lead to a safety threat that would need to be analyzed from a Cybersecurity perspective. Thus, traditional hazard controls are not sufficient as Cybersecurity controls and as stated, may be used against a system by causing a denial of service or a potential safety-related threat to occur.

With respect to detailed hazard analysis and vulnerability analysis, the analysis techniques may be analogous to each other, but the methods and goals are unique. For example, a detailed hazard analysis technique may utilize **Fault Tree Analysis (FTA)**. Similarly, in system Cybersecurity, a detailed threat analysis technique may utilize **Attack Tree Analysis (ATA)**. Though the methods are analogous to each other, they are unique. In Fault Tree Analysis the analyst identifies potential causes of the top hazard event and looks for single-point and multi-point random hardware failures that can lead to the top-level hazard. Attack Tree Analysis is not concerned with single-point and multi-point random hardware failures, but rather with determining potential paths that an attacker could take through the system to lead to the top level threat. The underlying goals are synonymous – in FTA the goal is to identify single and multi-point random hardware failures that may lead to the top hazard so safety mechanisms can be added to detect and mitigate potential causes, and in ATA the goal is to identify potential vulnerabilities that could be exploited to lead to the top level threat so that Cybersecurity controls can be identified to eliminate the vulnerabilities or to make them more difficult to exploit.

In the implementation and verification/validation stages, static code analysis used in system safety is used to help identify bugs that directly affect primary functionality. In system Cybersecurity, static code analysis is used to identify potential Cybersecurity vulnerabilities in the code. Valid or correct code from a safety perspective may still have Cybersecurity vulnerabilities.

Finally, some verification/validation methods for Cybersecurity are different and more difficult than verification/validation methods used in system safety. For example, in system safety fault injection tests are performed to verify that the identified faults are detected and that the appropriate response occurs, however, in Cybersecurity there is no particular fault that can be injected to see if the system vulnerabilities are closed. Cybersecurity relies on attack (vulnerability) testing or penetration testing vs. fault injection testing. In penetration testing, a pseudo attacker(s) attempts to identify and exploit vulnerabilities in the system. This is clearly not as straightforward as fault injection testing. Penetration testing is also not intended to confirm that the correct response (i.e., specific Cybersecurity controls added to the design) has been made relative to a potential vulnerability. Alternatively, traditional structured testing of the effectiveness of Cybersecurity Controls (which can confirm that the design meets its requirements) is not sufficient to address black-hat out-of-the-box types of attack. Cybersecurity may use both traditional structured testing and penetration testing to address the unpredictability of attacker methods.

A more general difference between Cybersecurity and safety is that Cybersecurity risks evolve over time as attacker's motivations and capabilities change. This makes Cybersecurity especially difficult, since it involves defense against techniques that may not be understood at the time the system is created.

It is also possible for safety and Cybersecurity to conflict with each other in some cases. For example, Cybersecurity countermeasures can conflict with safety requirements and vice versa. Systems engineering principles consider the overall integration of requirements for the system that includes integrating Cybersecurity and safety requirements. To help maintain consistency and completeness between safety and Cybersecurity, various communications points between safety and Cybersecurity should be identified and established. Also appropriate checkpoints or gate reviews should be added in the product lifecycle between safety and Cybersecurity.

5. GUIDING PRINCIPLES ON CYBERSECURITY FOR CYBER-PHYSICAL VEHICLE SYSTEMS (CPS)

The Guiding Principles for Cybersecurity presented in this section are intended to work for a wide variety of companies in the vehicle industry. Since each company is likely to have its own internal processes by which it manages its product development, this Recommended Practice provides a set of guiding principles with respect to Cybersecurity that can be applied by any organization within a company. The following guiding principles are tailored for cyber-physical vehicle systems Cybersecurity from Microsoft's **Security Development Lifecycle (SDL)** guiding principles (3), and IEEE's **Avoiding the Top 10 Software Security Design Flaws** (4). In addition to these guiding principles, identify legislation or regulatory requirements that may be applicable with respect to Cybersecurity.

5.1 Know Your System's Cybersecurity Potential

It is very important to understand what the potential Cybersecurity vulnerabilities are for your system (e.g., attack surfaces that can be identified by conducting the appropriate vulnerability analyses). The concept phase for system development should consider what defense to use for these potential vulnerabilities. For example:

- Will there be any Sensitive data and/or Personally Identifiable Information (PII) stored on, or transmitted by, your system that could make your system a target?
- What role does your system have (if any) in the safety-critical functions of a vehicle?
- What communications or connections will your system have with entities that are external to the vehicle's electrical architecture?
- Can your system be used as a "stepping stone" to an attack on another system?
- Can information about your system (e.g., timing, power consumption) be used to mount a side channel attack?
- Conduct the appropriate Threat Analysis and Risk Assessment.

5.2 Understand Key Cybersecurity Principles

The following lists some key principles relative to Cybersecurity for cyber-physical systems.

- Protect Personally Identifiable Information (PII) and Sensitive data: One potential reference source that provides guidance on how to do this can be found in the Auto Alliance and Global Automakers Consumer Privacy Protection Principles (5). PII stored on the vehicle should be protected, and access to stored PII data should be controlled and limited:
 - Utilize conservative default access settings for customers' data.
 - Obtain appropriate consent from the responsible body before collecting or transferring any data.
 - Prevent **unauthorized access** by protecting customers' data stored in access control lists.
- Use the principle of "Least Privilege" - All components run with the fewest possible permissions.
- Apply "Defense in Depth", particularly for the highest risk threats. This means that threat mitigation should not rely on only a single Cybersecurity Control while leaving other vulnerabilities in the system that could be exploited if the primary Cybersecurity control is penetrated.

- Prohibit changes to calibrations and/or software that have not been thoroughly analyzed and tested.
- Prevent vehicle owners from intentionally or unintentionally making unauthorized changes to the vehicle's systems that could introduce potential vulnerabilities. Some ways vehicle owners may introduce vulnerabilities include:
 - "Tuners" who change calibration settings and/or software to get different powertrain performance features,
 - Software from devices such as **DVD's**, Bluetooth-paired phone's, etc. that may attempt to install itself via the vehicle's entertainment systems, without informing the user or telling the users about possible risks. The installed software may not have malicious intent, however, it may have vulnerabilities that may be exploited.

5.3 Consider the Vehicle Owners' Use of the System

Consider how your system will be used by the owner of the vehicle your system will be in.

- Minimize data collection. Collect the minimum amount of personal data that is required for a particular purpose, and use the least sensitive form of that data (e.g., User name is less sensitive than social security number).
- Enable user policy and control. Enable owners to manage privacy settings on their vehicle systems, provide authorization where applicable, and update/revoke authorization when they wish. Also enable manufacturers to manage privacy settings for their operations.
- Protect the storage, usage, and transfer of PII. Ensure that data usage complies with uses communicated to the OEM and the vehicle owners.
- Provide appropriate notice about data that is collected, stored, or shared so that owners can make informed decisions about their personal information.
- Develop appropriate material for dealerships, customer assistance help lines, websites, and owner's manuals. The goal of this material is to set customer expectations relative to data privacy, and to inform them of the capabilities and limitations of the systems, as well as promote general cybersecurity practices.

5.4 Implement Cybersecurity in Concept and Design Phases

- Design the feature with Cybersecurity in mind, starting in the concept phase of the development lifecycle. Engineers should consider Cybersecurity when defining the requirements that are to be met for the system and feature(s).
- Analyze threats (i.e., initiated external or internal to the system) to determine what will be faced by the system. For the determined threats, identify any vulnerabilities and determine the appropriate Cybersecurity controls.
- Implement Cybersecurity analysis (and management tools) that enable engineers to determine and configure the optimal Cybersecurity level for the system.

5.5 Implement Cybersecurity in Development & Validation

- Have status reviews to assess whether design work is on track to meeting the Cybersecurity requirements. For any Cybersecurity requirements that are at risk of not being met, work with appropriate stakeholders to develop a plan to resolve the open issues.
- Conduct testing to confirm the requirements that were established for Cybersecurity have been met in the feature.
- Ensure that any risks associated with the mechanism for doing re-flashes to the feature/vehicle software are minimized or eliminated.

