INTERNATIONAL DESIGN CONFERENCE - DESIGN 2018
https://doi.org/10.21278/idc.2018.0211

A METHOD FOR FUNCTION INTEGRITY DIAGNOSIS AND DOCUMENTATION: FIDD

R. L. Wichmann, K. Gericke, B. Eisenbart and H. Moser

Abstract

This paper introduces a method to perform systematic diagnosis of function integrity. The proposed method advances the Integrated Function Modelling framework to extend its application to risk identification and documentation tasks. By analyzing the system model of interdisciplinary designs, this method guides the designer to explore function vulnerability by systematic decoupling of inherent design entities. Thereby it provides unique opportunities for failure mode identification in complex, interdisciplinary systems. The motivation for this method is ensuring system function integrity.

Keywords: conceptual design, risk management, risk identification, functional modelling, design structure matrix (DSM)

1. Introduction

With the scale of required investment and the wide range of critical mission parameters, the term 'space qualified components' in aerospace engineering has become synonymous with extraordinary quality requirements and high system complexity (McLoughlin et al., 2003). Such components require rigorous design and production processing, are time consuming in their instalment and subjected to highly sensitive tolerances. Aerospace engineering still demands these costly components to assure system robustness and minimize the likelihood of failure in systems. However, this strategy of quality assurance is expensive and places excessive importance on the final stages of development, which are then typically dominated by lengthy and iterative testing and adjusting of every single component (Wertz and Larson, 1999).

An alternative strategy has come up in the aerospace sector: in an effort to increase competitiveness through reduction of development and manufacturing costs, designers have started rethinking their conception of system reliability and robustness (Chen et al., 2012; Gluchshenko, 2012). While the current approach underlying the use of space grade components is to ensure robust designs by minimizing the absolute likelihood of failure (i.e. failure is NOT an option), the new approach allows a demand-driven margin for failure whilst system functionality remains ensured (failure IS an option, in certain areas). Instead of manufacturing every single component under extremely sensitive tolerance requirements, the system design could then be changed to afford some degree of irregularity to occur whilst still fulfil its central function unimpededly. Alternatively, building in strategic redundancies may achieve a similar tolerance for less than space grade components (McLoughlin et al., 2003). This article focuses on the decision making involved with determining which particular change *should* or *can be* made following the new strategy for system robustness. Designers will have to make well-informed choices on where the system may - and where it cannot - afford less than space grade components without increasing the level of risk to an unacceptable level.

Such decisions should ideally be made during the conceptual design phase as these decisions will affect the way functions are fulfilled, thus will affect the system architecture. An effective support lies within system modelling i.e. function and product architecture modelling. This combination aids the management of system interaction, facilitates design communication and consequently supports to create a robust design (Eppinger and Salminen, 2001).
System modelling has the benefit that models can be more easily tailored for a variety of uses. System models are simplified representations of reality that can include necessary information for users (Gericke et al., 2016). As long as the simplifications are known as limitations of the model, users (both modeller and reviewer) can focus their attention to facilitate specific design tasks. One method to focus this attention is to channel the perspective. The benefit of a model with a functional perspective is that the designer focuses on function integrity rather than working principles. The functional perspective guides designers to communicate referring to functionality, which is more inclusive than technical terminology and suitable for common understanding (Hirtz et al., 2002). This is especially beneficial in interdisciplinary design as design solutions require extensive effort to achieve concept cohesion (Eisenbart et al., 2017). System modelling also simplifies the transition from conceptual to embodiment design as designers can emphasise working interfaces during product development (PD) progression. One model that has evolved for the purposes of interdisciplinary design is the Integrated Function Modelling (IFM) framework (Eisenbart et al., 2017).
The IFM framework supports modelling of design information during the transition from conceptual to embodiment design. It is intended for interdisciplinary collaboration offering multi-perspective descriptions of a system at an abstract level (Eisenbart et al., 2013). It is structured in a framework that documents identified direct interaction in a system and links them to intended functionality. With few rules in notation, the IFM framework efficiently prepares the information so that design content is easily understood from intended function to interacting actors in one integrated function (IF) model.
Experienced designers will have insightful reason for their own design decisions including function fulfilment and possible risks. Risk management (RM) is the validation of design integrity and functional deployment. In many design projects designers are responsible for their own design validation. However, at the point of any legal certification, designs must be reviewed by a third party. Such a review i.e. RM can create an organizational and technical challenge. RM is complex and requires thorough documentation to facilitate the traceability of consequent design decisions. If RM is not adequately integrated into the PD process, risk information is likely to be incomplete and inadequate (Smith and Merritt, 2002). This can be critical for design integrity as RM demands comprehensive system understanding in order to reduce gaps in risk identification.
Unknown unknowns (i.e. unknown risks) jeopardize the success of development as experience with novel design solutions is not available. Designers could benefit during RM from a support that facilitates their holistic understanding of a novel system and thereby reducing the likelihood of unknown unknowns. This paper introduces the function integrity diagnosis and documentation (FIDD) method, an approach that pairs system modelling with system model analysis in order to support the designer in risk identification. The FIDD method guides the designer during the analysis of a system using an IF model to provide context and reference for possible risks. It is a means to facilitate comprehensive risk identification in order to perform effective RM and achieve robust design without reliance on space grade components.
This paper will begin with summarizing key features of system and function modelling that are applied in the IFM framework. These will be fundamental to the inherent design description for consequent model analysis. Next, it will discuss two established risk identification methods and outline their potential for application in model analysis. Finally, it will present the FIDD methodology and illustrate its application within an industrial case study example.

