HSI2024
Human Systems Integration
Conference
Jeju, Korea
August 27-29, 2024

Usability Challenges of Failure Mode and Effects Analysis (FMEA) within the V-Model

Dan Perreault
Colorado State University
6029 Campus Delivery
Fort Collins CO 80523
Dan.Perreault@colostate.edu

Erika E. Gallegos
Colorado State University
6029 Campus Delivery
Fort Collins CO 80523
Erika3@colostate.edu

Vincent Paglioni
Colorado State University
6029 Campus Delivery
Fort Collins CO 80523
Vincent.Paglioni@colostate.edu

Thomas H. Bradley
Colorado State University
6029 Campus Delivery
Fort Collins CO 80523
Thomas.Bradley@colostate.edu

Abstract. For over 70 years, failure mode and effects analysis (FMEA) has been used in development and assessment across products, processes, and services worldwide. In particular has been its application for useability and use error analysis. FMEA is considered a mainstay of predictive failure analysis and reliability, prescribed by multiple international standards. However, despite this level of adoption, FMEA encounters consistent and regular criticisms, particularly related to its ease of use and effectiveness. Research on improvement often focus on specific elements rather than on overall usability of the tool for practitioners. At the same time, the V-model has become a common approach for product design in systems engineering. However, the integration of these two popular processes together can be cumbersome and incompatible under their current uses. In this paper, we review current methodology for FMEA against similar V-model standards. We identify systemic challenges in using FMEA within the systems engineering V-model and suggest approaches for addressing these challenges to better serve FMEA users.

Introduction

Failure mode effects and criticality analysis (FMECA) or FMEA with criticality implied, hereafter referred to as FMEA, is a common risk and reliability analysis technique for identifying potential failures and their associated consequences. In many regulated areas, such as medical devices, the importance of user interfaces has led to FMEA application in human factors analysis to prevent use errors. Standards such as IEC 62366 (AAMI, 2021), which specifically outlines the need to analyze medical devices to address use errors in design, have been harmonized across many geographies, including the US, as an expected standard to comply to. The US Food and Drug Administration specifically reference FMEA as tool in their guidance on applying human factors and usability engineering to medical devices (US FDA, 2016) to drive improvements in device safety throughout the end to end design lifecycle The inherent complexity of systems within the scope of systems engineering presents, in theory, an ideal application for FMEA, where a structured approach to proactively identify potential failures can be significantly advantageous. Meanwhile, systems engineering relies heavily on the V-model for system development. The V-model, with its emphasis on validation and verification, is also well suited for complex and high-risk systems. As such, these tools together could be used to develop robust systems. However, in practice, systematic challenges in applying FMEA within the V-model limit its value-add. The purpose of this paper is to discuss the challenges

associated with using FMEA within the V-model in the context of standards and principles of design. There is a well-documented history of complaints in applying FMEA within the V-model framework, yet it is still commonly used. We present a review of this literature, highlight these systematic problems, and propose a systematic solution for improving this tool.

This paper is designed to thoroughly review both FMEA and the V-model processes, and their applications within systems engineering. Section 2 provides the background and process of FMEA as a risk analysis tool, and Section 3 discusses the use of the V-model in the systems engineering development process. Section 4 then examines how FMEA and the V-model could be synthesized, and the challenges presented by unifying these critical analysis processes. Lastly, Section 5 concludes with a summary of the findings and avenues for pursuing future research in this area.

Failure Mode and Effects Analysis (FMEA)

Background. In 1949, the US Military published MIL-P-1629, later replaced by MIL-STD-1629A, wherein the first description of failure mode effects and criticality analysis was presented (DOD, 1949; DOD, 1980). This new methodology focused on predicting potential failures, rating these potential failures, and establishing a prioritized list of critical potential failures to be mitigated prior to release of a design. This predictive approach, considering the possibility and nature of failures before a design is completed, was a substantial shift from the previous focus on testing as a means of addressing failures after design completion. Since its introduction, the FMEA methodology has been propagated across industries, as evidenced by the multiple international standards that have been updated as recently as 2019 (Automotive Industry Action Group, 2019). The core FMEA process has maintained the same purpose since its introduction, but has expanded to address design, processes, usability, and service (Geum, Cho, & Park, 2011). For example, in the medical usability space, application of FMEA to address prediction and avoidance of use errors is an active topic for regulators and researchers (US FDA, 2016). Additionally, FMEA research extends into process areas of healthcare (Chiozza & Ponzetti, 2009) and product areas of healthcare (Ravizza et al., 2019). Further, recent research has shown the effectiveness that FMEA can have in areas such as reducing medical errors (Setiasih & Purnawan, 2017), encouraging the criticality of FMEA as a tool in the usability engineer's toolkit.

As an analytical tool, FMEA has maintained remarkable consistency with the initial intent described in its origins. The proliferation of FMEA through different applications and the publication of associated industry standards have presented issues with FMEA implementation, such as connectivity between different forms of FMEA. Consequently, significant research has been conducted focusing on refinements to different elements within FMEA execution; however, the purpose has remained the same. One of the reasons behind this lack of change is the history of standards both from government and industry, which ensured the core process remained consistent over the course of that period.

Process. The process steps in conducting an FMEA can be broken down into three major steps: 1) Plan the FMEA, which includes defining the objectives, scope, system boundaries, decision criteria, and documentation; 2) Perform the analysis, which includes sub-dividing the system into elements, identifying functions, failure modes, failure causes, scoring of failures, and actions; and 3) Documenting the FMEA, which includes synthesizing the results and generating a living document (International Electrotechnical Commission, 2018).