5.6 Implement Cybersecurity in Incident Response

- Revise (or create) an Incident Response Process that comprehends both the tracking of, and the response to, Cybersecurity incidents. This Incident Response Process should emphasize the importance of responding promptly to reports of Cybersecurity vulnerabilities/incidents, and of communicating information about security updates to affected users and stakeholders. These Incident Response processes need to be documented and published.
- Determine how software and/or calibration updates will be made if there is an incident. For example, if a secure Over-the-Air (OTA) mechanism is available, that method could be used to make authorized modifications of calibrations and/or software.

5.7 Cybersecurity Considerations When the Vehicle Owner Changes

The vehicle owner changes when a vehicle owner sells their vehicle, when a vehicle is totaled in an accident and goes to a salvage yard, when a dealer's demo vehicle needs to be prepared for sale to a customer, etc. To plan for when the vehicle owner changes:

- Determine whether there are any systems on the vehicle that have software or Customer Personal Information that might need to be erased to protect the customer and/or to protect the organization (e.g., immobilizer, cell phone pairing).
- Provide a method to remove personal information from vehicle systems when change of ownership and/or end of vehicle life occurs. This should be described in the Vehicle Owner's/Operator's Manual or in instructions for vehicle service providers. See NIST Special Publication 800-88, "Guidelines for Media Sanitization" (6), for information on methods for cleansing the storage media.

6. CYBERSECURITY PROCESS OVERVIEW

6.1 Motivation for a Well-Defined and Well-Structured Process

As with system safety, Cybersecurity should be built in to the system rather than added on at the end of development. Attempting to add Cybersecurity on to an existing system, or using an ad-hoc approach to identify and implement Cybersecurity Controls can lead to:

- Unneeded Cybersecurity Controls that require valuable limited resources (cost and engineers) to identify, develop, and implement,
- Incorrect Cybersecurity Controls,
- Incomplete or inconsistent Cybersecurity Controls,
- Unintentional insertion of additional and unknown vulnerabilities.

No system can be guaranteed to be 100% secure. However, following a well-defined and well-structured process provides a means to help reduce the likelihood of a successful attack. A **well-defined and well-structured (WDWS)** process establishes a repeatable, structured method to systematically identify threats, vulnerabilities that could be exploited to achieve a threat, and appropriate Cybersecurity Controls to design in to the system during development to protect against the identified vulnerabilities. A WDWS process provides guidance throughout the entire life-cycle, from concept phase through production, operation, and service.

Reducing the likelihood of a successful attack can be likened to reducing the likelihood of potential hazards. To reduce the likelihood of potential hazards from occurring, the vehicle industry applies the principles of system safety engineering in the design and development of **safety-critical** systems. In a similar way, to reduce the likelihood of successful **cyber-attacks** on vehicles, the vehicle industry may apply principles of system Cybersecurity engineering to the design and development of Cybersecurity-critical cyber-physical vehicle systems.

6.2 Process Framework

Figure 3 shows an overall Cybersecurity engineering process framework for cyber-physical vehicle systems that considers the entire lifecycle from concept phase through production, operation, and service. The lifecycle shown in the figure is analogous to the process framework from ISO 26262 Functional Safety Road Vehicles standard (1). This analogous lifecycle is chosen to allow organizations with safety processes based on ISO 26262 to use a common framework between Cybersecurity and safety to facilitate:

- Development of a tailored Cybersecurity process by capitalizing on aspects of an organization's existing safety process that are common to both Cybersecurity and safety, for example, the supporting process procedures and templates,
- Maintaining consistency between Cybersecurity and safety given the interrelationships between the two areas.

The process framework consists of the management of Cybersecurity, the core Cybersecurity engineering activities, and the supporting processes. The core Cybersecurity engineering activities include concept phase activities, activities for product development at the system, hardware, and software levels, and production, operation, and maintenance activities. Supporting process activities include activities that are applicable across different life-cycle phases, such as configuration management, change management, etc.

6.2.1 Overall Management of Cybersecurity

Management of Cybersecurity consists of two aspects: 1.) the overall management of Cybersecurity; and 2.) management of Cybersecurity activities within specific stages of the development lifecycle. Part of the overall management of Cybersecurity includes:

- Creating, fostering, and sustaining a Cybersecurity culture that supports and encourages effective achievement of Cybersecurity within the organization,
- Establishing methods to help ensure compliance to an adopted Cybersecurity engineering process,
- Identifying and establishing needed communication channels with respect to Cybersecurity, both internally and externally,
- Development and implementation of training and mentoring to achieve a competence in Cybersecurity for cyber-physical vehicle systems,
- Incorporating an expanded field monitoring process that includes monitoring **hacker chatter** (including online and at conferences where potential attacks/vulnerability conversations may occur), reporting unsuccessful attacks, etc.,
- Incorporating an incident response process is important and should include an attack incident reporting procedure, and attack incident investigation, resolution, and action procedures.

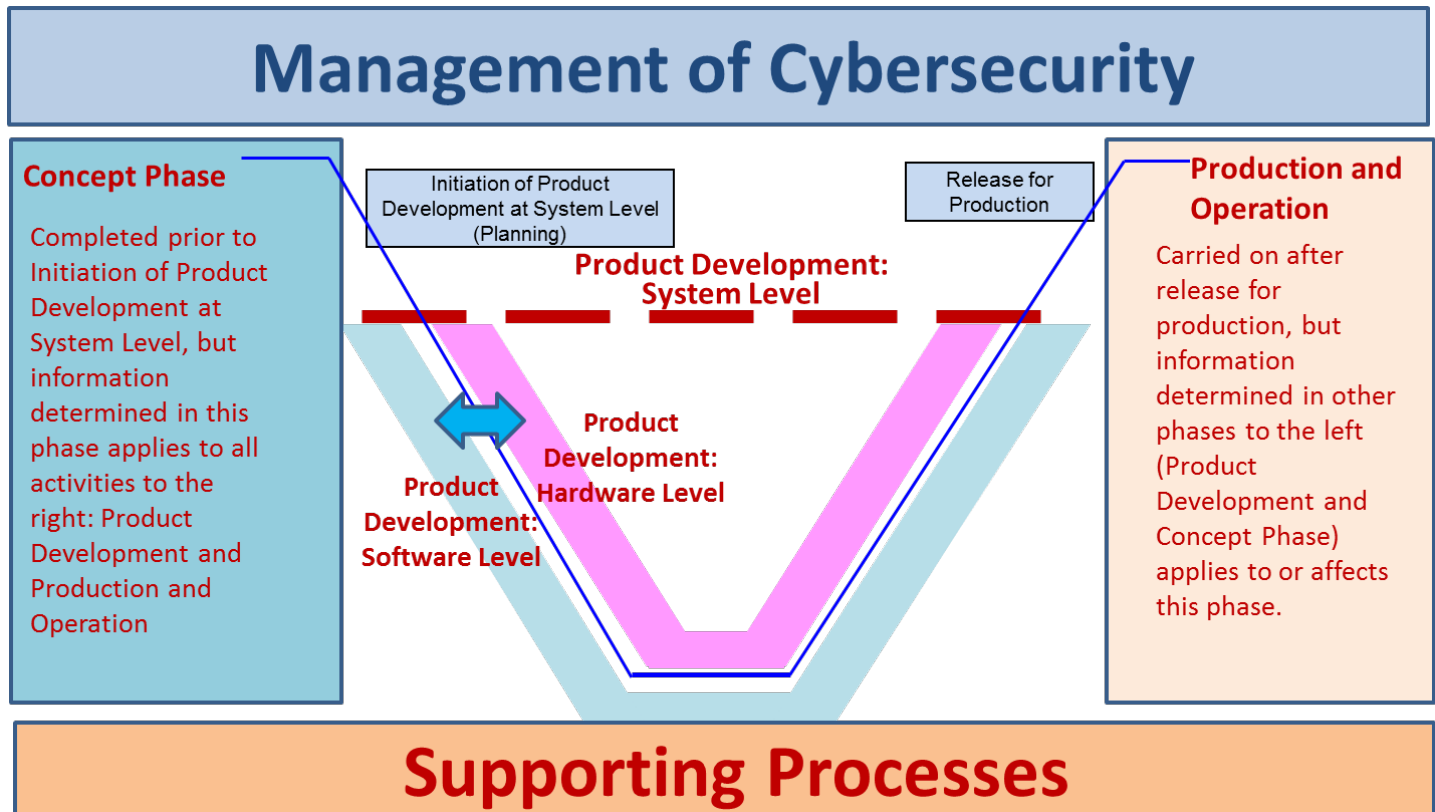


Figure 3 - Overall Cybersecurity process framework

In the concept phase, management of Cybersecurity activities may include assigning a Cybersecurity manager to oversee the Cybersecurity activities, and to be responsible for planning and overseeing the Cybersecurity activities, including developing a **Cybersecurity Program Plan**.