2. System and function modelling

A means for securing competitiveness in aerospace engineering is to provide a range of services where customers can tailor deliverables to their needs (Johnstone et al., 2009). Satellite manufacturers have to offer multi-functional designs to serve the demand for a broad variety of applications. This leads to an increase in number of requirements which, by extension, drives the complexity of the technical portfolio

and the collaboration of interdisciplinary expertise. The challenge of such collaboration is communicating concept (idea) cohesion among non-experts (Moser, 2014). With the engagement of design teams involving a high degree of diversity among technical backgrounds, it becomes difficult to facilitate a dialogue where none are experts in all disciplines.
It has become common practice to apply system modelling to help in PD progression, and the largest potential to (re-)shape an emergent design easily and with limited additional costs and efforts lies in the conceptual design phase (Maarten Bonnema and Van Houten, 2006). In the conceptual design phase, functional requirements are linked with a proposed working solution, which constitutes the central step between abstract and concrete (Andreasen, 1994).
Design research and practice have produced a variety of different function modelling approaches (Vermaas, 2011). The IFM framework offers a possibility to accommodate interdisciplinary design description by allowing the designer to integrate six different design entities typically used for function modelling and model them as inherently linked views (Eisenbart et al., 2017). Table 1 describes these entities. The benefit of modelling these different design entities is that it guides the designer to explicitly consider different descriptive content.

Table 1. Description of entities addressed in IFM framework (Eisenbart, 2014)

Entities		Description
Use Case		Different cases of applying the system. This is typically associated to the interaction of actors with the system under development, which may require subsequent transformation processes to take place. The associated set of processes lead to an observable result, in order to provide some kind of value to users.
Process	**Transformation process**	Processes executed by actors, which (from the designers' perspective) are part of the system under consideration and may lead to a change of state of actors or of operands. *Technical processes* are transformation processes related to technical sub-systems; *human processes* are related to stakeholders (thus, including service activities).
	Interaction process	Representation of interaction processes of actors, which (from the designers' perspective) are *not* part of a system, with actors, which *are* part of the system under consideration.
Effects		Representation of the required physiochemical effects, which have to be provided, in order to enable or support transformation and/or interaction process(es).
States		Representation of the states of actors or of operands before (input) and after (output) a transformation process.
Operands		Operands are typically specifications of energy, material, and information.
Actor	**Stakeholder**	Stakeholder comprises (groups of) animate beings affected by or affecting the system under consideration (including any related services).
	Environment	Environment includes all active and passive parts of nature in general surrounding the system under development.
	Technical sub-system	Technical sub-systems encompass technical systems (i.e. technical products, potentially combining mechanical, electrical, and software systems with associates services), which are part of the system under consideration. They can be composed of more technical sub-systems.

Another advantage of the IFM framework is the way it represents modelling information. Adopting the approach of design structure matrices (DSM) (Eppinger and Browning, 2012), an IF model is a matrix based representation that visualizes design content in a clearly structured manner (Eisenbart et al., 2017). The six design entities are documented in interlinked matrices as can be seen in Figure 1.
A completed IF model would encompass design description of all six design entities and would allow the designer to effectively track the inherent system interactions by use of the interlinked matrices. The designer has the possibility to visually compare the modelled design entities for logical consistency. This creates ideal conditions to assure model accuracy and facilitates model analysis. What makes the IFM framework interesting for further development is this potential to be applied in further model analysis. It distinguishes itself from other modelling approaches with the successful integration of three characteristics. The first being its focus on system function creating the potential to be involved in the earliest conceptual design stages of PD. The second is how it accommodates interdisciplinary design descriptions by providing a means to model design entities relevant across disciplines. And thirdly, the interlinked framework of matrices allows structuring design information for effective review. These three characteristics prompt the research for further development of the IFM framework as a tool supporting effective risk management at a function-related level.

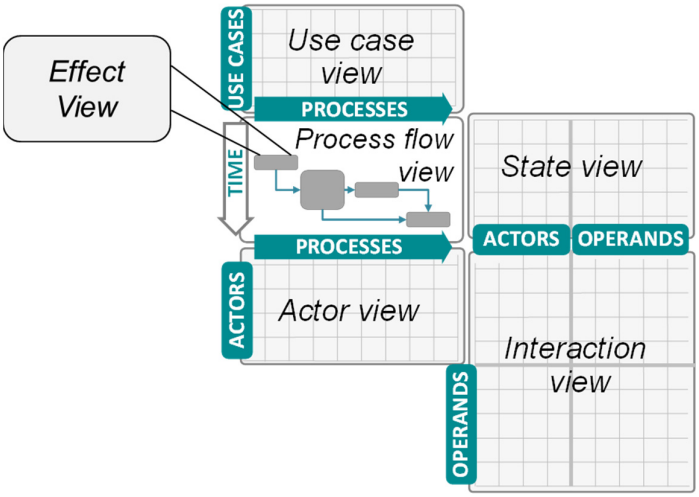

Figure 1. Integrated Function Modelling framework (Eisenbart, 2014)

3. Risk management

A precondition for creating successful designs is the validation of project deliverables to assure that known factors and the degree of risk do not jeopardize the integrity of system function. With the assumption that risk free design cannot be assured in PD, industrial practice prescribes that there has to be an acceptance of some risk for any selection of a working concept (Aven, 2016). Fault free design, similar to space grade components, is not economical. The goals for successful design is *managing* system risk effectively rather than *eliminating* it. One of the significant developments in this respect is the integration of RM into the PD process (Bassler et al., 2011). This section will focus on the topic of state-of-the-art RM and the necessity of comprehensive risk identification in design.