Typically, the output of the FMEA process is documented in a tabular form, though there are many variants and alternatives posited in research literature. For the purposes of illustration, we present an example FMEA table split into three sections of columns (Tables 1, 2, and 3), where in a full FMEA, these columns would be bound together. Each of the columns across these tables represent items under step "2) Perform the analysis" as mentioned above.

These first eight items are broken down in Table 1, representing the decomposition of the system and identification of functions and failures. The first row of cells provides the column headers, and the second row provides the typical information that would be populated to support the headers in the first row.

Table 1: First Set of Columns in a Sample FMEA Table

ID	Element	Functions & Performance	Failure Mode	Local Effect of Failure	Final Effect of Failure	Cause of Failure	Existing Controls
#	Component of the system	What the element does	How the element fails to meet its function	What happens at the element level	What happens at the system/ user level	What creates the failure mode	Mitigations that already exist

It is important to note that these columns represent the initial state before new design mitigations are applied. While there often are iterations to this portion of the FMEA, at some point it is expected to be completed such that the remainder of the process can be executed. A more detailed description of these columns is as follows:

ID: A unique number for the line. Generally, only unique within a given table to differentiate lines.

Element: A discrete portion of the system identified for analysis.

Functions & Performance: This typically describes the expected behavior of the element, often with acceptance criteria for this behavior.

Failure Mode: This represents a way that the element can violate the "Functions & Performance." It does not represent what might have failed in the system, rather the unacceptable behavior that might occur.

Local Effect of Failure: This represents the element level effect of the "Failure Mode" identified in the previous column. For example, if a circuit board signal is expected to trigger a software monitoring function, and the circuit board fails to send the signal, the local effect would be that the software monitoring function would not be triggered.

Final Effect of Failure: This represents the system-level (and/or user-level) effect of the item "Failure Mode," i.e., how the failure propagates through the system. The intent is to assess the chain of events to a system or user. Continuing the example from the local effect if the software monitoring function is not triggered, a warning to the user is not presented regarding the error state of system.

Cause of Failure: This represents what part of the element failed to create the "Failure Mode," in effect tracking the failure mechanisms for the element and associated "Failure Mode." Rather, it represents the physical (or digital) problem in the element, for example, continuing the circuit board example, damage to a component on the board.

Existing Controls: This represents a proven control that already exists in the new design. Most commonly this comes from well proven elements from a predicate product or from a well-established off-the-shelf design that already has proven controls for a possible failure mode.

The next three typical elements, which comprise the initial state scoring table are presented in Table 2. These are used to calculate the Risk Priority Number (RPN) which used for sorting the failure modes. This is typically constructed by multiplying the numeric scores for each of the categories.

Example values are included in Table 2 to demonstrate typical data, where severity, occurrence, and detection can range from 1 to 10, meaning RPN can range from 1 to 1000.

Table 2: Second Set of Columns in a Sample FMEA Table

Severity Score	Occurrence Score	Detection Score	RPN (SxOxD)
10	5	10	500

For both occurrence and detection, the scoring is related to the "Failure Mode" column rather than "Cause of Failure" column, to accommodate circumstances where there can be a many-to-one relationship between the two. These columns can be explained in more detail as follows:

Severity Score: This is related to the "Final Effect of Failure" column from Table 1 and designed to measure the impact of the effect on the system, should the failure mode occur.

Occurrence Score: This is related to the "Failure Mode" and the likelihood of the failure mode occurring.

Detection Score: This is also related to the "Failure Mode" and the ability to detect it in time to mitigate the "Final Effect of Failure." It is of note that the detection score is typically inverted in comparison to the other factors. For example, on a 10-point scale, a score of 10 would indicate the least level of detectability and a score of 1 would indicate the highest level of detectability.

RPN: This is used to prioritize the risks, where a higher value indicates higher priority of mitigation. Since the resulting RPN value is based on a combination of the factors, scales are typically the same for all factors to avoid a structural weighting of the factor, vs. the score.

Lastly, Table 3 presents the final set of columns in the FMEA, relating to mitigation in response to risks identified.

Table 3: Third (and Final) Set of Columns in a Sample FMEA Table

Future State Mitigation	Post Mitigation Severity Score	Post Mitigation Occurrence Score	Post Mitigation Detection Score	Post Mitigated RPN	Evidence of Effectiveness	Additional Coding
Mitigation in design	10	1	1	10	Verification test report	Critical to safety

To complete an FMEA, the expectation is that for the appropriately selected RPN score lines, the design is modified to introduce a mitigation. The columns presented in Table 3 can be further described as:

Future State Mitigation: These are design changes made to address the "Failure Mode" identified in Table 1. Typical examples are forms of design redundancy or higher grade of components to reduce the "Occurrence Score." It is typically not the case that design mitigations can reduce "Severity Scores" because this is scored based on the assumption that the failure mode occurs.

Scoring Columns: These represent the score for the line based on the mitigation in the first column. Essentially, this represents the expected effect of the design change on the "Failure Mode," presumed to be an improvement. Typically, improvements are identified that reduce the opportunities for

failure, i.e., reducing the chances that the "Cause of Failure" from Table 1 occurs which then reduces the "Occurrence Score" for the "Failure Mode."