During product development, management of Cybersecurity activities may include:

- Beginning a preliminary **Cybersecurity assessment** that will be refined throughout the development process and reviewed at major milestones and will culminate into the final Cybersecurity assessment (**Cybersecurity case**),
- Identifying and overseeing reviews to confirm that the appropriate activities are performed correctly.

Any open issues with respect to Cybersecurity would be recorded and appropriate follow-up action stated. If open Cybersecurity issues were contained in a previous Cybersecurity assessment, these should be addressed in the updated assessment. The final Cybersecurity issue assessment is the Cybersecurity Case. In the Cybersecurity Case, any open Cybersecurity issues would be resolved, or a rationale would be included stating why the open issue is acceptable, and the final arguments and evidence to support the claims would be provided.

6.2.2 Concept Phase

Figure 4 shows the flow of activities during the concept phase. The **feature** definition activity is to define the feature being developed, including identifying the boundaries and the Cybersecurity perimeter, and identifying the external dependencies and assets. Defining the feature clarifies the boundaries and scope for the future analysis activities. A well-defined scope helps to bound future analysis activities so the analyses can be completed more efficiently and effectively.

The initiation of the Cybersecurity lifecycle includes development of the Cybersecurity Program Plan that describes the activities to be carried out as part of the Cybersecurity lifecycle. The **Threat Analysis and Risk Assessment (TARA)** activity is used to identify and assess the potential threats to the system and to determine the risk associated with each identified threat. The TARA results will drive future analysis activities by focusing future analyses on the highest risk Cybersecurity threats.

Cybersecurity goals are determined for the highest risk potential threats. At the highest level, Cybersecurity goals may be the inverse of the potential threat; for example, if a potential threat is malicious braking, the highest level Cybersecurity goal may be to prevent or reduce the likelihood of malicious braking from occurring, or mitigate the potential consequences of malicious braking. Once the Cybersecurity goals are determined for the highest level threats, a **Cybersecurity Concept** can be developed to describe the high-level Cybersecurity strategy for the feature.

From the Cybersecurity Concept and the Cybersecurity goals, the high-level Cybersecurity requirements can be identified and derived. These high-level Cybersecurity requirements can then be refined further in the product development stages. At the end of the concept phase a preliminary Cybersecurity Assessment may be performed to assess the state of Cybersecurity that is proposed for the feature.

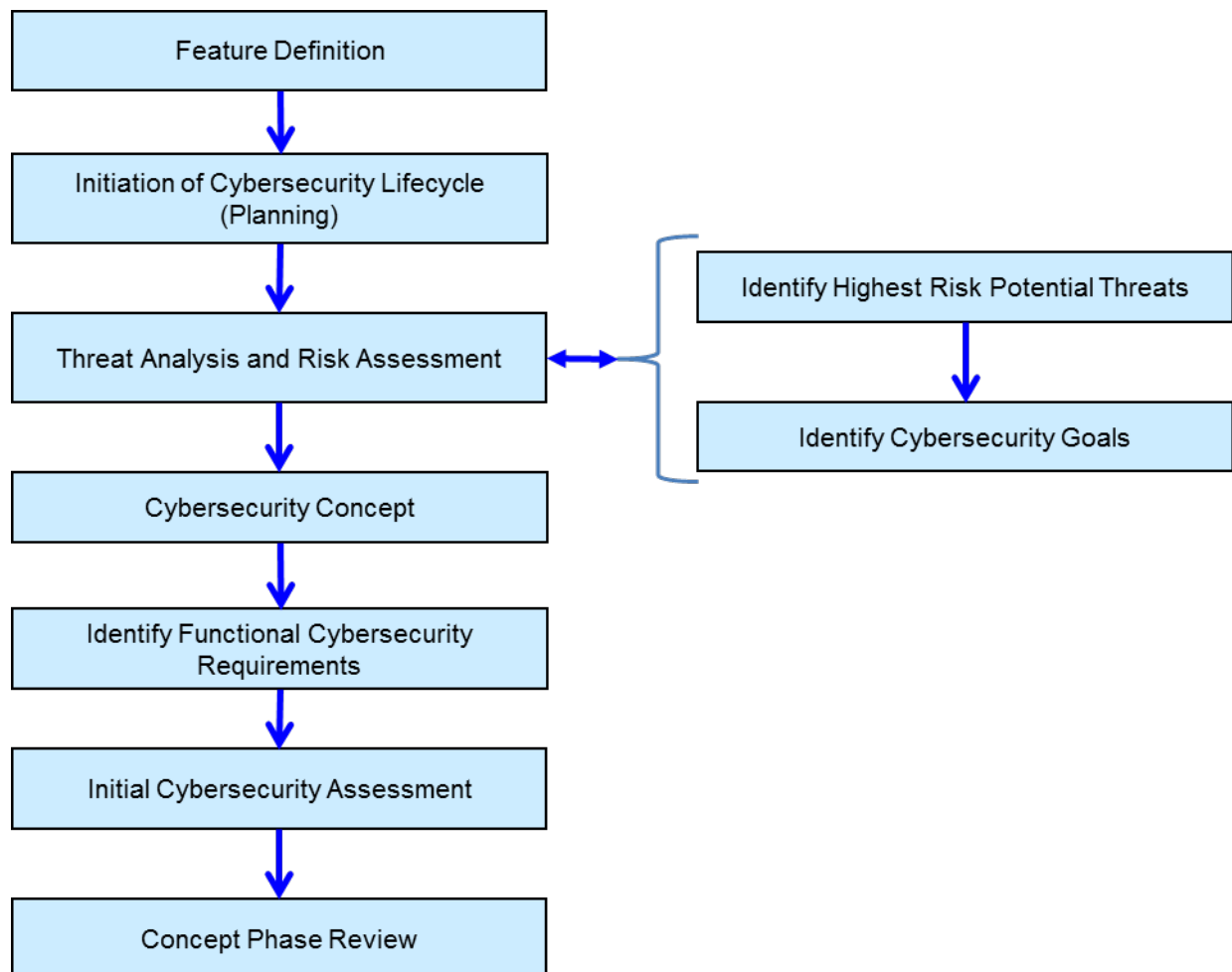


Figure 4 - Concept phase activities

6.2.3 Product Development

The Product Development phase of the lifecycle consists of product development at the system level, product development at the hardware level and product development at the software level.

Figure 5 shows an overview of the product development phase, and the relationships between product development at the system-level design phase and product development at the hardware and software levels.

NOTE: Iteration occurs throughout many phases of the lifecycle; however, these iterations are not depicted to avoid over-complicating the diagrams.