3.1. Identification of failure modes

One of the challenges of RM is accommodating for uncertainty and reducing any gaps in assumptions about system parameters (Loch et al., 2007). This highlights the condition that unknown risks (no matter how severe) are more hazardous than any known risk (Kloss and Moss, 2008); unidentified risk is unacceptable risk. Identified risks can be reduced or mitigated, though the obstacles to risk reduction are often unsystematic diagnosis and missing documentation. Designers intuitively create designs well suited against known risks, however neglecting to document their process and decision making intensifies the need for guided risk identification. In the review of a design, the effectiveness of risk diagnosis is essential in assuring successful PD and system integrity (Bahr, 2014).

This paper will apply the definitions of state-of-the-art PD terminology. "Risk" includes a vulnerability to a function and "failure" is any situation in which a function does not reach its intended degree of performance (briefly or irrevocably) (Pahl et al., 2007). These risk carriers (characteristic that jeopardizes function) will be referred to as a failure mode. Risk identification is to make a comprehensive inventory of all conceivable failure modes present in a system.

A technique that is tailored for the application of identifying failure modes is the fault tree analysis (FTA) (Vesely et al., 1981). FTA begins by focusing on a single top-level system requirement and reformulating its meaning into an undesirable event. It then prescribes chain-event-logic to diagnose the failure for the causing failure mode(s). This continues until the designer has documented all conceivable upstream (causing) failure modes of every failure mode. The resulting diagram resembles a tree with spreading branches as failure modes accumulate in reference to the original top-down failure. These ends of the logic chains are then documented as failure modes are analysed to what degree they jeopardize the integrity of the system in the form of risk. A generic example of a FTA branch diagram is illustrated in Figure 2.

However, FTA also has limitations: while FTA prescribes formal diagram notation and mathematical probability description (Vesely et al., 1981), it offers no procedure to support deductive reasoning or

diagnosis procedures. This becomes particularly challenging when RM is insufficiently integrated in novel design projects. Performing an FTA requires experience and system knowledge. With designs of high technical novelty, system knowledge could be limited and existing designs may lack background information to offer an approach for system diagnosis. Depending on the level of detail in a given design, the FTA could yield thousands of failure modes but with no previous system experience, the designer may miss crucial system dependencies. With an unknown system, the designer performing an FTA will have a difficult time gauging whether the assumptions are accurate or if there are gaps in possible failure sources.

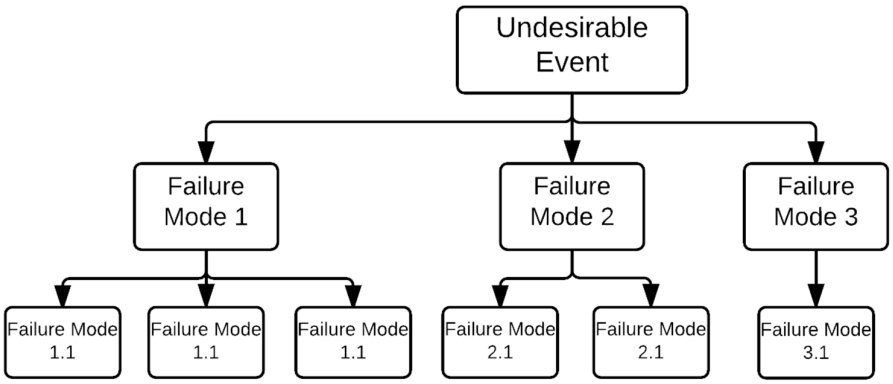

Figure 2. Generic FTA branch diagram

3.2. Tracking of failure modes

Comprehensive risk identification is a prerequisite of all subsequent RM processes. A key factor determining system integrity is how well the found failure modes are evaluated in further assessment. The resulting information must be prepared in an effective way to make assessment clear and comprehensible. This requires that there is a systematic scheme to contextualize the failure mode in how it effects the system. However, this is where the few existing rules of notation quickly reach their limitations. The branch representation of a failure tree supports the process of tracing the logical sequence of failure modes but reaches its limits at a certain degree of granularity. Even in the scale of projects with less than one hundred actors, such a representation can quickly become overwhelming and should be limited to workshop discussions. One approach to manage these large numbers of failure modes is to make inventory of them in form of lists. An established method that applies this approach is the failure mode and effect analysis (FMEA).

