Failure modes and criticality analysis of the preliminary design phase of the Mars Desert Research Station considering human factors

[*1]Elif Oguz, [2]Martin Kubicek, [3]David Clelland

*[*1,3]Naval Architecture, Ocean and Maine Engineering, University of Strathclyde, Glasgow, Scotland*

[2]Mechanical and Aerospace Engineering, University of Strathclyde, Glasgow, Scotland

Abstract

This work presents an extension to the traditional FMECA (Failure Modes, Effects and Criticality Analysis) method to include the effects of human factors concerning accessibility/repairability, probability of contact and degree of contact. The authors refer to this extension to the traditional FMECA as the Human Design Approach (HDA). All data used in this study was collected during the stay of two of the authors at the Mars Desert Research Station (MDRS) in the Utah desert, USA. The MDRS is a laboratory for carrying out research in order to understand and investigate the difficulties of how to live and work on another planet. The results show that following the HDA can enhance the safety and reliability of the MDRS. There is still a significant amount of research required concerning reliability analysis of the space habitat in terms of the selection of optimum designs, the modification of systems, as well as access, inspection and maintenance strategies, human factors and environmental impacts. This preliminary study will assist the design engineers with the selection of an optimum configuration for space habitats and can be extended to any case where humans can influence function of an environment.

Keywords: FMECA Analysis, Reliability on Mars, Mars Desert Research Station, human factors.

1. Introduction

There has been growing body of literature that recognises the importance of reliability analysis for scientific and industrial processes. As systems became more complex designers became more aware of the problems associated with reliability. It was not until the development of the V1 and V2 rockets, when Robert Lusser recognized the need to approach reliability as a separate discipline (Woo (2017)). The complexity of these rocket missiles highlighted the importance of designing systems and configurations which have resistance to failure. This requires an understanding of uncertainty in systems and knowledge of the

possible failure modes of systems and subsystems. A number of studies introduced the concept of 'human factors' as part of the design process and the reliability analysis (Degani (1996)). Methods such as the abstraction hierarchy model, PROCRU and Finite State Machine (FSM) theory and its derivatives such as Petri-nets have proved to be helpful methodologies for including human interactions and effects into the design process.

Abstraction hierarchy was developed for the purpose of designing and troubleshooting process control systems such as flight controls. *It describes the functionality of a given system in a multi-level representation that can be depicted as a pyramid* (Rasmussen, (1985) and Rasmussen (1986)). The system objectives are at the top of the pyramid (e.g. autopilot). Descending from the top of the pyramid, each level becomes less abstract in specifying the process objectives (roll stabiliser). The bottom of the pyramid describes the actual physical component (aileron for example). *The abstraction hierarchy is a potentially useful model for understanding the relationships between the system's functional purpose and the modes of the system. However, the model is quite limited in identifying the behavioural aspects of the system that cause mode transitions and ambiguity* (Degani (1996)).

The Procedure Oriented Crew Model (PROCRU) is a computer based optimal control model, used to analyse flight crew procedures during landing approach. The model assumes the human operator as a rational controller who tries to optimize system performance. It is useful in identifying the contribution of information quality to the operator's decision making processes (Baron et al. 1980).

The Finite State Machine (FSM) theory tries to capture the behavioural aspect of a system. The combination of the theoretical and graphical format is quite appealing for representing human interaction with computer-based systems. Foley and Wallace (1974) used this notation to describe their concept of an interaction between the human and the computer. FSM models and their corresponding state transition diagrams can be used for design specification, coordination among design teams and for formal algorithmic checks for design errors. State transition diagrams generally cannot represent a hierarchical structure in an efficient and clear way. Hierarchy is a common characteristic in man-made systems and in this way we, as humans, understand complex systems.

Finite State Machine models and their various variants have considerable limitations in describing concurrent processes. Petri-Nets have the ability to model concurrency, as well as

the interaction between concurrent processes. The behavioural aspects of the model are denoted by the existence and dynamic assignment of tokens to different locations during net execution. Several modifications to the original Petri-Nets were developed to deal with some of their shortcomings. Coloured Petri-Nets use coloured tokens to indicate dedicated conditions. Coloured nets have been used for modelling the command post of a complex radar surveillance system, safety analyses, in particular, where potential faults are identified and modelled beforehand. (Johnson et al. 1995) used Petri-Nets to describe the sequence of events and decision making that contributed to an airline accident in 1990. *There are some concerns, however, that Petri-Nets, due to their lack of a hierarchical structure suffer some of the limitations of Finite State Machine models. One aspect which is not treated prominently in Net theory is the structural properties of systems composed from many interacting parts (Milner, 1989). In particular, given a complex system with many components and interactions among them, there is an explosion in the number of places and transitions, to the point they become unmanageable (Degani, (1996)).*

These methods have mostly been applied to electronic and computer control systems; however they can be used for many other systems. The different methodologies are reviewed in (Bell and Holroyd (2009)), which summarises the research on human reliability and also discusses the advantages and disadvantages of the various methods and approaches. Human factors and safety design relating to human interaction with computers and other electrical equipment is presented in (Leveson 2002).

