An FMECA Approach to Unmanned Vehicle Maintenance Optimization

Paul T. Dube **Jerry L. Thibodeaux**
Naval Undersea Warfare Center, Division Newport
1176 Howell St. Newport RI, 02841
UNITED STATES OF AMERICA

Paul.Dube@navy.mil Jerry.Thibodeaux@navy.mil

Keywords: Functional FMECA, Physical FMECA, NAVSEA, Health Monitoring, Predictive Engineering

ABSTRACT

All Unmanned Vehicles (UxVs) have a multitude of missions they are expected to support. Each mission requires both common and unique functions from the vehicle. There are however no single set of mission critical tasks that can be used for all vehicle designs. Some missions will be long in duration, measured in weeks or months, while others will be shorter, and measured in hours. As such, the maintenance strategy of any UxV needs to align closely with the level of reliability needed from the mission critical components used in these systems. As UxVs move towards more autonomous capabilities, the vehicle will be required to autonomously respond to failures that occur within mission critical functions, otherwise the data, the vehicle, and the mission will be compromised. To achieve this capability, NUWC recommends the use of the combination of a functional and a physical Failure Modes Effects and Criticality Analysis (FMECA) process to enhance the development of UxV autonomy and maintenance strategies. This FMECA combination process provides an orderly means of defining and ranking all potential functional and component failure modes. Properly addressing each defined failure mode will ensure that the vehicle will respond properly to those failures that are most critical to mission success. The FMECA will inform the design of health monitoring (i.e. Built-in-Test) requirements needed to properly schedule both preventive and corrective maintenance actions.

1.0 INTRODUCTION

Proper maintenance of UxVs requires both early planning during the design phase as well as continuous monitoring of the components during operations. Through these actions, sustainment of the vehicles over their life expectancy is achieved. During the design phase, a functional and physical FMECA is used to inform the design of the vehicle's health monitoring system and autonomous functions that will allow the vehicle to properly respond to failures occurring during operation. The FMECA is used to optimize the design of reliability centered maintenance (RCM) used for preventive maintenance and condition based maintenance plus (CBM+) used for corrective maintenance planning and support. During Operations, the health monitoring system will inform updates to both RCM and CBM+ actions. This paper will discuss the FMECA and how it is performed. The paper will address how the FMECA is used to design a health monitoring system in support of continued uninterrupted operations.

1.1 Unmanned Vehicle Design

UxVs are being designed today in various sizes and shapes to support specific needs. Within the Naval Sea Systems Command (NAVSEA), we define those needs in terms of the UxV's intended mission(s). In general, a typical mission may involve sea floor mapping, contact identification, electronic surveillance, or recovery operations. Various mission purposes require a vehicle design to contain different sets of sensors and mechanical features in order to ensure that the mission is successfully accomplished. In some cases, when complex tasks are required, multiple UxVs may be required simply because designing one vehicle to support several tasks will result in an increase in design complexity and more opportunities for failure to occur.

The design of UxVs today are moving in several technological directions. For example, some vehicles may be battery powered and driven by electric motors, while others may be diesel powered and driven by combustion engines. Different technologies may also be used for UxV positioning such as Global Positioning Systems (GPS), or internal gyros. Different technologies require different sets of mechanical features and components in order to operate. Also, each function that an UxV may be designed to perform may consist of existing or new technologies. Therefore, because of these variabilities in system design, no one set of common mission critical components can be defined. Hence, each UxV design will require reliability engineers to analyse the operational mission profile for each type of task required at each phase of operation and determine which function(s) and components are critical to executing those tasks.

1.2 UxV Health Monitoring

In order to monitor the health of an UxV, the system must contain sensors capable of monitoring the physical state of those critical components for failure or potential failure. Another method of monitoring when failures are occurring is to analyse existing data sources built into the components. In order to fully understand the impact of failures when they are occurring, is to ensure that the design of health monitoring systems are capable of isolating failures to a specific failure mode within critical components. If failures are occurring in components that are necessary for critical functions, such as controlling the vehicle, data collection, or propulsion, then the UxV must have the autonomous programming that can direct specific actions needed to react to those failures such as signalling operators for direction on how to proceed with the mission or aborting the mission entirely. Because of the limitations in the overall size of UxVs, and the various technologies being used to design the UxVs, health monitoring systems must compete for the limited space and weight within the vehicle. Since successful performance of the UxV's mission is the intent of the design, any health monitoring systems must compete for space and weight budget after critical technologies are incorporated. To optimize the overall footprint of on board health monitoring systems, a design tool is needed to assist designers with the critical decisions of which components and systems require monitoring and how health monitoring will be performed. A Failure Modes Effects and Criticality Analysis (FMECA) provides such a tool to allow engineers to identify each and every failure mode within the vehicle and then prioritize them for decision making. It is important to understand that a FMECA must be performed early in the design phase in order to inform the designers in a timely fashion to ensure an optimum solution to the size and footprint of health monitoring systems.