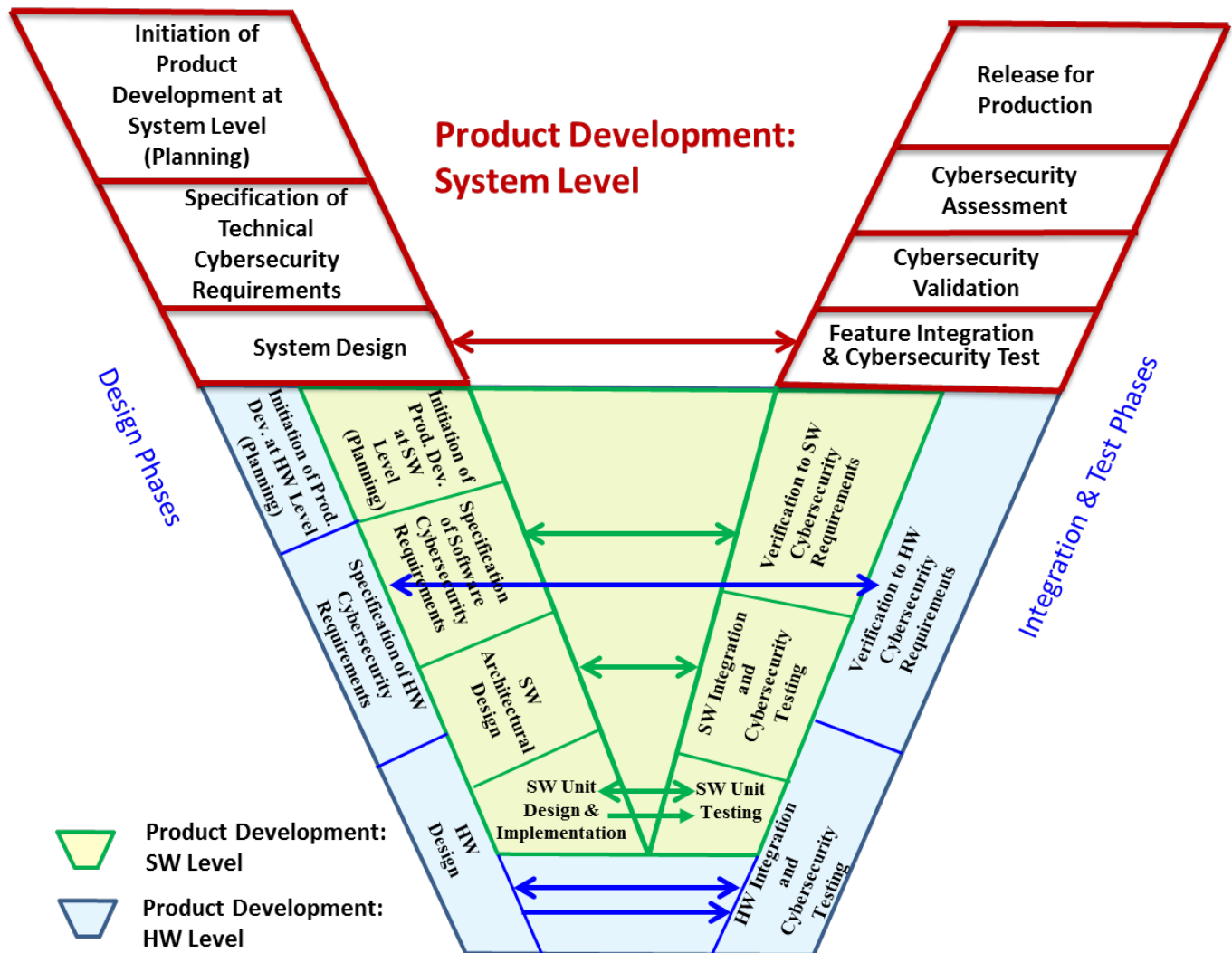


Figure 5 - Relationships between product development at the system, hardware, and software levels

6.2.3.1 Product Development: System Level

Figure 6 shows a V diagram for product development at the system level. During product development at the system level, the Cybersecurity Concept is refined into a **Technical Cybersecurity Concept** (i.e., the high-level Cybersecurity strategy described in the Cybersecurity Concept is refined into engineering terms). To help refine the Cybersecurity Concept into the Technical Cybersecurity Concept, a system level threat analysis or vulnerability analysis may be performed if there is significant new information available. Technical Cybersecurity requirements are then derived and refined from the high-level Cybersecurity requirements and the technical Cybersecurity strategy.

A **System Context** (hardware/software interface document) may be created to define the interfaces between the system's hardware and software, the key data flows, and storage and processing within the system. Using the System Context, the system-level technical Cybersecurity requirements are then allocated to hardware and software or to both. Once the technical Cybersecurity requirements have been allocated to hardware and/or software, the activities at the Product Development: Hardware Level (6.2.3.2) and Product Development: Software Level (6.2.3.3) can begin (see Figure 6).

Upon completion of the product development activities at the hardware and software level, hardware and software integration and testing is performed (Figure 6 and Figure 7). Vulnerability and Penetration testing may be performed on the integrated system, and verification/validation of the Cybersecurity technical requirements is performed. A final Cybersecurity assessment is performed resulting in the final Cybersecurity case. A final Cybersecurity review can then be completed prior to release for production.