Human reliability analysis (HRA) attempts to estimate the likelihood of human actions not being taken when required, or human actions that may cause hazardous events occurring. *HRA provides a logical comprehensive analysis of factors influencing human performance, leads to recommendations for improvement, supports the safety case, forces attention on safety critical tasks (Felice and Petrillo (2011)).*

Commonly used reliability analysis methods include (Hollnagel (1998)):

- *Probabilistic Safety Assessment (PSA), where the purpose is to identify the sources of risk in a system.*
- *Hazard Operability Studies (HAZOPS), where the purpose is to identify sources of failure.*
- *Failure Modes, Effects and Criticality Analysis (FMECA), where the purpose is to identify the degree of loss of activity objectives – as well as the recovery potential.*

The degree to which human action is included in the analysis varies for each method. FMECA (Failure Modes, Effects and Criticality Analysis) and HAZOPS (Hazard Operability Studies) are often carried out for the equipment without including the effects of human factors. PSA only identifies sources of risk and since the target systems usually involve human-machine interaction a consideration of human factors is required.

Human reliability analysis (HRA) takes a great deal of time, requiring significant input from experts, in order to collect useful human factors data (Connelly et al. (2012)). The inclusion of the effects of human factors is important where equipment and humans work in close proximity or where there is a strong interaction between human and machine. Ignoring these effects can reduce the confidence in the estimation of system performance, reliability and risk assessment. Well reported large-scale hazardous system accidents including Three Mile Island, Chernobyl and Bhopal showed the importance of human factors on system safety. As stated in Kirwan (1994), *current accident experience suggests that the so-called high-risk industries (and some so-called low-risk ones too) are still not particularly well-protected from human error.* The authors descibed the application of Human Reliability Assessment (HRA) as a means of *properly assessing the risks attributable to human error and for ways of reducing system vulnerability to human error impact.*

This paper describes a HRA applied to an earth based space habitat, the Mars Desert Research Station (MDRS), in order to identify risks, with the emphasis of human factors as well as providing information to designers in order to mitigate these risks at the design stage. The method extends the traditional FMECA, to include human factors, by including the Human Design Approach (HDA). HDA takes account of human factors which relate to accessibility/repairability and to the probability/degree of contact between human and machine. FMECA was selected since it employs a closed loop structure, shown in Figure 3, whereby risks can be identified and then reduced as an inherent part of the design process as well as the ease of integrating with HDA.

The MDRS, Figure 1, is an Earth-based research station, built in the Utah desert, which provides scientists and researchers an environment to investigate new and existing technologies, operations, and science in a simulated Martian environment.

Figure 1 View of the Mars Desert Research Station (MDRS), Utah, USA

A simulated inspection activity performed by the authors is shown in Figure 2.

Figure 2 Simulated inspection of the gas supply for the MDRS

Current FMECA methods do not consider the effects of human factors such as accessibility/repairability, probability of contact and degrees of contact which are important for manned space programs. Human factors have a large influence the reliability of space systems since any interaction between the human and the system has the potential to create a critical situation. Repairs or simple random interactions such as a tripping over improperly placed objects can lead to critical situations especially in closed environments such as the MDRS.

The two main objectives of this study is to extend the standard FMECA method to include the ideas of HDA namely:

- Human factors which relate to accessibility/repairability,
- Human factors which relate to the probability/degree of contact.

The procedures are illustrated by applying them to a critical system of the MDRS namely the electric generator. Since the possible failures and solutions, based on outcomes of this study, need to be further investigated, the authors cannot provide the absolute solution at this point. The goal of the study was to define a preliminary design methodology to decrease the criticality of the MDRS generator. There may be many solutions such as implementation of the reliability/criticality rank of the subsystem in the production, assessment of its integration capabilities, and assessment of its affordance, endurance, and suggestion of integration of design standard. Within the scope of this study the authors tried to present an alternative view on reliability regarding human sourced problems.

This paper is organised as follows. Section 2 provides a brief background of FMECA methods, applications and major shortfalls and explains the main steps required for carrying out FMECA including the methods outlined in the HDA extension. Following this, Section 3 presents a case study illustrating how the two methods can be applied to one of the critical systems of the MDRS. Finally, a brief summary of the main results from this work are provided in Section 4 and suggestions are made for future study.

