International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

A CMMI-Based Framework for Integrating Safety and Security in IT and Engineering Product Development

Praveen K Harkawat

Head- BU Quality and Certifications & Assessments, L&T Technology Services, Vadodara (India)
Email: *pkharkawat[at]gmail.com, praveen.harkawat[at]ltts.com*

Abstract: ***Ensuring safety and security throughout the product lifecycle has become a pressing concern in engineering and IT industries. As automation expands and regulatory demands tighten, organizations are seeking integrative methods to embed safety and security within product design and development processes. This paper introduces a practical process/system framework based on CMMI's SAF and SEC domains, aimed at facilitating safer, more secure engineering outcomes. The proposed model incorporates best practices from global standards such as ISO 27001, ISO/IEC 26262, and GDPR, offering a hands-on approach adaptable to diverse technical fields including mechatronics, aerospace, and industrial control systems. It provides a scalable roadmap for companies already adhering to prior CMMI standards to integrate new safety (SAF) and security (SEC) requirements, reinforcing operational resilience and product integrity.***

Keywords: CMMI, Product Safety, IT Security, Process Framework, ISO Standards

1. Introduction

In the ever-changing and strict regulatory landscape, safety and security are becoming an integral element of the engineering product life cycle, from conception to field installation. A greater demand for more usable and practical processes/systems is being felt as designers across a range of industries, such as automotive, aerospace, consumer electronics, industrial equipment, software, and others, create new age solutions and services. Design for Safety & Security (DfSS) is getting more prominence and attention from product designers to ensure customer satisfaction/safety, regulatory compliance and standardization.

An essential component of any embedded system is safety. First and foremost, system or component safety failures can lead to financial losses for technology stakeholders as well as threats to users, the environment, and reputation.

In traditional safety-critical industries where safety considerations are accorded a higher premium, such automotive, aviation, and industrial control designs, safety analysis is more prominent. Using the reliability data of different components based on their configuration in the system, the safety analysis assesses the probability, causes, and seriousness of a prospective system element's failure or error at the design stage.

The rapid progress of automation has continued to offer humanity numerous benefits, including many security and safety-critical applications. However, unlocking the full potential of products / applications, especially in high-consequence domains, requires the assurance that products will not constitute risk hazards to the users or the environment. Many frameworks have been proposed to incorporate safety and security, among other features, in order to build products and systems that are safe, secure, and dependable. But most of the frameworks have limited inclusion of safety and security related processes and practices.

So, there was a need for a new holistic framework. In the year 2024, ISACA released CMMI 3.0 with multiple domains including Safety & Security. CMMI is one of the frameworks used by many companies across the globe. It has resulted into better processes and solutions. The companies across the globe have adopted this framework to manage complex project and product development. The same framework can we adopted by product development organizations to fast track their journey towards designing Safe and Secure solutions. The latest release of CMMI version 3.0 includes process area call "Enabling Safety" and "Enabling Security", which can help the organisations in design and development of sustainable & safe products and solutions. It can also be adopted by engineering companies developing and delivering solutions for industrial automation, automotive, aerospace, medical, telecom and other domains.

This paper aims to present a practical and integrative framework based on CMMI's SAF and SEC domains to guide IT and engineering organizations in embedding safety and security practices into their product and process development lifecycles.

The proposed suggestions can be used by the organizations to establish a holistic system meeting the requirements of CMMI SAF and SEC domains and other standards.

2. Literature Review

According to TUV, product security and safety continue to be important factors in an organization's business and purchasing decisions. Product safety, which is already a top concern for customers, is becoming a more significant factor in determining brand preference and purchasing patterns. Customers are willing to pay more for a higher level of product safety, according to the people who make business decisions.

There are several business advantages to meeting national, international, and industry-specific standards and

guaranteeing improved product safety and quality. These include increased brand differentiation, quicker and more extensive market access, and a lower chance of product recalls and reputational harm (TUV, 2024).

Public awareness of the security and safety of the items that people use and consume has increased as a result of several high-profile product safety incidents and recalls. Product safety is not a brand-new subject, but it is topical and important to discuss how the product design processes/framework contributes to or exacerbates safety risks and vulnerabilities (TUV, 2024).