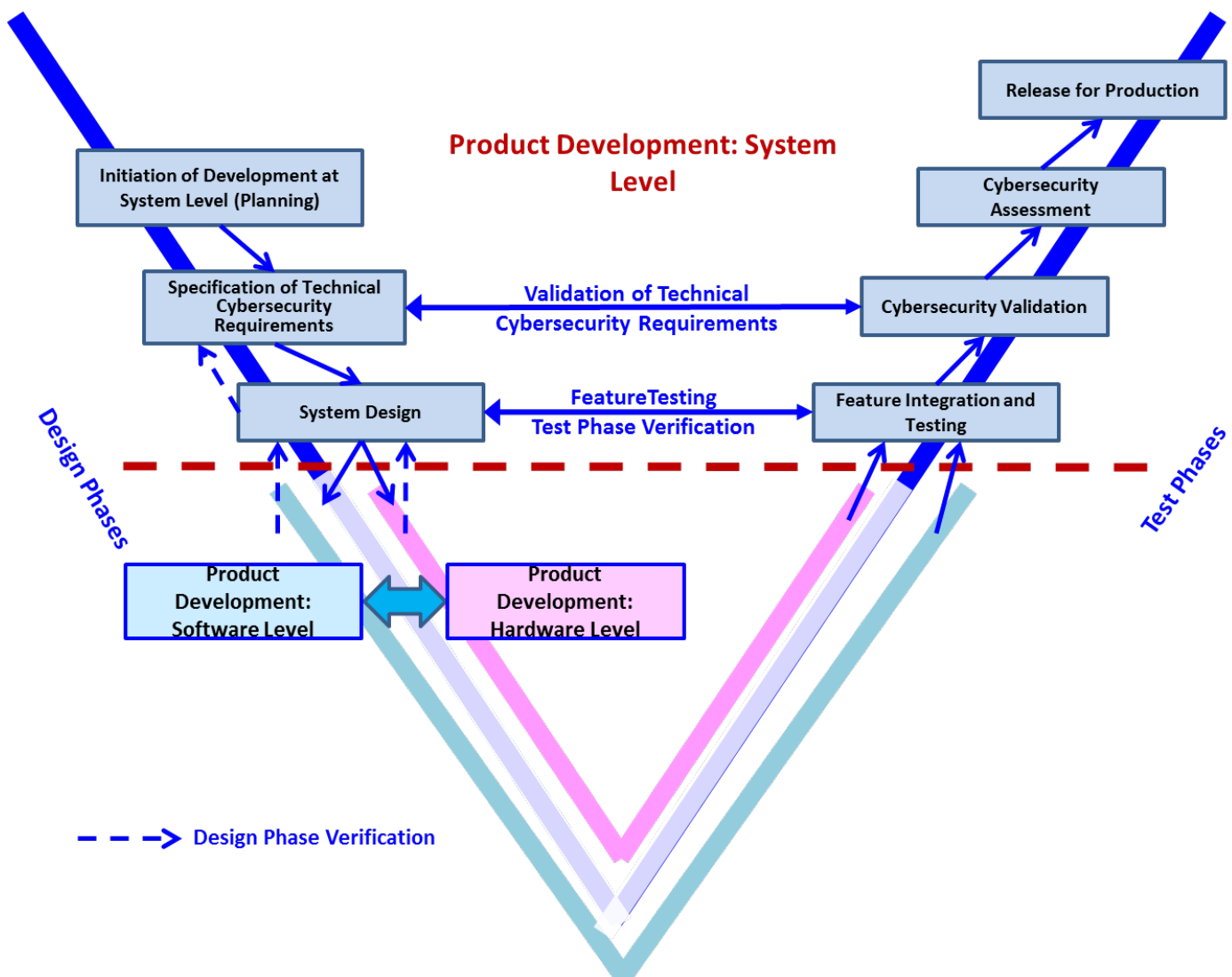


Figure 6 - V diagram for product development at the system level



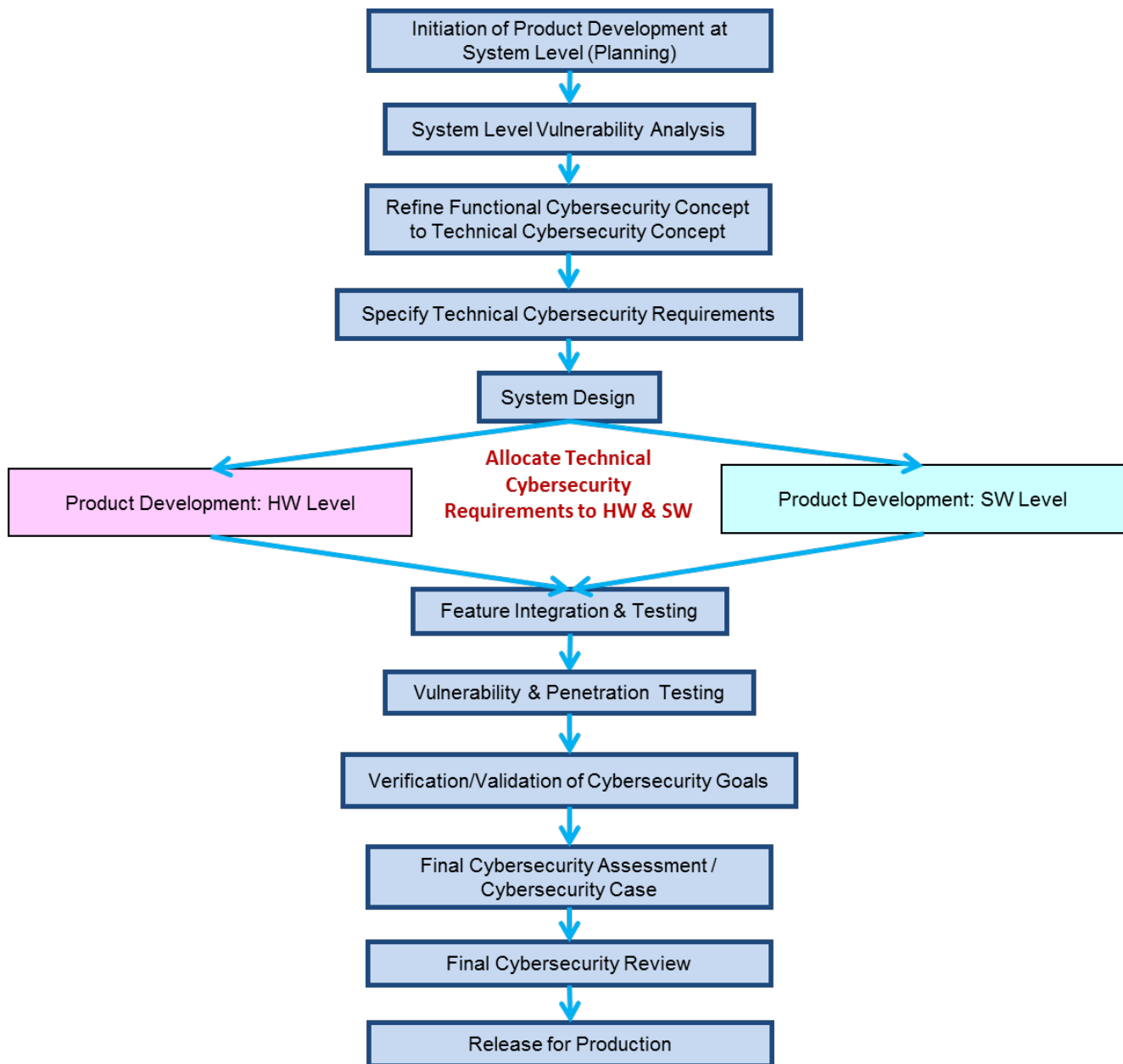


Figure 7 - Product development: system level

6.2.3.2 Product Development: Hardware Level

Figure 8 shows a V diagram for product development at the HW level in relation to product development at the system level. Figure 9 shows the flow of activities for product development at the hardware level. Hardware Cybersecurity requirements would be specified from the Cybersecurity requirements allocated to hardware during the system level development. If applicable, the Technical Cybersecurity Concept could be refined at this stage. Following hardware design, a vulnerability analysis would be performed to help identify potential vulnerabilities in the design and to help identify potential Cybersecurity Controls to address the potential vulnerabilities. Following hardware integration and testing, vulnerability and penetration testing may be applied to the hardware design. A Cybersecurity assessment is then performed and the preliminary Cybersecurity assessment is refined.

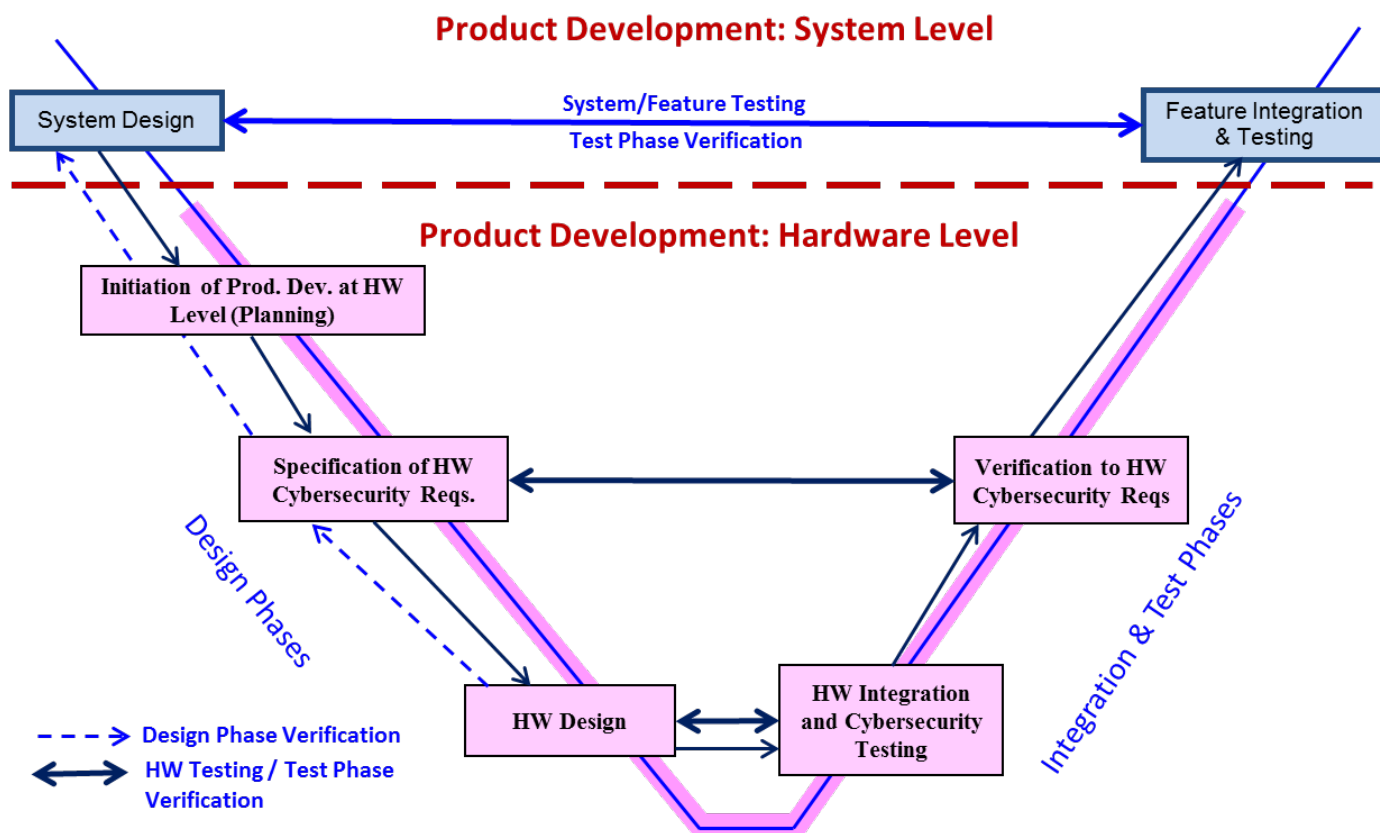


Figure 8 - V diagram showing product development at the HW level and its relationship to product development at the system level