2. FMECA background

The FMECA method was developed by the US Army; however, it was widely used during the 'space race' where the method was further developed by NASA for the Apollo missions which started in the 1960's (NASA (1966)). The FMECA concept developed for the Apollo missions still remains as one of the most commonly used methodologies. NASA's approach to risk analysis is summarised in (Cornel and Dillon (2001)). *"Rather than quantifying failure probabilities, the agency has generally preferred qualitative analyses such as Failure Mode and Effect Analysis (FMEA), Critical Item Lists (CILs), and Risk Matrices (Bowles (1998), Littlefield (1996), Onodera (1997)). FMEA/CIL relies on the logical identification of a system's weak points and of failure/event combinations (cut-sets) leading to its catastrophic failure. Risk matrices usually include, for different components or subsystems, qualitative information and corresponding scale indices about the likelihood of failure events (e.g. high, medium, or low) and the severity of their consequences (e.g. high, medium, or low). These matrices are often used as filters to decide which are the highest priority technical problems. A major difficulty when using risk matrices is to combine such information about the different components to characterize the robustness of the whole system."* Since the early Apollo

missions the FMECA method has gained in popularity and various modifications and extensions have been proposed.

FMECA is a reliability assessment/design technique which examines the potential failure modes within a system and its equipment, in order to determine the effects on equipment and system performance. FMECA consists of two different analyses, the Failure Mode and Effect Analysis (FMEA) and the Criticality Analysis (CA). As stated in Shirani and Demichela (2015) *"FMEA is a valuable tool in order to identify risks including those related to human factors".* Their findings showed the importance of human factors in terms of predicting major areas of risk. Since traditional analytical methods do not include human factors, methods such as FMEA, FMECA have steadily been gaining in importance in a number of fields. Using FMECA analysis, effects of each failure mode on system performance can be determined. This methodology provides data for identifying root failure causes and developing corrective actions.

After the successful application of FMEA by NASA during the Apollo, Viking, Voyager, Skylab missions, FMEA/FMECA was applied over a range of industries such as military, semiconductors, healthcare and food service during the 1970s. Shirani and Demichela (2015) applied a combination of FMEA and human factors to the entire supply chain of food production and they also presented their method by demonstrating a case study. It is stated in Tay and Lim (2006) that FMEA become a supportive tool for establishment of risk management policies. Felice and Petrillo (2011) presented a methodology which is based on FMECA and HRA to improve railway system reliability and railway transportation system.

Banghart et al. (2016) discussed some of the shortfalls of FMEA and possible approaches to reduce the effects due to bias and team dynamics, lack of validation and the subjective nature of estimating Risk Priority Numbers. In the paper the authors discuss methods to reducing expert bias/subjectivity including the application of a thorough review process, as well as a team-based approach. The authors report that *research-based validation of FMEA value and effectiveness is severely lacking, as are conclusive recommendations for improvement of the process, in terms of the human factor.* They also highlighted a number of studies (Konstandinidou et al. (2006), Shebl et al. (2009), Phipps et al. (2008), Apkon et al. (2004), Lyons et al. (2004)) where there were significant discrepancies between the severity ratings selected by different groups as well as the lack of correlation of risks identified.

The Risk Priority Number (RPN) in FMEA is a method aimed at ranking and prioritizing failure modes – in order to develop mitigation strategies and reduce the overall consequences of the failure mode occurring. Banghart et al. (2016) discusses a number of shortfalls of RPN including issues surrounding the combination of Severity (S) by probability of occurrence (O) and detectability (D) values:

- *Holes in the scale. The RPN scale is not continuous and various numbers between 1 and 1000 cannot be formed by the product of S, O and D. This is specifically evident in higher numbers (600+). Only 120 unique numbers can be formed with 88 % of the range empty.*

- *Duplication of RPNs. RPNs can be formed with many combinations of S, O and D thus making the inaccurate assumption that each factor is equally important.*

- *Sensitivity to small changes. The RPN can be affected significantly by a small change in one factor, especially if the other factors are large numbers.*

- *Utilizing a single dimension RP encourages management to set arbitrary unrealistic thresholds (Bowles (2003)).*

Basic guidelines for the FMECA study are outlined in the Military procedure - *Procedure for Performing a Failure Mode, Effects and Criticality Analysis* (MIL-STD-1629A). Since FMECA provides important information for maintainability, safety and logistics analysis, researchers have also used the method to enhance the quality of existing systems.

The main steps involved with FMECA are shown in Figure 3.

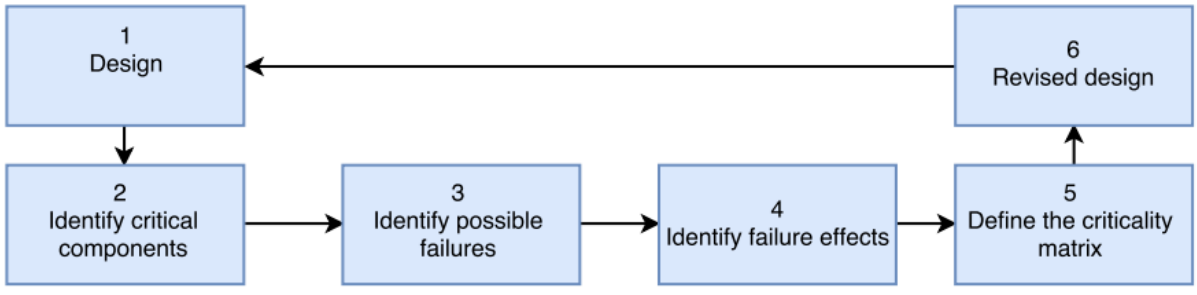

Figure 3 Main steps of traditional FMECA

Kmenta (2002) described the FMECA process as a number of district phases. The different phases, the necessary questions for these phases and the outputs of each phase, are illustrated in Table 1.