Beyond enterprise and application security, creating a comprehensive strategy for engineering product safety and security is now essential for business, not a hindrance. Engineering companies and Businesses who succeed in this regard will gain a definite competitive edge. Technology and Engineering companies have been implementing multiple frameworks/system as per ISO27001, ISO/IEC 26262, GDPR requirements to meet organizational as well as product/service safety and security needs. It has helped tech companies while launching new engineering products and services. However, there were limitations to businesses to overcome a number of obstacles brought on by legal restrictions, shifting consumer preferences, and shifting purchasing patterns. Companies are also facing challenges from rising expenses associated with failing product security, damage to their brand in the event that a product compromise occurs, and growing dangers from hackers. Also, product security is not only about "letting's get this thing out of the door and making sure it gets a security certification." It goes much beyond that. Similar to manufacturing, security requires everyone to put "safety first." Security is not a bonus feature (Raspotnig et al., 2018).

During engineering product design and development all applicable safety and security related features must be included in both the creation phase and the operational phase. The design and development team as a whole should consider how safe the product is and how well-prepared it is to defend against a security breach for every kind of customer, be it manufacturing, industrial, aerospace, or medical (Mashkoor et al., 2023).

There is a new trend of digital transformation along with all the new difficulties and advances in technology. Since it has spread to every industry, software is currently used by every company. Businesses must safeguard the bottom line by fostering faith in their products and services without compromising the speed and agility that will keep them competitive in the market, regardless of whether they are developing embedded software to run their own operations or selling it directly to consumers. (Mashkoor et al., 2023).

When it comes to incorporating safety and security into their engineering product development life cycle (EPDLC), many firms continue to lag behind. Too many development teams still view security as a bottleneck that keeps them from releasing great new features and requires them to rethink code they thought was finished. Products that are hazardous and insecure increase the risk to their firm. Customers will not be protected by cool new features if the product is vulnerable to hacker exploitation. By establishing, putting into practice, and adhering to the procedures that facilitate rather than impede the release of superior, highly secure products onto the market, the product team must integrate safety and security.

The first multi-domain maturity framework was created in 1986 by Carnegie Mellon University's Software Engineering Institute (SEI). The first maturity model to direct software development was the Capability and Maturity Model (CMM). CMM The Capability Maturity Model Integration (CMMI) was first published in 1993. The CMM was created especially to offer a structured, disciplined framework for addressing issues related to software management and engineering processes. Later, CMM evolved into the Capability Maturity Model Integration (CMMI), which offers a means of evaluating and showcasing an organization's practices and operations in relation to recognized standards.

CMMI Performance Solutions is a proven, outcome-based performance improvement model providing faster, better, and cheaper results. CMMI is the globally accepted standard that improves and enhances organizational capability and performance. CMMI provides a prioritized pathway to build and implement new capabilities that deliver consistently measurable results and outcomes. For 25+ years, high-performing organizations have achieved clear, sustainable business results with ISACA®'s Capability Maturity Model Integration (CMMI®) model. Originally created for the U.S. Department of Defense to assess the quality and capability of their software contractors, the CMMI model has expanded beyond software engineering to help organizations around the world, in any industry, understand their current level of capability and performance and offer a guide to optimize business results. The model is used by companies in 106 countries. CMMI Performance Solutions helps organizations quickly understand their current level of capability and performance in the context of their own business objectives and compared to similar organizations. CMMI's performance improvement model has helped thousands of globally recognized companies—including many Fortune 500 organizations (Product Team, 2010).

Within the field of new product management, product safety and security are a developing area that has drawn more scholarly interest in the past few years. There is increasing interest in the assurance of the design of safe & secure products.

By aligning CMMI's SAF and SEC domains with existing international standards, this framework offers a comprehensive and adaptable solution for engineering firms aiming to enhance product safety, reduce risks, and meet global compliance demands.

3. Objectives of the Study

As there is increasing demand for safe and secure products/services/solutions, organizations are required to establish a robust system in order to ensure that customer expectations are met in light of evolving requirements. There are IT and ERD companies where CMMI is being used/implemented. Now ISACA has released a new CMMI

with additional domains Safety and Security, which will help companies to design and implement safety/security related solutions in better and optimal ways. The researcher intends to propose a new framework through this study / paper.