Evidence of Effectiveness: Particularly in regulated industries, FMEA can be an essential aspect of design controls and therefore some form of formal verification of effectiveness of the mitigation is performed.

Additional Coding: Similarly, there can be additional coding aspects where designators such as "critical to safety" can be placed on the mitigation leading to additional activities to ensure that the mitigation is present in product.

At this point, the FMEA process is considered complete for a given (set of) design(s). There is common discussion in all standards dating back to the origins of FMEA. The FMEA should be a living object which is referenced and updated when making design changes, incorporating aspects of the design into a new design, as new failure modes are discovered, or if the scoring proves incorrect (DOD, 1949; DOD, 1980). Thus, while the expectation is that there is a completion point for a given FMEA analysis, it is expected to have high reuse throughout the life of the system.

Criticisms of FMEA. During the more than 70 years of use across many industries, practitioners of FMEA have identified challenges in the process' application. As an example, McKinney discussed the difficulties in applying FMECA in a case study on an approach radar system, establishing seven categories of deficiencies (McKinney, 1991). Ten years prior to the McKinney article, the US Military had further codified the FMEA process into a military standard, MIL-STD-1629A (DOD, 1980). In this revised standard, the Department of Defense (DoD) had specifically addressed the seven issues that McKinney (1991) identified as deficiencies in his analysis. However, McKinney evaluated FMEAs from nine different vendors and discovered that all of them had some fraction of his seven deficiencies, with at least one of them having all seven deficiencies (McKinney, 1991). This existed despite the MIL-STD-1629A being part of contract language for the generation of the applied FMEAs (DOD, 1980).

A comparison of the McKinney (1991) deficiencies to the military standard reference (DOD, 1980) is shown in Table 4. In his analysis, he emphasizes that the intent of the activity is for, "early identification of all catastrophic, critical and safety related failure possibility so they can be eliminated or minimized through design changes" [emphasis in the original] (McKinney, 1991). This clearly mirrors the intent of the FMEA process from its military origins, with nearly verbatim language in the original standard (DOD, 1949). Thus, despite the military standard providing specific procedures, instructions, and references to related standards, the errors occurred regardless.

Table 4: Comparison of McKinney (1991) Deficiencies vs MIL-STD-1629A (DOD, 1980)

McKinney Issue	**MIL-STD-1629A Related Section**
Lack of defined failure causes	5.4 Failure modes and causes – includes potential for lower level failures causing failures at higher levels in the system
Reckless and improper severity classification	3.3 Failure mode severity classification – provides both a severity scale and procedure for assessing different scenarios of failure in system.
No Data Sources	4.4.1.4 Reliability data – specifically calls out the requirements for use of reliability data in the analysis and calls out standards to govern the data generation.
Failure to recognize deficiencies and failure	4.5.2 Reliability criticality item list part e) – specifically calls out the use of the history of the design or similar designs

modes from earlier systems of similar design	
Lack of recommendations pertaining to the operation and support of the system	4.1.1 Mission functions and operational modes – specifically calls out starting at a high level and decomposing to lower system levels. It also calls out identifying alternative operation modes.
Narrow scope of analysis	4.4.2 FMEA part a) Define the system to be analyzed – articulates the need for complete system definition, including internal and interface levels as well as performance expectations at all levels of the system design.
Untimely submission	Appendix A 50.1.2 Timing – calls out that the analysis needs to provide actionable information "at or before a project decision point". Further, it indicates that the FMECA plan must provide support to design during system development

Similarly, but more recently, Bluvband and Grabov (2009) performed a direct analysis of the FMEA process identifying specific pitfalls. While the exact terminology is somewhat different, they identify issues in the FMEA process remarkably similar to McKinney (1991). Interestingly, Bluvband and Grabov (2009) did not reference McKinney (1991) anywhere within their article, indicating that their research was independent of McKinney's work from 18 years earlier. And even more recently, Silverman and Johnson (2013) performed an analysis of FMEA independent of these two previously mentioned analyses. However, Silverman and Johnson (2013) took a different approach in their research from the previous two, looking at organizational implementation issues for FMEA rather than direct execution problems; in which they also articulate a set of reasons why FMEAs fail, several of which are familiar from both McKinney (1991) and Bluvband and Grabov (2009). Table 5 shows how the three different independent analyses concluded largely similar problems in FMEA application.

Table 5: Comparison of Issues within FMEA Identified by Three Independent Articles

Issue Category	McKinney (1991)	Bluvband and Grabov (2009)	Silverman and Johnson (2013)
Data	No data sources	Use of irrelevant statistics	*No direct equivalent*
Severity Classification	Reckless and improper severity classification	Wrongly defined criteria for high priority items and undefined risk acceptance criteria	Scoring system not customized/ Scoring system not developed ahead
Design Stage Use	Failure to recognize deficiencies and failure modes from earlier systems of similar design	Missing failure modes and lack of guidelines for the optimal choice	Identifying failure modes but not prioritizing/ mitigating the correct ones
FMEA Scope	Narrow scope of analysis	Narrow definition of failure (related to scope)	Agenda not clear from the start/ Try to take on too big of an FMEA

Even more recently, a meta-analysis on FMEA literature was performed, in which they synthesized published criticisms of FMEA across 220 scientific papers and 109 patents (Spreafico, Russo, &

Rizzi, 2017). Spreafico et al. (2017) identified four major problem classifications affecting FMEA: 1) Applicability, referenced in 86 citations, relating to it being time-consuming, expensive, lack of repeatability, subjectivity of results based on users, difficulty in managing data/information, and late applicability; 2) Cause and Effects, referenced in 38 citations, relating to shortcomings in failure determination; 3) Risk Analysis, cited in 45 publications, relating to ambiguous criteria for quantifying risks; and 4) Problem Solving, referenced in 22 papers, relating to poorly-defined problems and poor solution implementation.