Table 1 FMECA Phases adopted from (Kmenta, 2002)

Phase	Question	Output	FMECA step (Figure 3)
Identify	What can go wrong?	Failure descriptions Causes Failure Modes Effects	2,3,4
Analyse	How likely is a failure? What are the consequences?	Failure rates RPN=Risk Priority Number	5
Act	What can be done? How can we eliminate the cause? How can we reduce the severity?	Design solutions Test plans Manufacturing changes Error proofing, etc.	6

The necessary steps for carrying out FMECA analysis are shown in Table 2. The extended human factor considerations such as accessibility and human machine interactions not included in the traditional approach are highlighted.

Table 2 FMECA and HDA Steps

Main Steps	Sub steps	Description
1. System selection and analysis level.	System selection	The selection is based on data availability,expert judgement and the importance of system/subsystem to future development.
	Establishing level of analysis	System/subsystems can be divided into smaller parts e.g. radio to speaker, electric main board, power supply etc.
2. Gathering information about targeted systems	Functional analysis	Gathering information about functionality of each system and subsystem
	Possible failure modes	Identification of the failure modes of each system and subsystem
	Connections to other systems	Establish the connections and interactions and dependences between systems and subsystems. Each system is analysed as a separate part and also, as a part of a larger system
	Assembly logic of systems	The assembly approach (how each subsystem is assembled into a system) can change the criticality of system. This information is necessary as part of the human factor assessment
	Obtaining human factor modifiers	A series of factors describing accessibility/repairability and human interaction with the system/subsystem are established
3. Gathering information about environmental conditions	Environmental conditions	Each system and subsystem is required to operate over rage of different environmental conditions such as vibration, temperature, humidity, pressure etc. Operating within prescribed conditions is vital for functionality of the given system
	Running time	Predict the operational time requirements for the each system and subsystem based on previous related research combined with expert knowledge
4. Criticality assessment	Identification of failures and consequences	An assessment of failure modes and consequences of failure e.g. catastrophic, critical, marginal or minor is carried out for each system and subsystem
	Probability of system failure	Probability of failure is determined for each system/subsystem based on literature [6, 8, and 9] and expert knowledge
5. Assessment of system modification, accessibility and human interaction	Modification assessment	Systems and subsystems are interconnected. Design changes must be assessed to determine if changes in one subsystem lead to fundamental changes in the functionality of the system.
	Repairability	The effect of design changes on aspects of repairability in particular accessibility must be assessed
	Human interaction	The effect of design changes on aspects of human interaction must be assessed e.g. how the design/modification influence human behaviour and vice versa.
6. Modifying criticality assessment to include human factors	Determining the probability of system failure with human interaction	Consideration of the modification of probability of failures based on different human interactions. This includes modification of criticality of system based on human interaction.

3. Case study – MDRS Electric Generator

3.1 Developed Methodology

In this paper, the standard FMECA method is extended to include the effect of human behaviour on the design process by applying a Human Design Approach (HDA). The easy to implement approach provides an estimate of the probability of failure due to human interaction by combining both the probability and the degrees of contact as well as reflecting the accessibility degree of a given part i.e. how easy it is for a human to access part of a system. In a similar manner to evaluating risk priority numbers (RPN) in the standard FMEA (Failure mode effects analysis) the

HDA also requires subjective input from experts in order to quantify the various probabilities which is a well-known weakness of such methods.

In order to improve the reliability of the MDRS electric generator possible failures caused by human interactions were investigated. This study demonstrated the importance of including the effects of human interactions on the MDRS system components using an extended FMECA analysis.

It would be interesting to extend the work by including, for example, more human interactions and greater subsystem detail in order to investigate the efficacy of the relatively crude model used in this study as well as investigating the effects of applying reported methods in order to reduce subjectivity.

Failure modes, probabilities of failure occurrence and accessibility degrees of the selected MDRS systems are presented in this section. Since almost everything on MDRS requires electrical power, the generator set is selected as the most important system. This study includes only sub-assemblies since there was no data available for a deeper analysis at individual component level. The main sub-assemblies of the electric generator are the diesel engine, exhaust and starting battery shown in Figure 4.

Figure 4 MDRS Generator

3.2 Failure occurrence and failure modes

The probabilities of failure occurrence and failure modes are based on the approaches outlined in (MIL-STD-1629A, (1980), MIL-HDBK-217F, (1990), FMD-91, (1991)). The probability of failure occurrence levels is shown in Table 3.