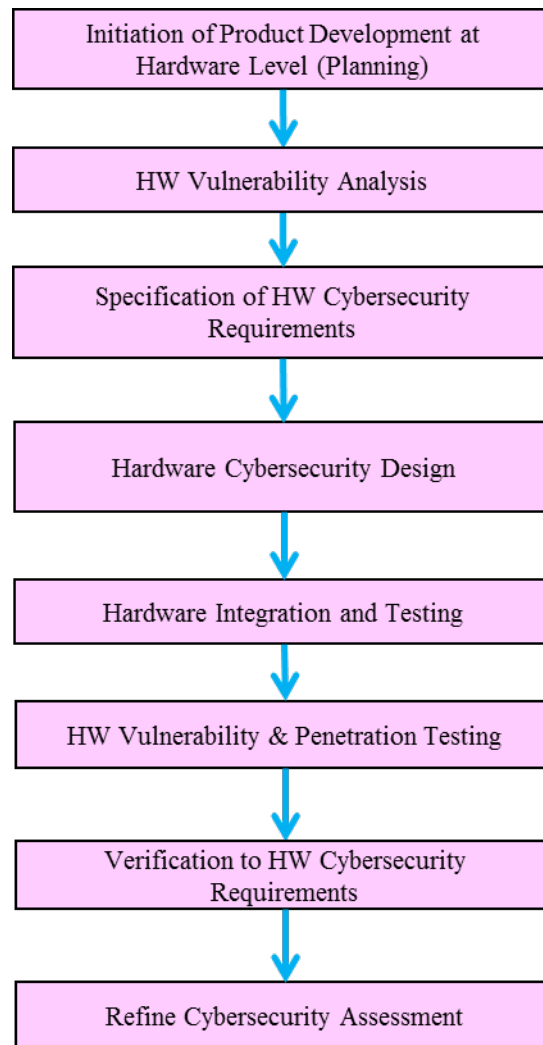


Figure 9 - Product development: hardware level

6.2.3.3 Product Development: Software Level

Figure 10 shows a V diagram for product development at the software level in relation to product development at the system level. Figure 11 shows the flow of activities for product development at the software level. Software Cybersecurity requirements would be specified from the Cybersecurity requirements allocated to software during the system level development. If applicable, the Technical Cybersecurity Concept could be refined at this stage. Following software architectural design, a vulnerability analysis may be performed to help identify potential vulnerabilities in the software architectural design and to help identify potential Cybersecurity Controls to address the potential vulnerabilities. Following software unit design and implementation, a software level vulnerability analysis may be performed, followed by software unit testing and software integration and testing. The software Cybersecurity requirements are verified after software integration, and vulnerability and penetration testing may be performed on the software. A Cybersecurity assessment is then performed and the previous Cybersecurity assessment is refined.

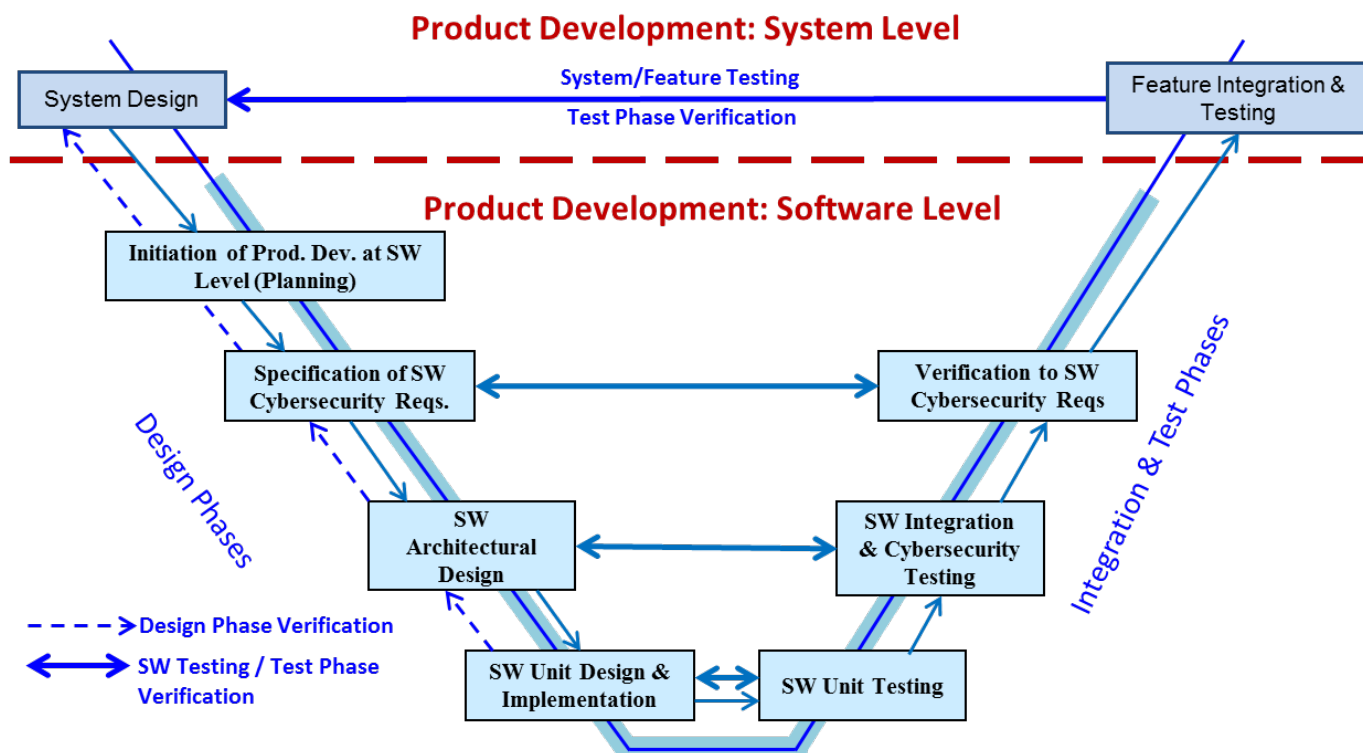


Figure 10 - V diagram for product development at the software level in relation to product development at the system level

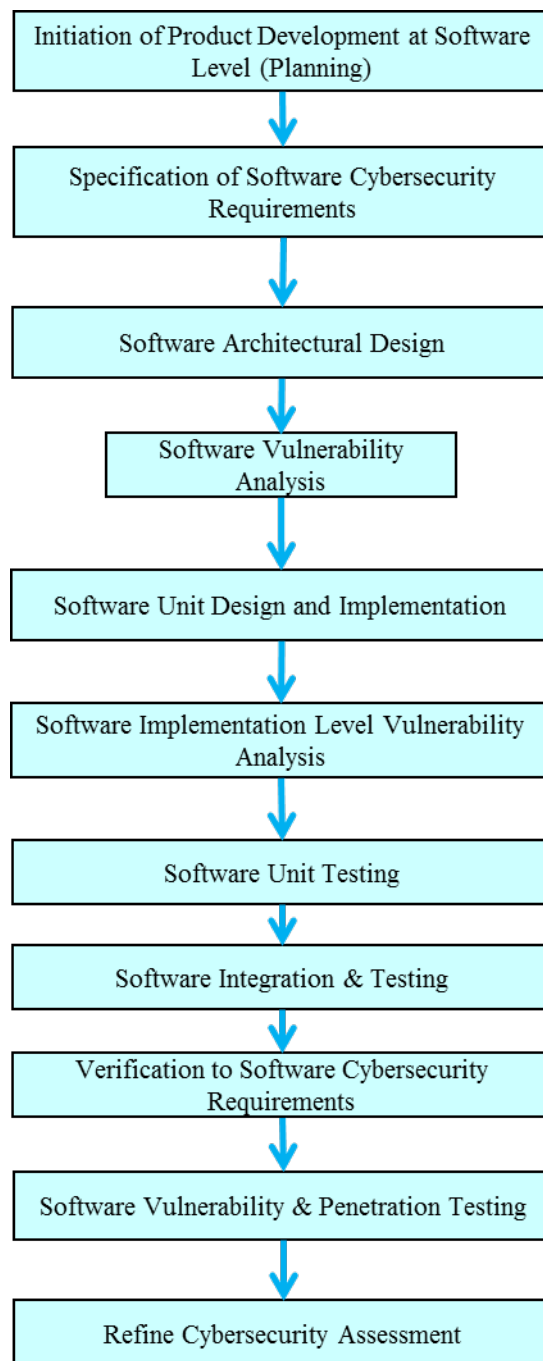


Figure 11 - Product development: software level

6.2.4 Production, Operation & Service

Activities in the production phase include production planning with respect to any Cybersecurity-related requirements that may impact the production process, including requirements relative to having specific portions of the manufacturing process secure. Cybersecurity-related production requirements may be included in the existing production plan. Cybersecurity requirements for the system may affect the specific process by which software will be flashed in the manufacturing facility onto ECU's, for example by requiring that the tools used for flashing be secure.

The operation phase includes both operation and service. Service includes normal maintenance activities and repair. Any requirements specific to Cybersecurity during operation, should be recorded within the appropriate documents (e.g., Vehicle Owner's Operating Manual). With respect to service, any maintenance and repair activities that have the potential to adversely affect Cybersecurity should have been identified in earlier lifecycle phases, and appropriate procedures should have been specified on how to maintain Cybersecurity during maintenance and repair; for example, maintenance procedures, and repair procedures. Service that could affect Cybersecurity includes re-flashing ECU's, connecting to the on-board diagnostics port, telematics system updates, vehicle/cloud computing interfaces, etc.