Each industry has its own standards for applying the FMEA; but it generally serves as the documentation of failure modes and can potentially complement all RM tasks in design projects. However, to effectively facilitate the evaluation of failure modes, the FMEA also requires a systematic scheme of contextualization.

3.3. Towards a function based approach

Classical risk analysis methods have the tendency to be applied in the mature stages of design. For example the FMEA is a bottom-up approach evaluating the reliability of individual components (Pahl et al., 2007). Thus, such an analysis requires knowledge about explicit actors, which usually is not available during conceptual design.

Following the philosophy that quality should be designed and not controlled (Karapetrovic and Willborn, 2000) it is necessary to integrate RM procedures into earlier design stages. Recent studies have facilitated this advancement of RM by adapting the RM methods to incorporate a function-based approach (Kurtoglu et al., 2010). A function based approach relies on the premise that failure modes are an inherent characteristic of function rather than an attribute of individual actors (Tumer and Stone, 2003). The benefit is that risk identification can be based on system models and only vague detail of design embodiment allowing designers to track failure modes back to function and therefore analyse system risk at an abstract level.

3.4. Potential improvements

To accommodate a margin for failure in design, the risk of an event must be foreseeable. This can only be achieved with comprehensive risk identification and effective RM. FTA and FMEA support risk identification and subsequent assessment and documentation. However, these methods still require improvisation of the designer. As discussed above, in FTA, the comprehensiveness of the documented failure modes is dependent on the designers' understanding of the system. The weakness of FTA is that in a very novel design, designers might not be aware and unable to apprehend all relevant failure modes. This should not be attributed to human error as the degree of novelty could exceed that of established state-of-art, but rather bring attention to a lack of methodology guiding the designer. In addition, an FMEA in its generic description offers little reference in documenting failure mode context. Such limitations raise the potential for development. If there was a method to guide designers during the diagnosis of failure modes then one could place more confidence in the resulting FTA and documentation. This paper will introduce a method that aims to accomplish the following objectives:

- Be applicable in conceptual design stages;
- Provide structure in design diagnosis;
- Prepare documentation to be comprehensible and with context.

4. Function integrity diagnosis and documentation method

In an effort to accomplish the aforementioned objectives, the FIDD method evolved out of integrating system model analysis, through utilising the IFM Framework, with established RM tools. The primary objective is to systematically analyse an IF model and make inventory of all possible failure modes. It prescribes a step-by-step diagnosis of an IF model to provide documentation to analyse if function integrity is in critical jeopardy. The resulting method will increase success of risk identification and support understanding of failure mode deduction. This section will describe a method to track system interfaces using the IFM Framework to perform a comprehensive FTA.

4.1. Method procedure

FIDD prescribes formal diagnosis guidelines to analyse design content and offers a repeatable process to create assumptions about possible failure modes. The FIDD method requires a preferably completed IF model. However, an IF model supports continuous refinement so completeness of all IF model views is not mandatory. Additional information can always be included as increased detail of an IF model determines the comprehensiveness of the resulting FTA.

The FIDD methodology is detailed in the following seven steps:

1. *Negate or reformulate the Use-Case into an undesirable event.*
   No matter the scope of the assessment, the designer will begin with the use-case view of the IF model. This ensures that the designer focuses on the overarching function of the system. This top-level function will be formulated as an undesirable event. If the designer lacks assumptions about the degree of the alteration, the use-case should be reformulated using opposing language to negate its meaning. (Example: Channel Fluid → Fluid Withheld or Fluid Not Channelled)
2. *List the transformation processes from upstream to down-stream as undesirable events.*
   Listing the transformation processes by process flow will have the benefit that the input flow of previous and/or requisite processes is included in the documentation. If there are parallel (simultaneous) transformation processes, they are listed separately. The processes are documented as undesirable events. If the process flow view notates functions as a verb + noun (Pahl et al., 2007) then these can also be negated using opposing language (Example: Open Valve → Valve Does Not Open).
3. *For each* transformation *process list the state-change as incomplete.*
   The state view documents the intended state change of each transformation process. The designer will take the final state of each transformation and assume that it has not been achieved. No matter the degree of the possible failure (99% of performance) the designer assumes that the system remains in its initial state. (Example: Closed Valve → Valve Remains Closed)
4. *For each incomplete state-change list all affecting actors and operands.*

Make no distinction in the treatment of actors and operands.

5. *For each affecting actor list all interactions in the interaction view.*
6. *Question the integrity of the documented constellation and list a failure* consequence.
   Ask the question, what is the consequence of the undesirable events occurring in the constellation in which they are documented? The result will formulate a failure.
   (Example: Valve Remains Closed → Vessel Pressure Rises)
7. *For each* failure *consequence list the possible failure mode.*
   Return to classical engineering/business instruction to formulate the possible failure mode.
   (Example: Vessel Pressure Rises → Valve Gate Is Jammed)

With these seven steps, FIDD can include a substantial inventory of direct interfaces and constellations that act as a premise for failure modes. Such a premise would provide the designer with the context to diagnose how system function could be vulnerable to risk.