Table 3 Probability of failure occurrence levels (frequency) (FMECA, 1993)

Level	Frequency

A	Frequent
B	Resonably probable
C	Occasional
D	Remote
E	Extremely Unlikely

3.3 Accessibility

The accessibility degree of a given part, i.e. how easy it is for a human to access the part with a given failure mode, is divided into four classifications shown in Table 4. Accessibility is closely linked to repairability.

Table 4 Accessibility degree classification

Accessibility Degree	Accessibility
1	Completely accessible
2	Accessible with minor difficulties
3	Accessible with major difficulties
4	Completely inaccessible

The authors propose four classifications to represent accessibility. The first classification represents failure modes on parts which are completely accessible. This means that the selected failure mode of the part can be easily accessed and repaired with tools or easily replaced with a new part. This often represents parts which are usually outside of the given machine. Typical examples would be batteries in a remote control or battery in a personal laptop, where the failure mode would be shorted battery or old battery.

The second classification represents failure modes where the access is difficult or the failure mode of given part means it is not easily repairable. An example could be the failure of a glow plug in the generator engine as changing the plug may be problematic due to constricted access as shown in Table 5.

The third classification represents a failure mode where access is very difficult or special tools are required to replace/repair the part. An example could include failure of the electrical starter motor of a combustion engine requiring replacing the starter or one of its components. A typical location for the starter would be behind the battery as it is seen in Figure 4. The replacement of the starter requires removing the battery and then removing the starter. The process is problematic due to the severely restricted space as well as interference from

numerous electric cables. This demonstrates a double point failure as the repairperson can make a mistake in removing battery or starter causing other damage to the system.

The last classification represents a failure mode where repair or replacement is not possible. An example failure mode would be a piston crack inside the combustion engine. In order to replace the piston, it is necessary to dismantle the whole engine and replace the piston. This represents a multiple point failure as the repair person has to dismantle other parts of engine and each part has possible failure in itself. Inaccessibility problems also occur due to poorly placed fasteners which cannot be accessed and are required to be untied in order to replace the part. Problems can be introduced by the assembly process carried out during manufacturing such as where the machine is assembled and then a protective cover is welded over it. After the welding process, the machine becomes a single failure problem as one failure is enough to lead to the replacement of the whole machine.

3.3.1 Accessibility matrix

Once failure modes and occurrence levels (from traditional FMECA), and accessibility (from HDA) are established, the 'accessibility matrix' can be constructed for each sub-assembly of the MDRS generator as shown in Table 6.

Table 5 Failure modes, failure occurrences and accessibilities of the MDRS generator

	FMECA			HDA	
	Part	**Label**	**Failure mode**	**Probability of failure occurrence**	**Accessibility degree**
GENERATOR	**ENGINE**	GEN_E1	Mechanical	D	4
		GEN_E2	Loss of Control	D	2
		GEN_E3	Cooling System	C	3
		GEN_E4	Air and Fuel System	C	3
		GEN_E5	Electrical	D	2
		GEN_E6	Seal/Gasket	C	4
		GEN_E7	Lubricating System	D	4
	EXHAUST	GEN_X1	Gasket Leak	B	3
		GEN_X2	Burst/Ruptured	B	3
		GEN_X3	Incorrect Fitting	D	3
	BATTERY	GEN_B1	Degraded Output	C	1
		GEN_B2	Worn	C	1
		GEN_B3	No Output	D	1
		GEN_B4	Connector	D	1
		GEN_B5	Short circuit	D	1
		GEN_B6	Leaking	E	1

Table 5 indicates that most inaccessible parts are in the diesel engine (GEN_E1, GEN_E6 and GEN_E7) showing that the current design is not suitable for carrying out repairs due to poor accessibility. If there is a failure of the engine, the process of repairs could be very problematic. Repairs to the exhaust system could also be problematic due to the relatively poor accessibility. On the other hand, it can be clearly seen that the battery is easily accessible. Table 6 shows the probability of failure occurrence (from FMECA) in relation to accessibility (from HDA). The table highlights problematic parts by combining accessibility and failure occurrence levels.

Table 6 Failure occurrence and Accessibility

Probability of failure occurence	**Label**			
A				
B			**GEN_X1 GEN_X2**	
C	GEN_B1 GEN_B2		GEN_E3 GEN_E4	**GEN_E6**
D	GEN_B3 GEN_B4 GEN_B5	GEN_E5 GEN_E2	GEN_X3	**GEN_E1 GEN_E7**
E	GEN_B6			
Accessibility	1	2	3	4

The authors observed that the rather coarse accessibility scale (1 to 4) is capable of catching all the major issues relating to MDRS generator design. Nevertheless Table 6 shows that of the three most inaccessible parts, mechanical failure and engine lubricating system (GEN_E1 and GEN_E7) have only remote failure occurrence levels while (GEN_E6) seals/gasket fail occasionally.

Highest failure rates occur for exhaust parts (GEN_X1 and GEN_X2) which have relatively poor accessibility. There are no parts of the generator where there is high probability of failure combined with no access.