The operation phase also includes performing and maintaining the field monitoring process that was defined and established in the overall management of Cybersecurity activities, and fulfilling the incident response procedure that was also defined and established in the overall management of Cybersecurity activities.

6.2.5 Supporting Processes

Some of the supporting process activities should be identical to activities applied as part of a system safety engineering process tailored to be consistent with ISO 26262. It is recommended that these processes be integrated into a company's existing product development process. These include: configuration management, documentation management, change management, etc. Other supporting process activities used in ISO 26262 may be tailored to be specific to Cybersecurity. These include: management of Cybersecurity requirements, requirements for dealing with distributed development, etc. The distributed development requirements are designed to help ensure the following:

- That a supplier is capable of developing and producing Cybersecurity-critical features according to a customer organizations internal Cybersecurity process,
- That the appropriate communication channels are established and maintained between the supplier and customer,
- That the Cybersecurity work products are agreed to,
- That appropriate reviews are established at key milestones with customer access to work products,
- That any changes that could affect Cybersecurity are evaluated and agreed to,
- That the final Cybersecurity case is reviewed and agreed to,
- That any Cybersecurity issues that the supplier may become aware of are reported to the customer in a timely manner, etc.

6.3 Milestone and Gate Reviews

Figure 12 shows the gate reviews that may be performed at each major milestone. These include the Concept Phase Review at the completion of the concept phase activities, the Requirements Review that may occur in stages (for example, functional requirements review and technical requirements review, including review of requirements allocated to hardware and software at the system level), the Design Review, Implementation Review, and Verification and Validation Review.

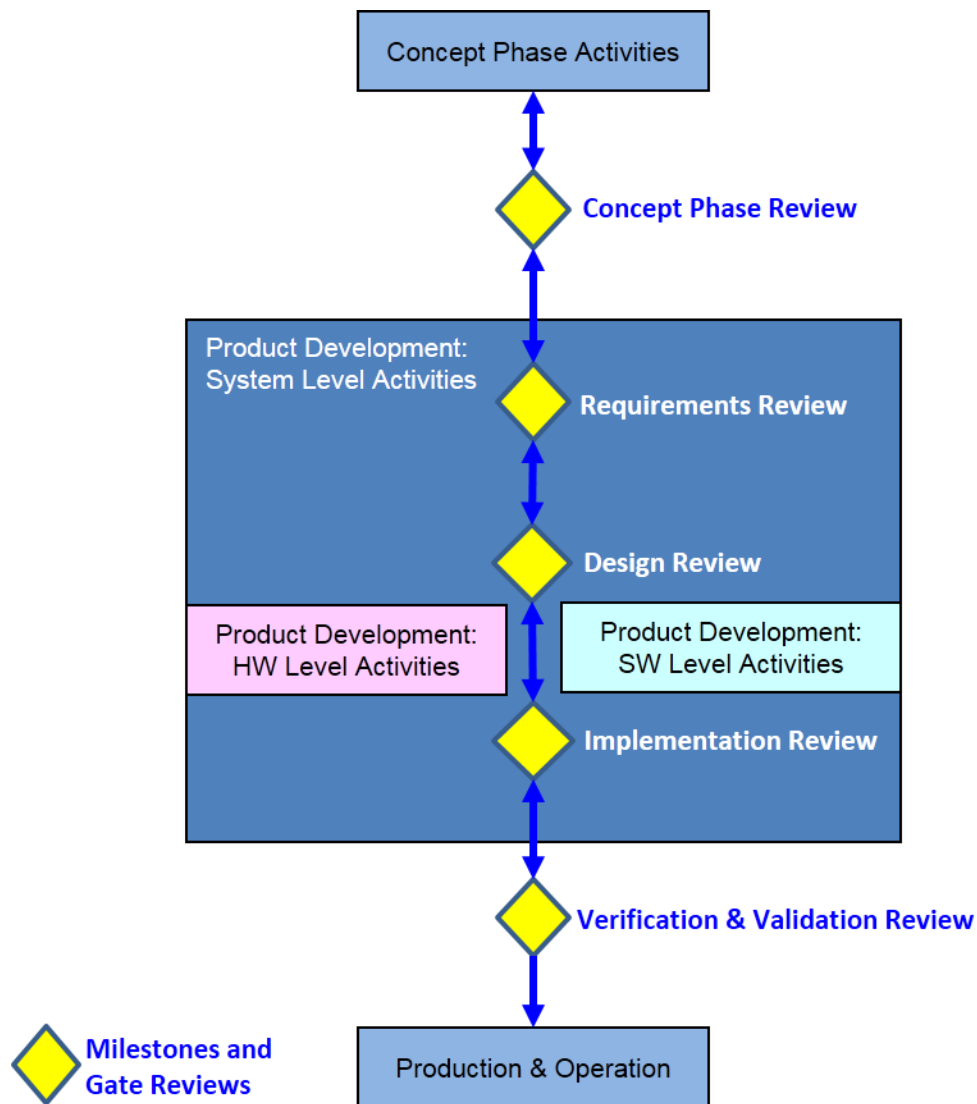


Figure 12 - Possible milestones and gate reviews

Figure 13 shows the tasks that may be reviewed at each of the major milestones. In the Concept Phase Gate Review, the review may include review of the Cybersecurity plan, the system definition, the threat analysis and risk assessment results (including the identified threats, threat classifications, and the Cybersecurity goals), the Functional Cybersecurity Concept, the refinement of the Cybersecurity goals into functional Cybersecurity requirements, and the Preliminary Cybersecurity Assessment. The Requirements Review may cross lifecycle phases and includes review of the functional Cybersecurity requirements, the technical Cybersecurity requirements refined or derived from the functional Cybersecurity requirements, and the technical Cybersecurity requirements allocated to hardware and software. It also includes reviews of analysis activities that were performed in identifying the requirements. The Design Review includes the analysis activities and results that affect the design, and the system design. The Implementation Review includes the analysis activities and results that affect the implementation, and the implementations at the hardware and software levels. The verification and validation review helps ensure that the system was designed and developed according to the requirements, and that the Cybersecurity Controls are appropriate and work as intended; note that in some cases, it may not be feasible or possible to verify and validate all of the Cybersecurity Controls. Common criteria methods may be considered to ensure comprehensive testing is conducted (7).

The gate reviews are intended to help ensure that appropriate activities have been performed and completed correctly and consistently before the next stage of development begins. These reviews may be conducted by a small (e.g., 3-4 person) team of technical experts that should ideally be independent of the feature development. To maintain consistency and completeness across the feature development, it is recommended that this same 3-4 person team participates in all of the reviews throughout the system development. The results of each review may be a pass, or a conditional pass (rework required). A gate review should be completed successfully prior to exiting the gate and moving on to the next phase.

There are two possible ways an organization may choose to complete the technical reviews. One is to use a technical “gate” review concept as described above, where the review is considered a gate to the next phase and is performed at the end of the development phase being completed, and the second approach is to perform a review of the activities completed during each development phase as each activity is completed. One advantage of the first approach (the gate review approach) is that the reviewers can follow the progression of definitions, descriptions, analyses, etc., for one review and this may make it easier to identify potential incomplete, inconsistent, or incorrect aspects across the activities when completing the reviews at the same time. A second potential advantage is that the technical experts are only required for a single meeting as opposed to multiple review meetings. Potential disadvantages of this approach are that issues may not be caught immediately and may propagate to the next activity, a greater amount of time is required during a given period to review multiple documents and the single meeting will require more time since more activities are being reviewed at one time. Providing the results of the activities well ahead of the review (e.g., at least two weeks ahead) may help to alleviate the first potential disadvantage by providing the reviewers with a period of time to review the results.

Potential advantages of the second approach, reviewing the results as each activity is completed, include that issues may be caught sooner and repaired before they propagate, less time is required to prepare for the review by reviewing a single documented result than would be required to review multiple results, and the review meetings for single documents will also be shorter. The primary disadvantage of this approach is that the continuity between results may be lost when the results are reviewed individually as opposed to collectively. As a result, in order to be thorough, the reviewers would be required to re-review previous results in order to check for completeness, consistency, and correctness across the results. This eliminates the advantage of less preparation time. It is up to an organization to determine the best approach to follow with respect to reviews. It may be beneficial as an organization is coming up to speed with Cybersecurity and a Cybersecurity process, to start out using the second approach and transition to the first approach as experience is gained in Cybersecurity.