Diagnosis and documentation should be a synchronised procedure in risk identification. The seven steps of diagnosis already infer the recording of failure mode information and act as inputs to the corresponding documentation. However, if visualized as a standard FTA diagram, the tree representation of FIDD method diagnosis would branch into seven levels. Due to the impracticality of this representation, FIDD does not adhere to the standard FTA representation and prescribes documenting all failure modes in a checklist comparable to an FMEA. FIDD proposes to contextualize failure modes in a list of seven columns which will ensure structured organization and allow for a systematic tracking of failure modes according to function. Figure 3 summarizes how the IF model is analysed to perform risk diagnosis and how each step serves as input to failure mode documentation.

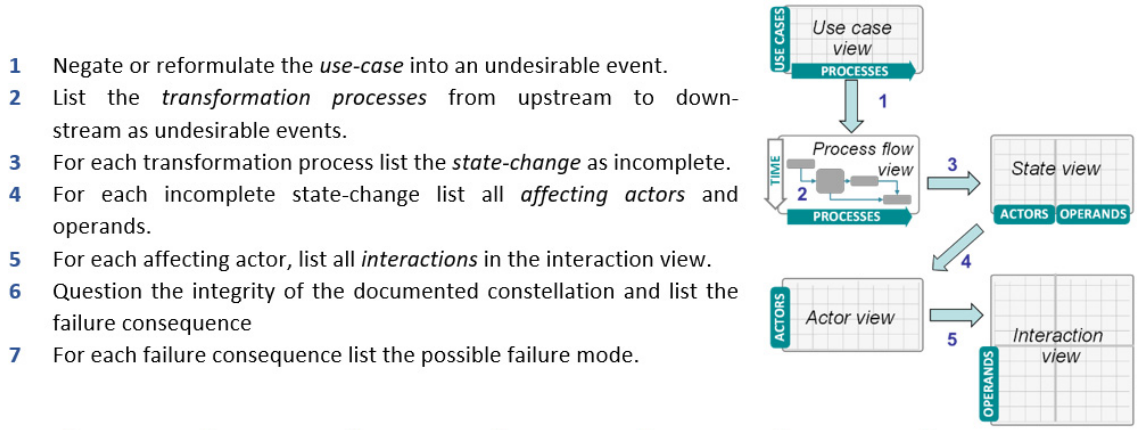

Figure 3. Analysing an IF model with FIDD

Five of the seven steps are illustrated to highlight how the designer can track function to failure mode by analysing an IF model. As the engagement of the designer and the involved effort cannot be predetermined, step six and seven are not explicitly visualized. Steps six and seven also determine that analysing an IF model cannot be algorithmically automated but requires the support of the designer to hypothesize about possible failure modes. The individual column content is detailed in Table 2 and will follow the example of the diagnosis procedure from left to right. The remaining three columns adhere to the standard FMEA procedure and document the qualitative severity, probability of occurrence and likelihood of detection (Pahl et al., 2007). The FIDD method provides no altering procedure to the quantitative assessment of the risk priority number (RPN).

Table 2. Description of FIDD column content

1. Potential Failure Mode (Use Case)	Provides context for the top level function; important for keeping a system view perspective.
2. Potential Failure Mode (Transformation Process)	Provides context about intended transformation process in the overall process flow.
3. Potential Failure Mode (State Change)	Provides context about what state changes must occur to perform each transformation process.
4. Potential Failure Mode (Affecting actors)	Provides context for which actors are necessary in performing a state change.
5. System Interaction (DSM)	Provides context for which actors share an interface (are involved) with the affecting actor.
6. Failure Consequence	Provides context for what undesirable event or consequence of failure is to be avoided.
7. Failure Mode	Provides context for what could be the source (failure mode) for the undesirable event.

5. Application of FIDD

To test the plausibility, the introduced method was applied in a case study with an SME in the aerospace sector. Motivated by the various solution concepts available in the satellite industry and with the aim to diagnose unique models, the following case study analysed a Hold-Down and Release Mechanism (HDRM). A HDRM is a satellite module with two intended use cases; hold-down folded solar wings during preparation and launch, and release (deploy) the solar wings once in orbit. Folding the solar panels is needed due to volume constraints during launch. The two use cases contribute to overall system performance in case the HDRM does not function, the satellite will not generate power, empty its batteries and stop functioning. Therefore, the HDRM is a critical element in the operational deployment of a satellite. Figure 4 illustrates the transition from a stowed solar wing configuration to a deployed solar wing configuration.

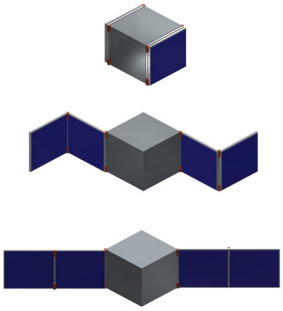

Figure 4. Solar wing transition from stowed to deployment

Due to the conditions of operating in such adverse working environments and cost-of-mass launched into orbit, the aerospace market has developed a variety concepts to create HDRMs. The engineering challenge of this mechanism is that it must be capable of mechanical contradiction. The HDRM must be able to securely fasten the solar wings in their folded position to prevent damage during launch but also be able to remotely cancel this connection for deployment.

5.1. Case example

This paper will discuss a case example of an HDRM functioning on the working principle of a thermal cutter. Independent researchers applied the FIDD method in order to make inventory of failure modes with unfamiliar designs. Their findings were compared and appraised by the enterprises' internal designers for discussion. This following section will go through the step by step process of interpreting the derived FIDD results for two specifically critical failure modes. The exert from documented failure modes is shown in Table 3, and the highlighted text is explained from left to right in a step by step approach.