3.4 Probability and Degrees of contact

The second aspect of the HDA concerns degrees and probability of contact which describes the probability of a human interacting with a part. The first step is to define how each part can be in contact with human operator (degrees of contact). It is clear that a part or unit which is hidden behind a cover is less likely to come into contact with a human than a part which is

in the open. For each degree of contact there is associated probability of contact as illustrated in Table 7 which is based on Risk Management Probability Definitions relating to probability of occurrence. These probabilities are defined over the predicted life time of given part (Engert and Lansdowne (1999)).

Table 7 Probabilities and degrees of contacts (Engert and Lansdowne (1999))

Degrees of contact	Probability of contact	Description
1	0.00 - 0.10	Almost impossible to interact with human
2	0.11 - 0.40	Unlikely that human can be interact with part
3	0.41 - 0.60	It is likely that human can be interact with part
4	0.61 - 0.90	Highly probable that human can be interact with part
5	0.91 - 1.00	Almost certain that part can be interact with human

The first degree of contact represents a part behind a cover or some sort of protection. This could be a button behind a glass, where it is necessary to break the glass to touch the button or a battery which is completely enclosed by a cover. It should be noted that the cover needs to be handled first in order to get into the battery. The reader should bear in mind that there is still some minimal probability that human can interact with the part. Even when a part is behind a protective cover there is still possibility of damage due to human interaction, e.g. impact with heavy object during transportation.

The second degree of contact represents a part which can be directly accessed by a human, but it is still well covered by the environment. An example would be a control panel. The third degree represents an object which is partly covered but allows possible interaction with a human such as the exhaust. The fourth degree of contact represents an object which lies in path of the human, but it is clearly visible, i.e. the object is in visual range, or the human is constantly aware of the object. The last degree represents a part where there is a high probability of human interaction.

3.5 Failure modes due to human interaction

This section describes two basic failure modes due to human interaction. The first mode accounts for failures due to accidental human interaction such as a cup of coffee spilled on a keyboard. The second failure mode accounts for failures due to improper human operation such as using excessive force on a part and breaking it. This also includes, improper “playing” or ‘fiddling’ such as described in (Finch and Cameron (1955)) with a part: humans have a tendency “to play” with parts which are freely accessible. An example is the

accidental damage (mode 1) to the fire extinguisher bracket shown in Figure 5 caused by a worker improperly leaning on it (mode 2) while talking to a co-worker.

Figure 5 Damaged fire extinguisher bracket on the MDRS

In the frame of this study, accidental interaction and improper manipulation are considered as human factors each of which has an associated probability of appearance. The probability of appearance, a subjective value obtained from expert opinion, is the probability that a particular human factor will occur in a subsystem. It is important to note that since the sum of probabilities of appearance for each sub-system is one, adding more human factors tends to reduce the probability of appearance of a particular human factor.

Here the authors define the probability of accident which is the product of probability of appearance and probability of contact as shown in equation (1).

$$P_{accident}=P_{contact}*P_{appearance} \quad (1)$$

Table 8 shows the generator subsystems and the human factors relating to each subsystem. It also shows how the probability of accident is determined for each human factor. The mid-range of the probability of contact values in Table 7 were combined with probability of appearance values in order to calculate the probability of accident for each human factor in the subsystem.

Table 8 Results for human interactions with the generator

Sub System	Label	Human factor	Type of damage	Probability of appearance	Degree of contact	Probability of contact	Probability of accident	Degree of severity
ENGINE	HEN1	Accidental interaction - cover damaged	Mechanical damage	0.389	4	0.7	**0.272**	1
	HEN2	Accidental interaction - damage to fuel box	Mechanical damage	0.389	4	0.7	**0.272**	3
	HEN3	Improper operation - impact due to transportation	Mechanical damage	0.111	4	0.7	**0.078**	4
	HEN4	Accidental interaction – electric cables and fuel pipes.	Mechanical damage	0.056	4	0.7	**0.039**	3
	HEN5	Improper operation - control panel damaged and inoperable	Mechanical and Electrical damage	0.056	4	0.7	**0.039**	4
EXHAUST	HEP1	Accidental interaction - silencer damage due to impact	Mechanical damage	0.273	3	0.45	**0.123**	2
	HEP2	Accidental interaction- silencer loss due to impact	Mechanical damage	0.136	3	0.45	**0.061**	3
	HEP3	Accidental interaction - pipe damage due to impact causes gas leakage	Mechanical damage	0.364	3	0.45	**0.164**	2
	HEP4	Accidental interaction - pipe damage due to impact - hole and gas leakage	Mechanical damage	0.227	3	0.45	**0.102**	3
BATTERY	HBA1	Improper operation - battery shorted	Electrical damage	0.262	5	0.95	**0.249**	4
	HBA2	Improper operation - terminal damage	Electrical damage	0.033	5	0.95	**0.031**	3
	HBA3	Accidental interaction - battery loss due to impact	Mechanical damage	0.164	5	0.95	**0.156**	4
	HBA4	Accidental interaction - battery leakage of acid	Mechanical damage	0.230	5	0.95	**0.219**	4
	HBA5	Accidental interaction - terminal damage due to human.	Mechanical damage	0.311	5	0.95	**0.295**	3
BATTERY CABLE	HBAc1	Accidental interaction - cable break	Mechanical damage	0.360	5	0.95	**0.342**	4
	HBAc2	Accidental interaction - cable damaged	Mechanical damage	0.520	5	0.95	**0.494**	4
	HBAc3	Improper manipulation - cable is damaged	Mechanical damage	0.120	5	0.95	**0.114**	4

The degree of severity is shown in Table 9.