As further evidence of the consistency with which similar issues in FMEA are identified, Ouyang et al. (2021) outlined three major flaws in applying FMEA to real-world problems: 1) Difficulty in obtaining accurate values of risk factors for every failure mode; 2) Weighting the risk factors not being considered; and 3) Issues with the use of the RPN methodology. Once again, the same themes emerge regarding criticisms of FMEA across the various authors of these papers.

These specific flaws identified by Ouyang et al. (2021) clearly trace to the type of scoring and prioritization issues raised by McKinney (1991) more than 30 years prior. As with their predecessors, Ouyang et al. (2021) propose methods to address these flaws, largely through scoring methodology improvements. While their proposals are interesting and sophisticated, it is not clear that they, like their predecessors, solve these problems that continue to be raised in research.

Scoring methodology is among the most active areas of research regarding FMEA and in identifying challenges with the common scoring methodologies (Spreafico, Russo, & Rizzi, 2017). Particularly when using either criticality matrix or RPN methods, equivalent resulting scores may not represent equivalent concerns to the business. Despite the appearance of the RPN being a mathematical expression, the resulting values represent an ordinal sorting of the ID lines, not a mathematical one. Therefore, the relative difference between scores is not necessarily representative of the relative importance of the issue to the system design or the business. This research extends into review of the effectiveness of FMEA risk assessment by construction of a model for creating indices to measure the effectiveness to more sophisticated methods to augment the RPN approach (Panyukov et al., 2022; Lo & Liou, 2018). In the field of usability, these same challenges with FMEA (i.e., prioritization, scoring, and identification of risk factors) are becoming more common. Researchers are taking similar paths in the usability space to address these challenges as researchers in other areas have previously (Li & Zhu, 2020).

Viewing the body of research in total, we see that many of the same themes continue to persist since McKinney (1991). Further, in review of the standards dating back to the original MIL-P-1629, these problems are anticipated with cautions and various guidance provided to users to avoid them. These cautions and guidance have continued to be refined in the standards literature up to the most current releases such as IEC 60812:2018 (International Electrotechnical Commission, 2018) and the joint FMEA handbook (Automotive Industry Action Group, 2019). For such problems to continue to persist implies some form of systemic mismatch between the FMEA logic and typical system development logic. Therefore, the next section will introduce and discuss one of the most common systems development models currently in practice, the systems V-model.

Systems Engineering V-Model

Background. As software development activities became more significant in the 1980s, the need for management of software development became prevalent. In 1985, the US DoD issued DOD-STD-2167, superseded by DOD-STD2167A three years later, to provide expectations for management of defense software development (DOD, 1985; DOD, 1988). This standard discussed many systems engineering concepts associated with progression of development with parallel paths for both software and hardware development, as summarized in Figure 1. This standard provided detailed

expectations of work products for military projects, clearly articulating an expectation of familiar ideas of system decomposition, system block diagrams to define architecture, and related work products.

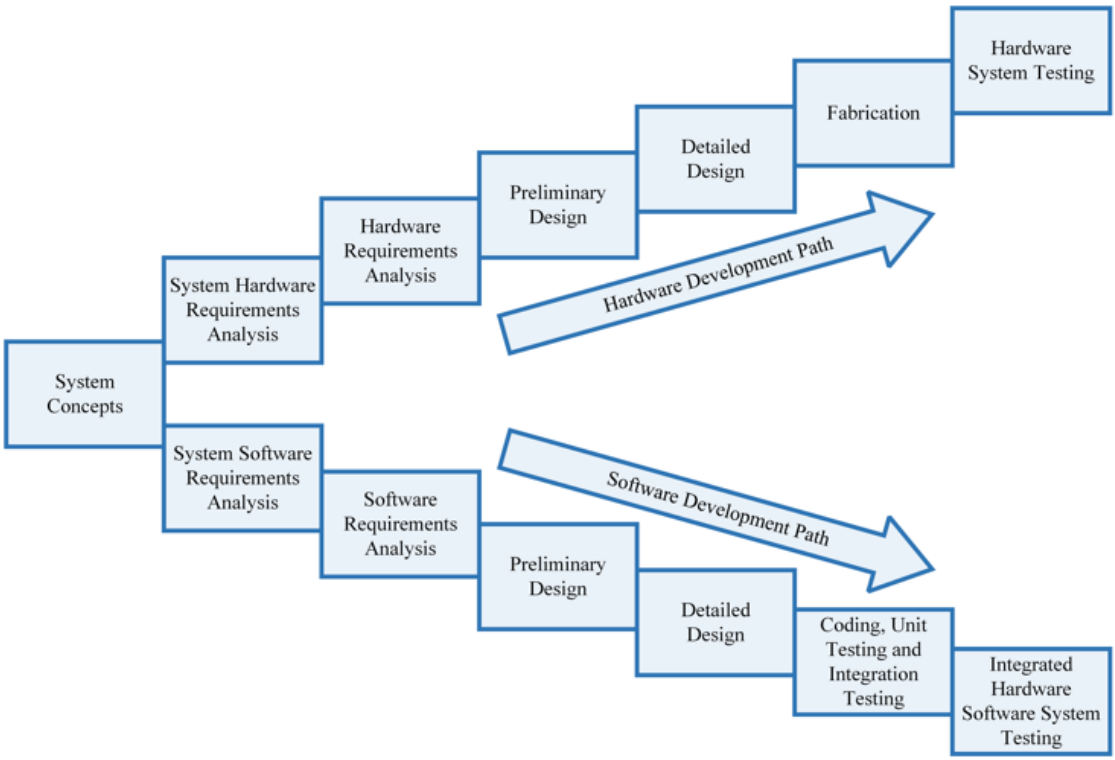

Figure 1. Adapted from DOD-STD-2167A Development Logic (DOD, 1988)