1. This analysis focused on the use case *Hold-Down Solar Wings* during handling, launch, and acceleration. It defines the undesirable event as *Solar Wings unsupported*. The first column documents which overarching function (the use case) is the focus of the analysis.
2. The use case Hold-Down solar wings has many contributing functions (not in visual) one of which is In-Plane Fixation. This function is negated and documented as *No In-Plane Fixation*.
3. The function In-Plane Fixation involves two state changes. One of which is *dampen system* and the other is *sustain preload*. These state changes are treated as failed (ineffective). This explanation will continue with the failed state change *Does not Sustain Preload*.
4. The state change *Sustain Preload* has 12 directly affecting actors. These actors are listed and the explanation will continue with *Melting Assay*.
5. Each affecting actor has system interactions that are documented in the DSM of the IF Model. These interactions should all be documented; the melting assay has three direct interactions. Actors, such as Coil Clamp, Latch Sleeve and Screws should all be listed.
6. With the context provided from the previous columns the designer can now start creating assumptions about possible failure consequences. Using the three conceptual descriptions (use case, function and state change) of the IF model, the designer should be provided enough context to question the integrity of the given constellation. In the context of the *Melting Assay* and the *Coil Clamp*, the undesirable event is *Loss of Position*.
7. With the assumption about the undesirable event and knowledge of the specific constellation, the designer can return to classical engineering/business instruction. In the given instance, mechanical resonance is the systems response to vibrations and depending on their magnitude they can be fairly destructive to the structural integrity. Given the context between the interface of the *Melting Assay* and the *Coil Clamp* the designer can assume that the system is in jeopardy from *Vibration*s.

This summarises how the first group of failure modes are found from analysing an IF model. However, the designer should not be constrained to limit their consideration to these failure modes. Independent of interacting actors, the IF model provides enough context to explore further design weaknesses for singular actors. In Table 3, there is a second highlighted row that illustrates how the designer found failure modes for the *Melting Assay*. This assay is nothing more than a melting coil with imbedded ends; it too is subjected to the accelerating vibrations and is in jeopardy of severing. Such assumptions should never be neglected in risk identification and are therefore also documented.
The seven left columns of Table 3 are constituent of FIDD method. They prepare the information for further risk analysis. The four right columns adhere to the standard FMEA risk assessment procedure and are visualized to provide a more comprehensive example.

Table 3. Sample of FIDD results

							Current Situation			
Potential Failure Mode (Use Case)	Potential Failure Mode (Transformation Process)	Potential Failure Mode (State Change)	Potential Failure Mode (Affecting Actos)	System Interaction (DSM)	Failure Consequence	Failure Mode	S	P	D	RPN
Solar Wings Unsupported	No In-Plane Fixation	Does Not Dampen	Frame	Payload	Amplified Vibrations	Exceeding Assumptions	9	1	2	18
				Satellite Body	Amplified Vibrations	Improper Assembly	9	1	1	9
				-	Amplified Vibrations	Improper Assembly	9	1	2	18
			Satellite Body	Payload	Amplified Vibrations	Exceeding Assumptions	9	1	2	18
				Control Unit	Disabled Connections	Exceeding Assumptions	9	1	1	9
				Power Supply	Disabled Connections	Exceeding Assumptions	9	1	1	9
			Housing	Push-Up Tube	Amplified Vibrations	Loss of Preload	9	1	1	9
				Wedge	Amplified Vibrations	Loss of Preload	9	1	1	9
				Socket Screw	Amplified Vibrations	Loosening of Bolts	9	1	1	9
				Screws to Keyway	Amplified Vibrations	Loosening of Bolts	9	1	1	9
		Does Not Sustain Preload	Melting Assay	Coil Clamp	Loss of Position	Acceleration Vibrations	9	7	2	126
				Latch Sleeve	Torsion Stress	Askew Assembly	9	1	1	9
				Screws	Loss of Position	Loosening of Bolts	9	1	1	9
				-	Molten Coil	Wrong Heat Assumptions	9	5	2	90
				-	Degraded Coil	Exceeding Radiation	9	3	2	54
				-	Severed Coil	Acceleration Vibrations	9	5	3	135
				-	Amplified Vibration	Wrong Assembly	9	1	1	9
				-	Amplified Vibration	Material Yield	9	2	1	18
			Coil Clamp	Latch Sleeve	Torsion Stress	Askew Assembly	9	1	1	9
				Screws	Loss of Position	Loosening of Bolts	9	1	1	9
				-	Loose Coil	Acceleration Vibrations	9	1	1	9
				-	Amplified Vibration	Wrong Assembly	9	3	2	54
				-	Amplified Vibration	Material Yield	9	6	2	108
			Latch Sleeve	Melting Assay	Loss of Position	Loosening of Bolts	9	1	1	9
			Spring Tube	Spring	Loss of Compression	Material Yield	9	3	1	27
				Housing	Loss of Position	Improper Assembly	9	1	1	9
			Clamp	Keyway	Loss of Position	Loss of Preload	9	3	1	27

5.2. Discussion

By providing a thorough basis in risk identification, successive RM procedures can be more effective in evaluating the degree of vulnerability of system functions. Being aware of system failure modes, designers will be able to gauge whether design concepts are robust to undesirable conditions and whether they can still sustain function integrity. The purpose of FIDD is to facilitate risk identification to be systematic and comprehensive. This method focusses on providing structured diagnosis procedures and contextualising failure modes in formatted documentation.