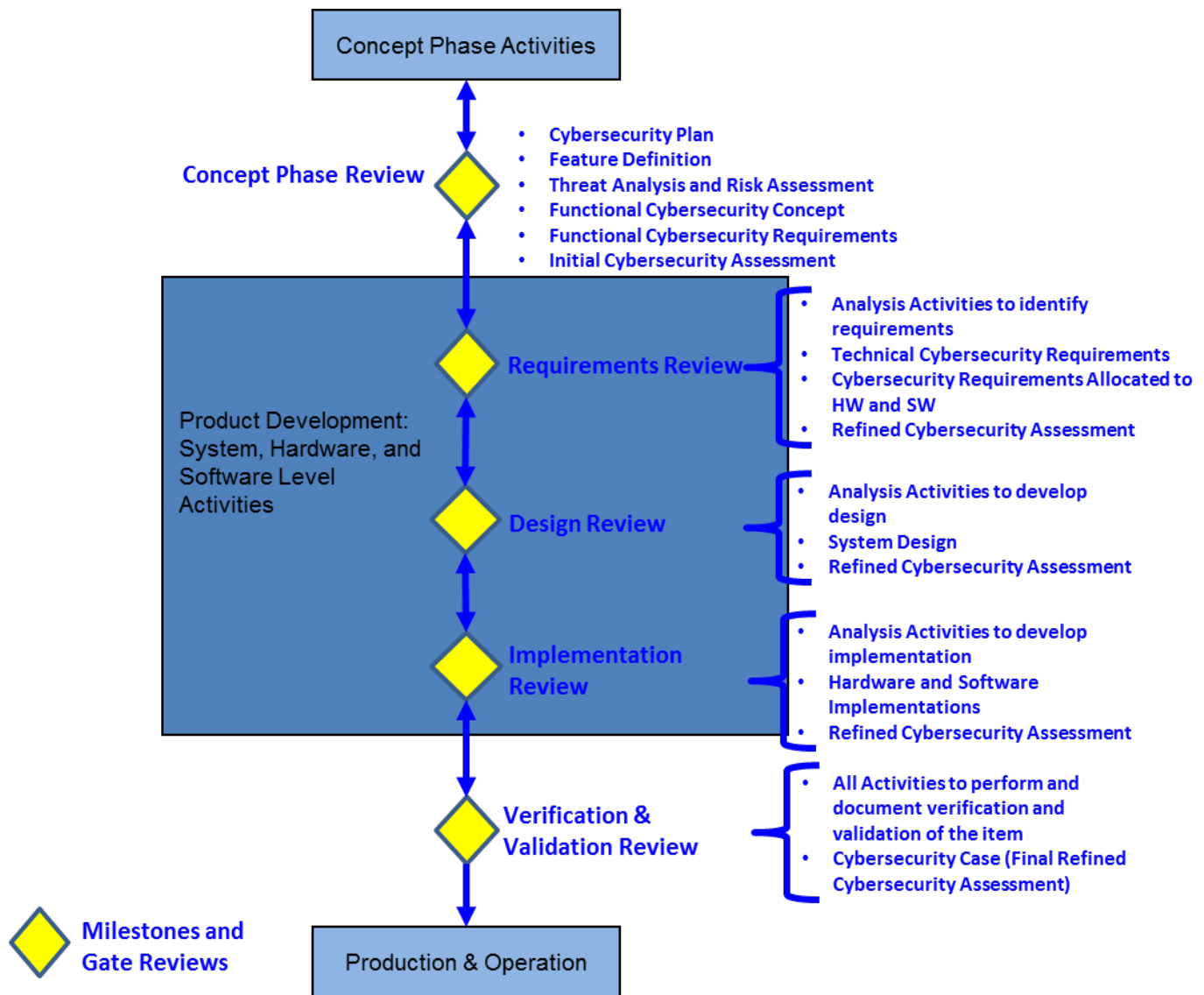


Figure 13 - Gate review activities

7. OVERALL MANAGEMENT OF CYBERSECURITY

As presented in Chapter 4, Cybersecurity Process Overview, part of the overall management of Cybersecurity includes:

- Creating, fostering, and sustaining a Cybersecurity culture that supports and encourages effective achievement of Cybersecurity within the organization,
- Establishing methods to help ensure compliance to an adopted Cybersecurity engineering process,
- Identifying and establishing needed communication channels with respect to Cybersecurity, both internally and externally,
- Development and implementation of training and mentoring to achieve a competence in Cybersecurity for cyber-physical vehicle systems,

- Incorporating a field monitoring process that includes monitoring hacker chatter (including online and at conferences where potential attacks/vulnerability conversations may occur), media articles, reporting unsuccessful attacks, etc.,
- Incorporating an incident response process that includes an attack incident reporting procedure, and attack incident investigation, resolution, and action procedures.

This chapter will describe these concepts in more detail.

7.1 Cybersecurity Culture

A Cybersecurity culture within an organization is an organizational culture that:

- Places high priority on Cybersecurity.
- Sets forth the organizational goal to stay ahead of potential threats.
- Makes addressing highest risk threats a priority.
- Works to create, foster, and sustain a Cybersecurity culture within the organization by:
 - Building a dedicated organizational structure to:
 - Develop and follow global Cybersecurity processes, practices, tools, and methods,
 - Train employees in the proper way to design and think about Cybersecurity,
 - Inform management on attack motivations and the potential detrimental effects to an organization if an attack is successful,
 - Develop a business case for Cybersecurity vulnerability resolution and product introduction (e.g., defined threats, rationale, benchmarking [if applicable], company impact, pros/cons, implementation implications [which groups/products are affected], and timing) and to
 - Champion Cybersecurity topics within the product development organization.

7.2 Measuring Conformance to a Cybersecurity Process

The Cybersecurity process should be followed throughout the product development lifecycle. With this process, threats that have been identified as having higher risk may require additional or more rigorous analysis. This process is described below.

The goal is a holistic process whereby an organization monitors “daily events” and warns and notifies those with a need-to-know, determines threats of greatest risk, analyzes data, plans upgrades, maintains systems, ensures compliance to standards and regulations, responds to Cybersecurity issues, and is always monitoring new technologies.

Based on level of risk, there will be more or less rigor for process implementation. Some activities may include:

- Ensuring conformance to a company’s internal Cybersecurity process and requirements.
- Holding technical reviews at each of the development milestones.
- Performing audits to ensure process is followed.
- Submitting performance and verification/validation plans.

7.3 Identifying and Establishing Communication Channels

The organization structure should be clearly identified so appropriate communication channels are used. The organization should know how to communicate:

- New media articles and events to those appropriate groups and organizations.
- Processes for an individual (both internal and external) to report incidents.
- Processes for companies to report incidents as appropriate to their suppliers and/or vehicle manufacturer.
- Processes (and dedicated groups) to address and respond to government, media, public, and internal inquiries.
- Internal organization structure within the company so employees know who to go to about any type of Cybersecurity question or issue.

7.4 Developing and Implementing Training and Mentoring

Empowering the employees in your organization to recognize common threats can be beneficial to the organizations Cybersecurity health. Cybersecurity awareness and training teaches employees to understand vulnerabilities and threats to business operations and products.

- Employees should realize that all products and processes have vulnerabilities.
- A regimented threat analysis and risk assessment should be performed to direct where resources should be spent. This regimented threat analysis and risk assessment should occur early in the development of new features/products because it is more expensive to fix any issues late in the product lifecycle.
- Mentoring should occur from an experienced Cybersecurity engineer.
- Share Cybersecurity best practices and organizational insights on what really works.
- Encourage an open exchange of ideas and questions in a non-threatening environment.
- Continually emphasize the critical nature of data and product Cybersecurity and that it's the employee's responsibility to be aware and build this in to their designs.
- Incorporate Cybersecurity awareness into existing processes and forums, as appropriate.
- Provide ongoing training on what the Cybersecurity process is and how it should be implemented.
- Provide ongoing technical Cybersecurity training sessions to improve individual engineering competency.
- Inform employees of Cybersecurity design and evaluation tools as well as make them aware of industry standards and best practices that are available.
- Fold in learning of vulnerabilities from previous products into new and future products.