Rook (1986) introduced one of the first papers on the management of software development, which was based on the idea that development should be science rather than an art. His paper introduced the concept of the V-model as a development approach. A significant novelty to Rook's (1986) work over the ideas of the DOD-STD-2167A standard was identifying confidence points for the development process which related to the development activity, which were not clearly articulated in the standard. He raised the reality that in software development, the stages identified in DOD-STD-2167A (DOD, 1988) were not as distinct and linear as the standard proposes, requiring some level of confidence at different levels. However, the development logic closely matches the logic proposed in DOD-STD-2167. A replication of this V-model is provided in Figure 2, with annotations from related elements in DOD-STD-2167A. Rook (1986) illustrates the importance of connection between testing and development as the development process occurs to achieve confidence in the design. By making the arrows bi-directional, he illustrated the iterative nature of software development, which is not recognized by DOD-STD-2167A. Similarly, Juristo et al. (2007) demonstrate that software design must include usability no later than the design stage, otherwise resulting in unusable software and intolerable costs. Further, Horskey et al. (2010) discuss the requirement of recurring usability evaluations during system design.

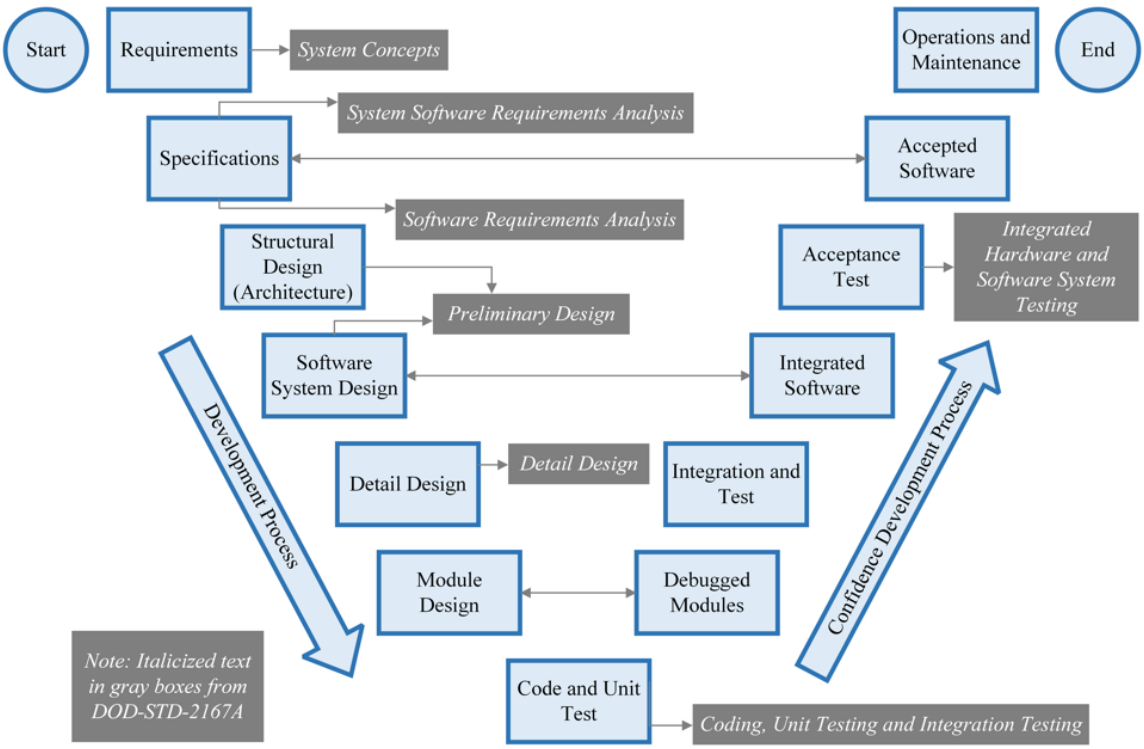

Figure 2. Adapted from Rook's (1986) V-model with Annotation *(gray boxes)* Overlaid from DOD-STD-2167A (DOD, 1988)