One challenge in identifying failure modes is that in some novel designs there remain gaps in assumptions about system parameters and interactions. Without structured diagnosis designers might lack a premise to hypothesise how function integrity could be in jeopardy in any given design constellation. FIDD enables the designer to take advantage of an IF model and consider six design entities to contextualise system function. The designer can then make assumptions about how different system constellations and function characteristics could evolve into risk. The probability that the designer overlooks failure modes should be significantly reduced when applying systematic diagnosis.

An added benefit of FIDD is that it can be applied in conceptual design. Without any embodiment considerations (i.e. without a complete or detailed actor view), steps one through three (of the FIDD method) require no mention of explicit actors. By only analysing use-cases, transformation processes, and intended state changes, the review of abstract working concepts could provide insight into identifying anticipative failure modes. Such an analysis could be considered premature and excessive in effort as design concepts are certain to change due to design progression. However, the notion of identifying failure modes based on function models and their inherent abstract information already finds application in creating robust working solutions (Tumer and Stone, 2003).

Another consideration to be made when analysing system models is the issue in understanding the diagnosis limitations. The relevance of the FIDD results are inherently dependent on the accuracy and granularity of the IF model. If there are errors or gaps in the model, the sequential diagnosis could be incomplete and lack revealing details. Adding to this, there is also the need to be aware that FIDD is a model analysis. This implies that FIDD offers descriptive context but does not provide guidelines for the diagnosis of pure embodiment risks. Embodiment failure modes such as notches require the assumptions of the designer and highlights how this method cannot be algorithmically automated.

If aware of such limitations this methodology provides the means for comprehensive risk identification. With a detailed IF model the FIDD method will deliver large amounts of failure mode information. FIDD prescribes an FMEA template that facilitates distinctive description of each failure mode. While this checklist documentation might be unattractive as an analysis medium is has immediate advantages in organization. It includes reference and context of individual failure modes enabling traceability to the intended system function. This provides a comprehensive premise that allows a reviewing designer to understand the assumptions behind every failure mode and with increased system understanding could even evolve into additional risk identification.

It has not been determined how cumbersome identified failure mode redundancies can be to risk analysis or if there is a means to reduce repetition. However, it has been considered that entirety in risk identification is paramount compared to reducing failure mode redundancy. It is also the aim of the researchers to define the effectiveness of FIDD in order to compare effort and reward between the FIDD methodology and unstructured diagnosis.

6. Conclusion

State-of-the-art PD aims to ensure system robustness with improved designs and effective RM. This paper introduces a new method which offers significant preconditions for successful RM. FIDD supports the designer in risk identification by providing a premise for failure mode diagnosis and documentation. With structured diagnosis it reduces possible gaps in knowledge as the designer systematically traces system characteristics from system function to potential failure mode. The FIDD method also includes procedure to document and contextualize the found failure mode information which supports the designers system understanding. We hope that by applying this method designers can place more confidence in the overall integrity of their risk identification.

References

Andreasen, M.M. (1994), "Modelling—The Language of the Designer", *Journal of Engineering Design*, Vol. 5 No. 2, pp. 103–115. https://doi.org/10.1080/09544829408907876

Aven, T. (2016), "Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation", *European Journal of Operational Research*, Vol. 253 No. 1, pp. 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Bahr, N.J. (2014), *System Safety Engineering and Risk Assessment: A Practical Approach*, 2nd ed., CRC Press, Washington, D.C.

Bassler, D., Oehmen, J., Seering, W. and Ben-Daya, M. (2011), "A Comparison of the Integration of Risk Management Principles in Product Development", *Proceedings of ICED'11 / the 18th International Conference on Engineering Design, Copenhagen, Denmark, August 15-18, 2011*, pp. 306–316.

Chen, Y., Gillespie, A.M., Monaghan, M.W., Sampson, M.J. and Hodson, R.F. (2012), "On Component Reliability and System Reliability for Space Missions", *2012 IEEE International Reliability Physics Symposium (IRPS)*, IEEE, p. 4B.2.1-4B.2.8. https://doi.org/10.1109/IRPS.2012.6241831

Eisenbart, B. (2014), Supporting Interdisciplinary System Development Through Integrated Function Modelling, PhD thesis, University of Luxembourg.

Eisenbart, B., Gericke, K. and Blessing, L.T.M. (2013), "An Analysis of Functional Modeling Approaches Across Disciplines", *Artificial Intelligence for Engineering Design, Analysis and Manufacturing*, Vol. 27 No. 3, pp. 281–289. https://doi.org/10.1017/S0890060413000280

Eisenbart, B., Gericke, K. and Blessing, L.T.M. (2017), "Taking a look at the utilisation of function models in interdisciplinary design: insights from ten engineering companies", *Research in Engineering Design*, Vol. 28 No. 3, pp. 299–331. https://doi.org/10.1007/s00163-016-0242-3

Eisenbart, B., Gericke, K., Blessing, L.T.M. and McAloone, T.C. (2017), "A DSM-based framework for integrated function modelling: concept, application and evaluation", *Research in Engineering Design*, Vol. 28 No. 1, pp. 25–51. https://doi.org/10.1007/s00163-016-0228-1

Eppinger, S.D. and Browning, T.R. (2012), *Design Structure Matrix Methods and Applications*, MIT Press, Cambridge.