4. Research gap and necessity of new framework

Many businesses implement new initiatives/ frameworks to increase productivity, customer satisfaction, processes, quality, and to ensure product's compliance with regulatory requirements. To develop safe products, services, and processes, there is a need for a new innovation and framework which includes practices/procedures related to safety, security, sustainability and compliance.

This paper aims to propose a new framework for safe and secure product/process/ service development and operations. The paper suggests a framework that can be used to design & develop reliable products, processes & services and operations. This framework will help in planning, monitoring & tracking of development of sustainable & safe product/service/process development and operations.

5. Methodology

The author looked at the existing capability /maturity models and observed that CMMI for Software is most widely used in the industry. There are few measurement frameworks built using CMMI as a based model. These are, People Capability Maturity Model (PCMM), Testing Maturity Model (TMM), Project Management Maturity Model (ProMMM) etc., which are used by many IT and other organizations. These models have multiple levels of maturity / capability and provide ratings (Maturity / Capability Level 2, 3…) as per the status of implementation of related practices in the organization.

For building the new framework, the researcher relied upon the secondary data available from research papers from different industries. The researcher also studied the existing product management processes & frameworks and their usage by IT and Engineering organizations. The researcher decided to use the proven and widely implemented CMMI-based practices and sub-practices to define a new framework for managing sustainable & safe product/process/services development & operations (Hou, L., Liu, Q., Saeed, K., Ali Haidery, S., Uddin, M. I., & Khattak, H.,2021); (Product Team, 2010). The new framework will have processes, practices, and sub-practices which must be followed while executing a sustainable product design & development project/program and operations.

6. New Framework: CMMI' Safety (SAF) and Security (SEC) Domain-based Process/ System

The new framework will focus on the new requirements of CMMI 3.0. We will identify the changes to be incorporated in the existing systems for the companies which are already CMMI 2.0 assessed. Let's discuss, what are the modifications required in the existing quality management system (QMS) to meet the CMMI SAF and SEC related requirements.

What changes are required to meet the requirements of CMMI SAF, SEC?

For CMMI 2.0 appraised companies following changes (indicative list) may be required to meet the requirements of SAF, SEC domains:

Level of Impact /Changes=> Practice Area Name	SAFETY (SAF) Domain Impact /Changes on the CMMI2.0 QMS	SECURITY (SEC) Domain Impact / Changes on the CMMI2.0 QMS
Causal Analysis and Resolution	No	No
Configuration Management	Less	Less
Decision Analysis and Resolution	Very Less	Very Less
Estimating	Less	Less
Governance	Medium	Medium
Implementation Infrastructure	Very High	High
Managing Performance and Management	High	High
Monitor and control	Medium	Medium
Organizational Training	Medium	Medium
Peer Reviews	Medium	High
Planning	High	High
Process Asset Development	Medium	Medium
Process Management	No	No
Process Quality Assurance	Medium	Medium
Product Integration	Less	High
Requirements Development & Management	Very High	Very High
Risk and Opportunity Management	High	High
Technical Solution	High	Very High
Verification and Validation	High	High

CMMI SAF, SEC Implementation Approach: The following flow diagram shows a practical way for implementation of SAF, SEC related practices.