In 1992, Forsberg and Mooz (1992) discussed the connection between the V-model and systems engineering, and the development of complex systems with hardware and software, not only software. Rook's (1986) "confidence development path," or how he related development to testing was recognized by both Foresberg and Mooz (1992) in research and by the US government in practice (Under Secretary of Defense Acquisition, 1991). Specifically, the DoD called out a requirement for prototypes as part of the development activities to demonstrate the maturity of design at the different levels (Under Secretary of Defense Acquisition, 1991). Forsberg and Mooz (1992) generalized the original work from Rook (1986) to apply to systems development more broadly, as shown in Figure 3. In their enhancement of the original model, Forsberg and Mooz (1992) condensed some of the steps without losing the essential idea that the design starts with a definition of end-user needs. In their process, the designers continue from there by decomposing and defining the design from the system level down to the level of individual elements and components (Forsberg & Mooz, 1992). Forsberg & Mooz (1992) presented the idea that at each level of design, the plan for inspection, verification, or validation of that element of design must be created as well. This inherently demands a level of discipline in the design in that three elements need to be present to generate any sort of verification plan: 1) A requirement or specification that needs to be met; 2) A method of inspection, verification or validation; and 3) An acceptance criterion to disposition the outcome of the inspection, verification or validation (Forsberg & Mooz, 1992). These elements, as Forsberg and Mooz (1992) discuss in their detailed diagrams and text of "off core" activities, drive a level of understanding and rigor in the design that may not be achieved otherwise.

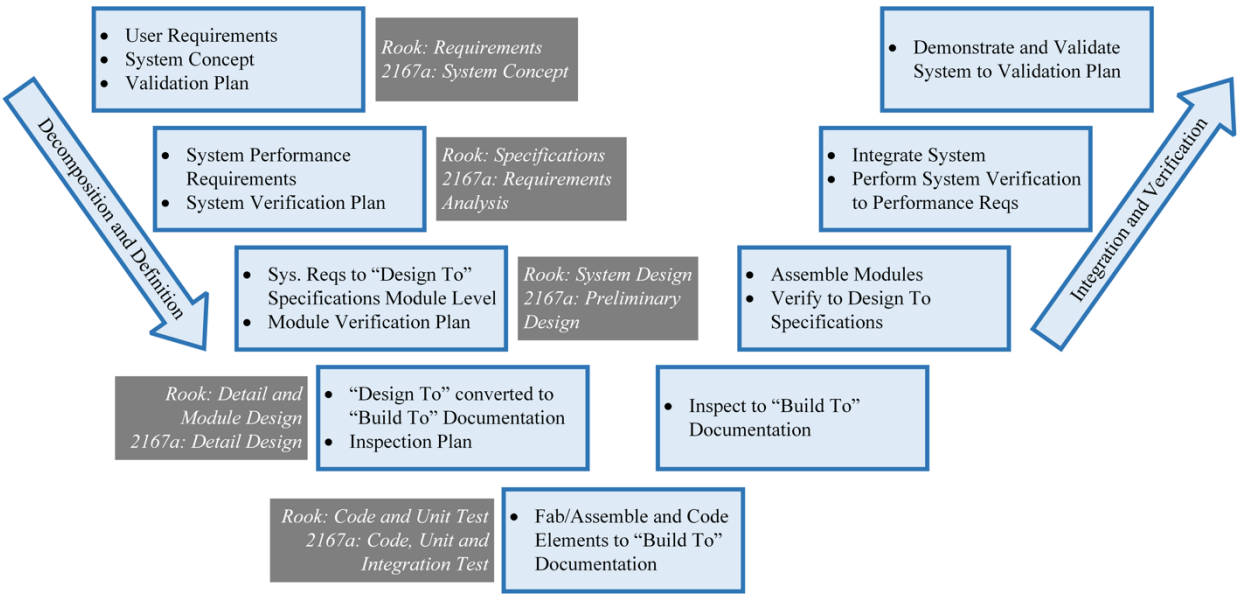

Figure 3. Adapted from Forsberg and Mooz (1992) V-model with Annotation *(gray boxes)* from Rook (1986) and DOD-STD-2167A (DOD, 1988)

In review of the three works from DOD-STD-2167A (1988) (the initial defense software development framework) to Rook's (1986) V-model (the creation of the V-model structure [for software development]) to Forsberg and Mooz's (1992) V-model (the application of the V-model to both software and hardware development), the V-model is refined, but the core elements remain the same. The V-model continues to be relevant in academic research and industry. Reflecting this in the usability research space shows that addressing usability in the development process is of great interest and as discussed previously, industry, particularly those that are closely regulated, have a need to incorporate usability into their development models.

Using FMEA within the V-Model

Building on the literature discussed above, a generic V-model can be described with the following basic steps and resulting objects contextualized for a human factors perspective:

1. *User Needs:* User requirements, user workflows, feature and function descriptions in user language and basic system concept.

2. *System Requirements:* High level system architecture/ platform with major subsystem decomposition and interfaces. System level performance requirements. This would be where the intended user interface for a system would be defined at a needs level.

3. *System Design:* Detailed system architecture, identification of subsystem design reuse elements, decomposition, and allocation of system requirements to subsystems.

4. *Detail Design:* Design of subsystems, decomposition, and allocation of requirements to modules.

5. *Module Design:* Design of modules, decomposition, and allocation of requirements to elements.

6. *Fabrication, Coding, Initial Integration:* Matured prototypes tested with initial integration and lower-level module testing.

These six steps represent the left side of the V, genericized to be applicable to both hardware and software systems, based on the foundational work of literature mentioned above (DOD, 1988; Rook, 1986; Forsberg & Mooz, 1992). To synthesize these arguments presented, Table 6 compares the typical columns of an FMEA (as detailed in Tables 1, 2 and 3) with the information required to perform an FMEA (as detailed in IEC 60812:2018), and with the earliest step of the V-model that this information is available for a system level FMEA (International Electrotechnical Commission, 2018).