Eppinger, S.D. and Salminen, V. (2001), "Patterns of Product Development Interactions", *13th International Conference on Engineering Design, ICED 01*, pp. 283–290. https://doi.org/10.7492/IJAEC.2013.001

Gericke, K., Eckert, C.M. and Wynn, D.C. (2016), "Towards a framework of choices made during the life-cycle of process models", *Proceedings of the DESIGN 2016 / 14th International Design Conference, Dubrovnik, Croatia, May 16-19, 2016,* The Design Society, Glasgow, pp. 1275–1284.

Gluchshenko, O. (2012), Definitions of Disturbance, Resilience and Robustness in ATM Context, DLR Report IB 112-2012/28, Braunschweig.

Hirtz, J., Stone, R.B., McAdams, D.A., Szykman, S. and Wood, K.L. (2002), "A Functional Basis for Engineering Design: Reconciling and Evolving Previous Efforts", *Research in Engineering Design*, Vol. 13 No. 2, pp. 65–82. https://doi.org/10.1007/s00163-001-0008-3

Johnstone, S., Dainty, A. and Wilkinson, A. (2009), "Integrating products and services through life: an aerospace experience", *International Journal of Operations & Production Management*, Vol. 29 No. 5, pp. 520–538. https://doi.org/10.1108/01443570910953612

Karapetrovic, S. and Willborn, W. (2000), "Quality Assurance and Effectiveness of Audit Systems", *International Journal of Quality & Reliability Management*, Vol. 17 No. 6, pp. 679–703. https://doi.org/10.1108/02656710010315256

Kloss, B. and Moss, M.A. (2008), "How to measure the effectiveness of risk management in engineering design projects? Presentation of RMPASS: a new method for assessing risk management performance and the impact of knowledge management—including a few results", *Research in Engineering Design*, Vol. 19 No. 2–3, pp. 71–100. https://doi.org/10.1007/s00163-008-0049-y

Kurtoglu, T., Jensen, D.C. and Tumer, I.Y. (2010), "A Functional Failure Reasoning Methodology for Evaluation of Conceptual System Architectures", *Research in Engineering Design*, Vol. 21 No. 4, pp. 209-234. https://doi.org/10.1007/s00163-010-0086-1

Loch, C.H., Solt, M.E. and Bailey, E.M. (2007), "Diagnosing Unforeseeable Uncertainty in a New Venture", *Journal of Product Innovation Management*, Vol. 25 No. 1, pp. 28–46. https://doi.org/10.1111/j.1540-5885.2007.00281.x

Maarten Bonnema, G. and Van Houten, F.J.A.M. (2006), "Use of Models in Conceptual Design", *Journal of Engineering Design*, Vol. 17 No. 6, pp. 549–562. https://doi.org/10.1080/09544820600664994

McLoughlin, I.V., Gupta, V., Sandhu, G.S., Lim, S. and Bretschneider, T.R. (2003), "Fault tolerance through redundant COTS components for satellite processing applications", *Fourth International Conference on*

Information, Communications & Signal Processing Fourth IEEE Pacific-Rim Conference On Multimedia, *Vol. 1*, IEEE, Singapore, pp. 296–299. https://doi.org/10.1109/ICICS.2003.1292463
Moser, H.A. (2014), *Systems Engineering, Systems Thinking, and Learning*, Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-03895-7
Pahl, G., Beitz, W., Feldhusen, J. and Grote, K.-H. (2007), *Engineering Design: A Systematic Approach*, 3rd ed., Springer London, London. https://doi.org/10.1007/978-1-84628-319-2
Smith, P.G. and Merritt, G.M. (2002), *Proactive Risk Management: Controlling Uncertainty in Product Development*, 1st ed., Productivity Press, New York.
Tumer, I.Y. and Stone, R.B. (2003), "Mapping function to failure mode during component development", *Research in Engineering Design*, Vol. 14 No. 1, pp. 25–33. https://doi.org/10.1007/s00163-002-0024-y
Vermaas, P.E. (2011), "Accepting ambiguity of engineering functional descriptions", *Proceedings of ICED'11 / the 18th International Conference on Engineering Design, Copenhagen, Denmark, August 15-18, 2011*, pp. 10.
Vesely, W.E., Goldberg, F.F., Roberts, N.H. and Haasl, D.F. (1981), Fault Tree Handbook, Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC (USA).
Wertz, J.R. and Larson, W. (1999), Space Mission Analysis and Design, 3rd ed., Springer Netherlands.

Robert Lawrence Wichmann, Master of Science in Engineering
Swinburne University of Technology, Faculty of Health, Arts and Design
Im Krautgarten, 82216 Maisach, Germany
Email: wichmann.robert.rw@gmail.com