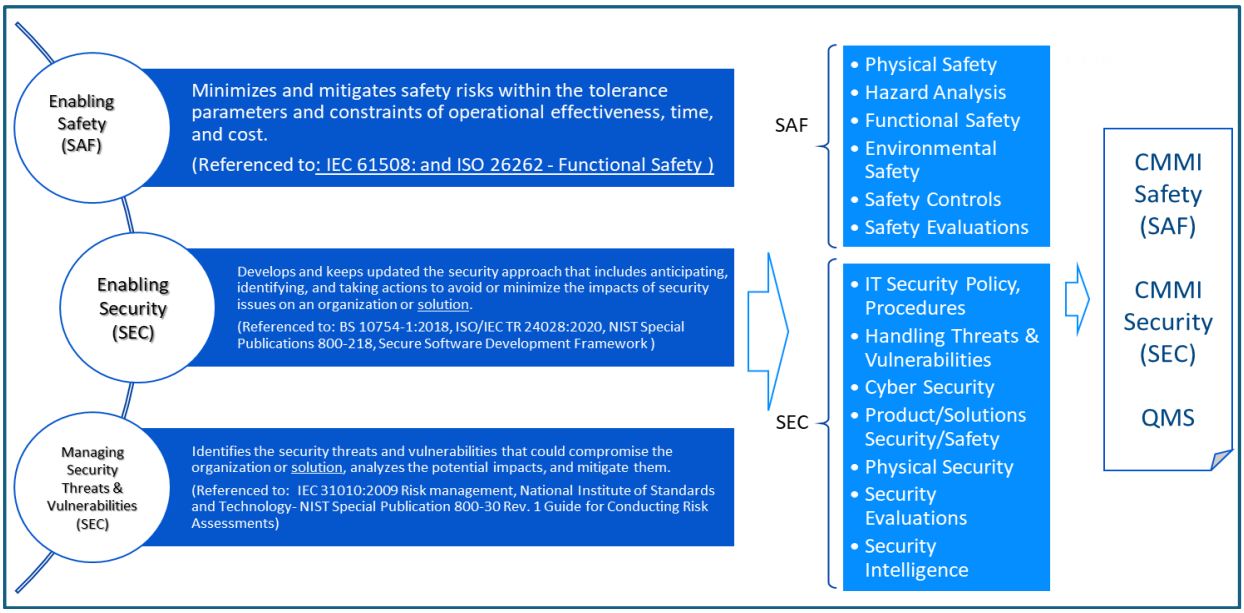

Figure 2: Mapping of CMMI SAF, SEC PA, Objectives, Activities and Outcomes (Documents)
(Source: CMMI Model book and Self Research)

- New version/domain is linked / referenced to multiple international standards (IEC 61508: and ISO 26262 - Functional Safety, BS 10754-1:2018, ISO/IEC TR 24028:2020, NIST Special Publications 800-218, Secure Software Development Framework, IEC 31010:2009 Risk management, National Institute of Standards and Technology- NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments)
- Include Product Safety/Security related practices
- Provides/Guides for usage of Security & Safety Intelligence (e.g. prediction models for product/network/data center failure)

Also, there are companies which are already certified ISO27001 & ISO 45001. Is there any way that existing standards can be leveraged to comply with the new CMMI 3.0?

For the organization certified with ISO 27001, ISO 45001 and GDPR compliance, there is scope for reusing the existing processes / systems, which will help to meet some of the requirements of CMMI.

Below table shows the mapping of CMMI SAF-SEC domain with other relevant standard documents / systems:

Standards >> CMMI 3.0 / Domain	ISO 27001 Certification	ISO 45001 Certification	GDPR	ISO/IEC 26262
Security (SEC)	Cyber Security IT Controls	Physical Security	Data Transmission Security Compliance	Product / Functional Security
Safety (SAF)	Technological Safety Controls	Physical Safety Access Control Work Environment		Functional Safety

(Source: Self-research and learning)

CMMI SAF-SEC domain brings a holistic approach to Organizational safety and security. ISO 27001: for ISMS, ensures that security controls are there is place to protect organizations sensitive information and IP. On the other hand, ISO 45001 focuses on protecting the physical safety and security of people and physical assets. Its being illustrated in the below table:

	ISO 27001 Certification		ISO 45001 Certification		GDPR		ISO/IEC 26262	
	Pro	Cons	Pros	Cons	Pros	Cons	Pros	Cons
Pros / Cons	IT Infra and Security Focused Well Known Standard	Does not cover product / solution's security	Health & Safety Focused Widely Accepted	Very Limited applicability in their industry. More oriented towards manufacturing	Accepted across the globe	Limited to data protection and transmission	Wide Acceptance in all domains	

(Source: Self-research and learning)

Having researched SAF, SEC requirements, let's elaborate on the phase-wise changes / additions required for new model / framework:

Some typical examples of changes / additions are:

Product/ Software Development Phase	New Changes/ Modifications to be incorporated
Requirement Design & Phase	Guidelines for Embedded SW, HW and Cloud including • Security Requirements Management • Security Variability Design and Analysis • Optimized Security Architectural Design • Standard Authentication Process • Guidelines for Stringent hardening of system software • Vulnerability Modeling • Creation of multiple layers • Intrusion Detection and Prevention system • Encryption and Decryption • Secure by Design, Secure by Default, • Guidelines for Security and Privacy Assessment Guidelines for Treat Modelling (identify security requirement, pinpoint security threats and potential vulnerabilities, quantify threat and vulnerable critically, and prioritize remediation methods)
	Guidelines for • Open- Source Software (OSS) assessment • SEI CERT coding for JAVA, C++ • The Open WebApp Security Practices (OWASP) • Coding guidelines for Cybersecurity vulnerabilities (CSV) safety and common Weakness Enumeration (CWE) list
Testing/ Verification & Validation Phase	Guidelines for Evaluation Assurance Levels (EALs) to ensure that application is • Functionally tested • Structurally Tested • Methodically Tested and Checked • Penetration Tested • Static Application Security Tested (SAST) • Dynamic Application Security Testing (DAST) • Security Tested

(Source: Self-research and learning)

The above proposed framework along with other supporting standards, establishes a set of requirements and direction for product safety, quality and reliability, with the goal of reducing security risk exposure for software platforms and products and services. This framework can be used by all software products and services developed by IT / Engineering companies, partners, and developers.

7. Results and Discussions

This paper introduces a comprehensive process/system framework rooted in CMMI's SAF and SEC domains, offering a pragmatic pathway for IT and engineering firms to design and manage safe, secure, and compliant products. By aligning with globally recognized standards, the framework holds the potential to bridge compliance and innovation. Although conceptual in nature, its applicability across multiple domains provides a strong foundation for future empirical validation and industry-specific customization.

This framework can be used by all software products and services developed by IT / Engineering companies which are CMMI 2.0, ISO 45001, ISO27001 and GPPR compliance.

8. Limitations and Suggestions for Future Work

The proposed framework has to be validated by a set of product and service companies for better understanding and customization as per organization and industry standards / requirements.

In future more practices related to product safety and security can be added for various industries / domains like aerospace, transportation, industrial product etc.

References

[1] Product Team, C. (2010). *CMMI ® for Development, Version 1.3 Improving processes for developing better products and services*. http://www.sei.cmu.edu

[2] Hou, L., Liu, Q., Saeed, K., Ali Haidery, S., Uddin, M. I., & Khattak, H. (2021). Enhancement of the Capability Maturity Model for Improving the Quality of Software Projects in Developing Countries. *Scientific Programming*, *2021*, 1–10. https://doi.org/10.1155/2021/9982227

[3] Keshta, I. (2022). A model for defining project lifecycle phases: Implementation of CMMI level 2 specific practice. *Journal of King Saud University - Computer and Information Sciences*, *34*(2), 398–407. https://doi.org/10.1016/j.jksuci.2019.10.013

[4] Liberato, M., Varajão, J., & Martins, P. (2015). *CMMI Implementation and Results: Case Study of a Software Company* (pp. 48–63). https://doi.org/10.4018/978-1-4666-7473-8.ch003

[5] Lin, J. J. Y., & Lin, Y.-S. (2008). *Research and Development of a CMMI-Compliant Requirement Management System for Software Engineering* (pp. 76–86). https://doi.org/10.1007/978-3-540-92719-8_8

[6] TUV, https://www.tuev-nord.de/en/company/certification/product-certification/functional-safety/

[7] Harkawat, P. K. (2022). KPI-based Performance Measurement Framework/Approach for Lean Implementation in Mining Industry. In International Journal of Innovative Science and Research Technology (Volume7, Issue12 - December). https://doi.org/10.5281/zenodo.7467453
[8] Harkawat, P. K. (2022). Goal Question Metrics (GQM) Based Measurement Framework / Approach for Lean Implementation In Mining. IJRAR22D2404 International Journal of Research and Analytical Reviews (IJRAR), www.ijrar.org
[9] Harkawat, P. K. (2023). A Combined Lean & PCMM-based Process Improvement Framework for Better Human Capital / Resource Management in Mining Industry. International Journal of Innovative Research in Computer Science & Technology, 11(1), 1–4. https://doi.org/10.55524/ijircst.2023.11.1.1
[10] CMMI 3.0 (2024), https://cmmiinstitute.com/getattachment/47a7c84e-472c-4f7f-a473-ddc21c6ae045/attachment.aspx
[11] CMM3.0 Changes (2024), https://processgroup.com/changes-in-cmmi-v3/