Table 6: Comparison of Information Required for an FMEA and Information Available based on V-model Process

FMEA Column	Information Necessary to Perform FMEA	When Information is Available in a Generic V-Model
Element	Element definition within architecture	Step 3 (System Design)
Functions and performance standard	Requirements defining the expected performance for the element and its interfaces	Step 2 (System Requirements)
Failure mode	All possible ways the element can fail to meet the requirements	Step 1 (User Requirements) and Step 2 (System Requirement)
Local effect of failure	Impact of the failure at the local level	Step 3 (System Design)
Final effect of failure	Impact of the failure at the user or system level	Step 1 (User Requirements)
Cause of failure	Design detail to determine how the element can physically fail to cause the failure mode	Step 4 (Detail Design)
Initial state mitigation	Detailed understanding of design reuse to determine mitigations that have proven effectiveness	Step 3 (System Design) and Step 4 (Detail Design)
Initial state scoring (S x O x D = RPN)	Detailed understanding of design with data to understand cause of failure, to failure mode logic with data to determine scores	Step 4 (Detail Design) and Step 5 (Module Design)
Future state mitigations	Detail understanding of what will be incorporated into the design to address the failure mode	Step 4 (Detail Design)
Post mitigation rescoring (combined S x O x D)	Detail understanding with test data to determine the score of the new mitigations	Step 6 (Fabrication and Initial Testing)
Evidence of effectiveness	Completed test reports showing mitigation effectiveness	Right side of the V (Verification Testing)

International standards and previous versions of FMEA advocates, and US military contracts may require, performing FMEA early in the design process before commitments have been made, so that

mitigations can be incorporated into design. However, Table 6 clearly shows that even with a system level FMEA, the information required to complete is realized throughout the entire V-model. Performing subsystem or module level FMEA, which are advocated for within the standards, will not have the required information for completion until the detail design stage at the earliest. When considering that FMEA is also typically an iterative process, with cycles of mitigation, test, new mitigation or modified mitigation, and new test, this problem becomes more stark.

When reviewing the research around the complaints and solutions presented, this topic is not explicitly discussed, rather only problems which are driven by this mismatch. Spreafico et al. (2017) specifically make the point that the majority of research they surveyed, whether industry or academic, related to some detailed aspect of FMEA execution: improvements in scoring, use of other tools to augment cause and effect analysis, and/or improvements to prioritization based on scoring. However, none of the works surveyed by Spreafico et al. (2017) offered an in-depth discussion of the mismatch between information required to perform the FMEA and what is available at the relevant phase in the V-model, beyond general research into the applicability of FMEA as a tool.

Further, in review of the V-model literature, the complexity of systems is represented with discussions on methods of managing decomposition and the like. In FMEA standards and literature, the decomposition need mirrors the V-model. However, this same literature provides little if any methods for managing this. Further, FMEA literature and standards emphasize capturing all failure modes and causes without providing an approach around how to adapt to this scale in large design efforts. In even moderately sophisticated products, it often is practically impossible to identify every failure mode and every failure cause.

Thus, it is reasonable to infer that a significant proportion of the historical reoccurring complaints about the use of the FMEA process derive from structural differences in information requirements between the FMEA logic and the V-model development logic, particularly as more complex designs are considered. Further, an emphasis on identifying all failure modes and causes of failures ignores the volume of these that can exist in complex design. Based on review of both research areas, there does not appear to be a focused activity to address this gap, and with increasing sophistication and complexity of products being developed, it is reasonable that the problems will persist and potentially worsen.

Conclusions

A possible conclusion of the analysis performed here is simply that FMEA and the V-model development are incompatible, requiring a choice of one or the other. Particularly for human factors, this would seem to be problematic as there is recognized efficacy in the use of FMEA as a tool in the use error and safety field, while also identifying methods to better integrate usability analysis into the systems development lifecycle. Therefore, we reject this premise, and believe that there is a way of adapting FMEA logic to the V-model development process. While further research is needed, in broad premise, this adaptation would modify FMEA in the following ways:

- Create a filtering process for evaluating the risks associated with an intended new design at an architectural level to determine where FMEA provides the greatest benefit. This filter would increase the design risk profile for new elements in the design in comparison to stable aspects of design with strong provenance being reused.

- Modify the FMEA process to allow it to be more flexible in information requirements to outputs depending on where in the V-model it is being applied.

- Create a structure to iterate and decompose the FMEA process in a synergistic fashion with the V-model process rather than a conflicting one.

- Take advantage of the “right-side” of the V-model to provide evidence of mitigation effectiveness consistent with the V-model process.

- Create the revised model as a framework for FMEA to operate under a V-model without preventing the use of improved methods being developed by other researchers in execution phases of FMEA.

As this work has shown, there is a significant mismatch between the information available at a given phase in the V-model process, and the information required to perform a rigorous FMEA. This informational mismatch, as Section 4 showed, underlies many of the issues identified by previous authors when integrating both processes. Further, this work has shown that there is an opportunity for novel research to address adaptation of the FMEA process to address these issues. Finally, we propose a direction for that research opportunity by describing topic elements to drive the framework for such a solution.

References

Association for the Advancement of Medical Instrumentation (AAMI) 2021, *Medical Devices - Part 1: Application Of Usability Engineering To Medical Devices + Amendment 1, ANSI/AAMI/IEC 62366-1:2015 (R2021)+AMD1:2020*, Arlington, VA (US).