Table 9 Severity Levels (FMECA, 1993)

Level	Severity
1	Catastrophic
2	Critical
3	Marginal
4	Minor

The relationship between the percentage probability of accident (from HDA) and the degree of severity (from FMECA) is shown in Table 10.

Table 10 Probability of accident and severity

Probability of accident (%)	**Label**			
50				HBAc2, HBAc1
30			HBA5	HBA4, HBA1
20		HEP3, HEP1	HEP4, HEN2, HEN1	HBAc3, HBA3
10			HBA2,HEP2,HEN4	HEN5,HEN3
Severity	1	2	3	4

Table 10 shows that the probability of interaction with the battery and cables is high but the severity is relatively low. The table also indicates that accidental interaction causing silencer damage due to impact (HEP1) and accidental interaction causing pipe damage and leakage of gas (HEP3) are the most severe human interaction conditions. It is worth noting that the results of the accessibility study in Section 3.3.1 also concluded that the exhaust was problematic, having the highest failure rates combined with relatively poor accessibility.

4. Discussion

This paper describes an easy to implement method named the Human Design Approach (HDA) which is an extension to the traditional FMECA method. HDA considers human factors concerning accessibility as well as human-machine interactions described by probability of contact.

The first part of HDA allows the relationship between accessibility (HDA) and probability of failure occurrence (FMECA) to be investigated which the authors titled ‘the accessibility matrix’. This can be used to highlight problematic parts which may have relatively high failure occurrence combined with poor accessibility. This has major consequences of repairability and may also indicate that design changes are required.

The second part of HDA allows the relationship between probability of accident (HDA) and severity (FMECA) to be established. The authors introduce the term probability of accident which is found by combining probability of appearance (FMECA) with probability of contact (HDA). This can be used to highlight parts which may have relatively high probability of

accident combined with high severity. Such parts will have a detrimental effect on overall reliability and will require to be redesigned.

The HDA approach was applied to a critical system on the Mars Desert Research Station (MDRS) namely the electric generator. The number of human interactions was limited to five, the machine subsystem level was just one, giving a relatively crude model and the generator used in an actual mission would be quite different from the one used in this study. Furthermore, due to the unique nature of the MDRS a degree of subjectivity was required in selecting probability values. Nevertheless the results from both HDA studies highlighted that the exhaust system was a critical component of the generator system in terms of reliability. This indicated that the 'space ready' generator would require a different approach to the exhaust design.

The overall design purpose of the MDRS is to provide a safe and reliable environment for astronauts. High reliability is critical for space systems due to the severity of the environment experience by both users and systems and the limited repair and reconfiguration options available during an actual mission. The FMECA approach combined with the HDA provides a closed loop system whereby risks (including those due to human factors) can be identified and then mitigated during the design process.

One of the main advantages of the FMECA/HDA method is that it combines a relatively well understood method for assessing reliability with a relatively easy to implement extension dealing with human interaction which allows probematic parts to be easily identified at the design stage.

Acknowledgement

Authors also would like to thank the rest of the team members; commander Ondrej Doule, green hab officer Lucie Poulet, journalist Tereza Pultorava, Health officer Filip Koubek. The authors acknowledge the support of NASA Ames and Mars Society to this work.

References

Apkon, M., Probst, L., Leonard, J., DeLizio, L., Vitale, R. (2004). Design of a safer approach to intravenous drug infusions: failure mode effects analysis. *Quality and Safety in Healthcare,* Vol.13, pp. 265-271.

Banghart, M., Babski-Reeves, K., Bian, L. (2016). Human Induced Variability during Failure Mode Effects Analysis (FMEA). *Reliability and Maintainability Symposium (RAMS), 25-28 Jan 2016.* DOI. 10.1109/RAMS.2016.7448000.

Baron, S., Muralidharan, R., Lancralt, R., Zacharias, G. (1980). "PROCRU: A model for analysing flight crew procedures in approach to landing". *NASA Contractor Report, 152397*. Moffett Field, CA: NASA Ames Research Center.

Bell J. and Holroyd J. (2009). Review of human reliability assessment methods. *Health and Safety Laboratory Research Report, RR679.* Hill Buxton, Derbyshire, SK17 9JN.