Automotive Industry Action Group 2019, *Failure Mode and Effects Analysis: FMEA Handbook,* Automotive Industry Action Group, Southfield, MI (US).

Bluvband, Z, & Grabov, P 2009, 'Failure analysis of FMEA', *Annual Reliability and Maintainability Symposium*, pp. 344-347.

Chiozza, ML, & Ponzetti, C 2009, 'FMEA: A model for reducing medical errors', *Clinica Chimica Acta*, 404(1), pp. 75-78.

Department of Defense 1949, 'Procedure for Performing a Failure Mode Effect and Criticality Analysis', *United States Military Procedure, MIL-P-1929*. Washington, DC (US).

Department of Defense 1980, 'Procedures For Performing a Failure Mode, Effects, and Criticality Analysis', *United States Military Standard, MIL-STD-1929A*. Washington, DC (US).

Department of Defense 1985, 'Defense System Software Development', *United States Military Standard, DOD-STD-2167*. Washington, DC (US).

Department of Defense 1988, 'Defense Systems Software Development', *United States Military Standard, DOD-STD-2167A*. Washington, DC (US).

Forsberg, K, & Mooz, H 1992. 'The relationship of systems engineering to the project cycle', *Engineering Management Journal*, 4(3), pp. 36-43.

Geum, Y, Cho, Y, & Park, Y 2011, 'A systematic approach for diagnosing service failure: Service-specific FMEA and grey relational analysis approach', *Mathematical and Computer Modelling*, 54(11-12), pp. 3126-3142.

Horsky, J, McColgan, K, Pang, JE, Melnikas, AJ, Linder, JA, Schnipper, JL, & Middleton, B 2010, 'Complementary methods of system usability evaluation: Surveys and observations during software design and development cycles', *Journal of Biomedical Informatics*, 43(5), pp. 782-790.

International Electrotechnical Commission 2018, 'Failure modes and effects analysis (FMEA and FMECA)', *International Standard, IEC 60812*, International Electrotechnical Commission, Geneva, Switzerland.

Juristo, N, Moreno, AM, & Sanchez-Segura, M-I 2007, 'Analysing the impact of usability on software design', *Journal of Systems and Software*, 80(9), pp. 1506-1516.

Lo, H-W, & Liou, JJH 2018, 'A novel multiple-criteria decision-making-based FMEA model for risk assessment', *Applied Soft Computing*, 73, pp. 684-696.

Li, Y, & Zhu, L 2020, 'Risk analysis of human error in interaction design by using a hybrid approach based on FMEA, SHERPA and fuzzy TOPSIS', *Qualiy and Reliability Engineering International*, 36(5), pp. 1657-1677.

McKinney, B 1991, 'FMECA, The Right Way', *Annual Reliability and Maintainability Symposium,* pp. 253-259.

Ouyang, L, Yan, L, Han, M, & Gu, X 2021, 'Survey of FMEA methods with improvement on performance inconsistency', *Quality and Reliability Engineering International*, 38(4), pp. 1850-1868.

Panyukov, DI, Kozlovskii, VN, Aidarov, DV, & Shakurskii, MV 2022, 'Effectiveness of FMEA risk analysis', *Russian Engineering Research*, 42, pp. 1070-1072.

Ravizza, A, Lantada, AD, Sanchez, LI, Sternini, F, & Bignardi, C 2019, 'Techniques for usability risk assessment during medical device design', *Proceedings of the 12th International Joint Conference on Biomedical Engineering Systems and Technologies*, pp. 207-214.

Rook, P 1986, 'Controlling software products', *Software Engineering Journal,* 1(1), pp. 7-16.

Setiasih, PI, & Purnawan, J 2017, 'Effectiveness of failure mode effects analysis (FMEA) to reduce medical error', *Journal of Indonesian Health Policy and Administration,* 2(2), pp. 25-29.

Silverman, M, & Johnson, JR 2013, 'FMEA on FMEA', *Proceedings Annual Reliability and Maintainability Symposium (RAMS)*, pp. 1-5.
Spreafico, C, Russo, D, & Rizzi, C 2017, 'A state-of-the-art review of FMEA/FMECA including patents', *Computer Science Review*, 25, pp. 19-28.
Under Secretary of Defense Acquisition 1991, *Defense Acquisition Management Documentation and Reports.* Washington, DC (US).
US Food and Drug Administration (US FDA) 2016, *Applying Human Factors and Usability Engineering to Medical Devices: Guidance for Industry and Food and Drug Administration Staff, FDA-2011-D-0469*, Center for Devices and Radiological Health, Rockville, MD (US).

Biography

Dan Perreault is a PhD candidate in the Systems Engineering Department at Colorado State University. He is also the Director of Design Quality Engineering for Philips Ultrasound.

Erika E Gallegos is an Assistant Professor in the Department of Systems Engineering at Colorado State University. She holds a BS in Civil Engineering from Oregon State University and an MS and PhD in Civil Engineering from the University of Washington.

Vincent Paglioni is an Assistant Professor in the Department of Systems Engineering at Colorado State University. He holds a BS in Nuclear & Radiological Engineering from Georgia Institute of Technology and an MS and PhD in Reliability Engineering from the University of Maryland.

Thomas H Bradley is the Department Head and Woodward Professor in the Department of Systems Engineering at Colorado State University. He holds a BS and MS in Mechanical Engineering from University of California at Davis and a PhD in Mechanical Engineering from Georgia Institute of Technology.