Bowles, J.B. (1998). The New SAE FMECA Standard. *Proceedings of the Annual Reliability and Maintainability Symposium.*

Bowles, J.B. (2003). An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis. *Proceedings of the Annual Reliability and Maintainability Symposium.*

Cornel, E.P., Dillon, R. (2001). Probabilistic risk analysis for the NASA space shuttle: a brief history and current work. *Reliability Engineering and System Safety,* 74, pp. 345-352.

Cornelly, S., Hussey, A., Becht, H. (2012). Practical Early-Lifecycle Application of Human Factors Assessment. *Proceedings of the Australian System Safety Conference,* Vol.145, pages: 47-54 (ASSC 2012).

Degani, A., (1996). Modeling Human-Machine Systems: On modes, error, and patterns of interaction. *School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, GA.*

Engert, P.E., Lansdowne, Z.F. (1999). Risk Matrix User's Guide, Version 2.2. *The MITRE Corporation, Bedford, Massachusetts.*

Felice, F.B. and Petrillo, A. (2011). Methodological Approach for Performing Human Reliability and Error Analysis in Railway Transportation System. *International Journal of Engineering and Technology,* Vol.3 (5), pp.241-253.

Finch, G., Cameron, F. (1955). Air Force Human Engineering, Personnel, and Training Research. *National Academy of Sciences, National Research Council.*

FMD-91(1991). Failure Mode/Mechanism Distributions. *Reliability and Defence Information Analysis Center.*

FMECA (1993). Failure Mode, Effects, and Criticality Analysis (FMECA). *Reliability Analysis Center, CRTA-FMECA.*

Foley, J. D., and Wallace, V. L. (1974).The art of natural graphic man-machine conversation. *Proceedings of the IEEE*, 62(4), 462-471.

Hollnagel, E. (1998). Cognitive Reliability and Error Analysis Method, Elsevier Science Ltd.

Johnson, C. W., McCarthy, J.C., Wright, P.C. (1995). Using a formal language to support natural language accident report. *Ergonomics,* 38(6), 1264-1282.

Kirwan, B. (1994). A Guide to Practical Human Reliability Analysis. *Taylor and Francis.*

Kmenta S., 2002. Scenario-based FMEA Using Expected Cost – A new Perspective on Evaluating Risk in FMEA.

Konstandinidou, M., Nivolianitou, Z., Kiranoudis, C., Markatos, N. (2006). A Fuzzy Modeling Application of CREAM Methodology for Human Reliability Analysis. *Reliability Engineering and System Safety,* Vol. 91, pp. 706-716.

Leveson N. G., 2002. System Safety Engineering: Back to the Future. *MIT: Aeronautics and Astronautics, Boston.*

Littlefield, M.L. (1996). FMEA/CIL Implementation for the Space Shuttle New Turbopumps. *Proceedings of the Annual Reliability and Maintainability Symposium.*

Lyons, M., Adams, S., Woloshynowych, M., Vincent, C. (2004). Human reliability analysis in healthcare: A review of techniques. *International Journal of Risk and Safety in Medicine,* Vol.16, pp.223-237.

MIL-HDBK-217F (1990). Military Handbook Reliability Prediction of Electronic Equipment. *Department of Defence Washington DC 20301*.

MIL-STD-1629A (1980). Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis. *United States Department of Defence*.

Milner, R. (1989). Communication and concurrency. *New York: Prentice Hall.*

NASA (1966). Procedure for Failure Mode, Effects and Criticality Analysis (FMECA). National Aeronautics and Space Administration. RA–006–013–1A. *Retrieved 2010-03-13. (NASA release for Apollo mission).*

Onodera, K. (1997). Effective Techniques of FMEA at Each Life-Cycle Stage. *Proceedings of the Annual Reliability and Maintainability Symposium.*

Phipps, D., Meakin, G.H., Beatty, P.C., Nsoedo, C., Parker, D. (2008). "Human factors in anaesthetic practice: Insights from task analysis." *British Journal of Anaesthesia,* Vol. 100, pp.333-343.

Rasmussen, J. (1985). The role of hierarchical knowledge representation in decision making and system management. *IEEE Transactions on Systems, Man, and Cybernetics*, *SMC-15*, 234-243.

Rasmussen, J. (1986). Information processing and human machine interaction: An approach to cognitive engineering. *New York: Elsevier.*

Shebl, N.A., Franklin, B.D., Barber, N. (2009). Is failure mode and effect analysis reliable? *Journal of Patient Safety,* Vol.5, pp. 86-94.

Shirani, M. and Demichela, M. (2015). Integration of FMEA and Human Factor in the Food Chain Risk Assessment. World Academy of Science, Engineering and Technology *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering,* Vol.9, No.12, pp.4216-4219.

Tay, K.M. and Lim, C.P. (2006). Fuzzy FMEA with A Guided Rules Reduction System for Prioritization of Failures, *International Journal of Quality & Reliability Management,* pp. 1047-1066.

Woo, S. (2017). Reliability Design of Mechanical Systems: A Guide for Mechanical and Civil Engineers, *Springer International Publishing.*