1.3 The Value of a FMECA

A FMECA is the process of defining each component within a system and identifying all potential failure modes that those components may experience. A FMECA can be accomplished in many ways, however it is important to understand what the FMECA must inform in order to support the vehicle design. A FMECA must inform the system's autonomy design such that the vehicle is capable of responding appropriately to any occurring failure. Some failures may require little to no action during a mission other than recording that a failure has occurred. Other failures may require a deviation of the mission objectives. A worst case scenario is a complete abortion of the mission requiring the initiation of actions necessary for the vehicle to return safely to a location for retrieval and repair. Besides informing the system's autonomy design, a FMECA must also inform engineers in the design of the health monitoring system's such that the proper failure modes are detectable to support system autonomy as well as direct maintenance activities once the UxV has returned to a position where maintenance is available. A FMECA is also used during initial design to inform the reliability centered maintenance process used by NAVSEA to develop and manage the fleet's preventive maintenance tasking. The intent of reliability centered maintenance is to formulate failure management strategies that allow assets to continue operating at the desired level of performance. After fielding, a health monitoring system will provide updates to the reliability centered maintenance process and improve preventive maintenance tasking. This is accomplished by optimizing activities necessary to prolong the life and reliability of the components. Besides informing the reliability centered maintenance process, a FMECA is used during design to inform the Condition Based Maintenance plus (CBM+) process also used by NAVSEA. CBM+ is the process of using

health-monitoring systems to inform what corrective maintenance is required and to expedite repairs. This is accomplished by pre-ordering repair parts, or planning overhaul actions prior to the vehicle returning to a maintenance activity for repairs. The health monitoring system can automatically inform maintenance activities as soon as failures occur thus expediting and optimizing the maintenance process.

As discussed above, the FMECA process must identify mission critical, safety critical and data critical failure modes to allow decisions to be made in the design of autonomy, health monitoring, reliability centered maintenance and condition based maintenance. Through the FMECA process, engineers can determine if a failure mode is detectable, or can be made detectable, and if the method of detection will isolate the failure to one or several other components in the system. If existing data sources cannot be used to detect the most critical failure modes, sensors may be required. In some cases detection of some critical failure modes may not be possible, or performance monitoring systems may not be able to isolate failures down to a single component. The FMECA will allow systematic identification, isolation and decision making surrounding the most critical aspects of the UxV design and will provide a holistic approach that engineers can use to properly design both autonomy and health monitoring systems as well as inform maintenance operators such that the UxV can be returned to service as quickly as possible.

1.3.1 FMECA Timing

Many programs have problems completing a physical FMECA in time to support the design of autonomy and health monitoring systems. These programs will instead use a FMECA to identify shortfalls in a system design once the design has been completed. The reasons for this is typically because of the difficulty of identifying all of the components needed in the design before completion and the amount of time it will take to complete the FMECA analysis. To ensure the full benefit of the FMECA process, a stepped approach to completing the FMECA is necessary. Engineers should first perform a functional FMECA followed by a physical FMECA. A functional FMECA should be completed when the functional baseline has been struck and a physical FMECA completed when all hardware and components have been identified. Normally a functional baseline identifies all functions that the UxV must perform and is completed well before the physical baseline can be struck. A functional FMECA will identify all functions within a system and score them appropriately to identify which functions are the most critical to pursue during the physical FMECA. This can expedite the physical FMECA by eliminating those functions which may be lower in criticality in terms of the overall mission objective. Normally all functions are identified early in the design phase such as propulsion, energy, steering, ballast, data analysis, data collection, handling and storage, heating and/or cooling, mission specific functions such as laser controls, or mechanical functions such as robotic arms or antennas for communication. Sometimes alternative technologies will be considered to support specific functions. For example, energy alternatives may be under consideration such as battery power or fuel power. Alternatives under investigation should be identified in the functional FMECA stage to allow engineers to consider how they will affect the physical FMECA. Using this technique, engineers can identify the hardware typically needed to support both alternatives and begin assessing the failure modes typically seen long before the actual components are chosen. This approach will allow engineers to determine if typical failure modes are sufficient for the completed functional FMECA or if the specific hardware should first be identified and analysed as part of the physical FMECA. A typical representation of a functional FMECA is shown in Figure 1 below. The functional FMECA allows the engineering team to identify and prioritize functions needed to ensure the successful completion of the design and physical baseline in time to support the analysis.

		Design Fixed?	Technology Solution(S)	Sub-Function(s)	Failure Mode	Mission Critical	FULL/PARTIAL /NON Mission Capable	Personal Safety Critical	Hardware Safety Critical	Criticality	Probability of Occurrence
Functions	Propulsion	N	combustion	Gear Drive	1	Y	Non	N	Y	4	B
					2	Y	Partial	N	Y	3	C
				Motor	1	N	Partial	N	N	1	A
					2	N	FULL	N	N	0	D
			Electric	Gear Drive	1	Y	Non	N	Y	4	C
					2	Y	Non	N	Y	4	B
				Motor	1	N	Partial	N	N	1	A
	Energy	N	Fuel	Monitoring	1	N	FULL	N	N	0	D
				Distribution	1	Y	Non	Y	Y	5	B
			Battery	Monitoring	1	N	FULL	N	N	0	C
				Storage	1	Y	Partial	Y	Y	4	B
	Steering	Y	x-plane	linkages	1	Y	Non	N	Y	4	C
				controllers	1	Y	Non	N	Y	4	D
	Ballast	Y	water	Valves	1	Y	Partial	N	Y	3	E
				Tanks	1	Y	Non	N	Y	4	D
	Data Sensors	N	various		TBD	Y		N	N		
	Data Handling	Y	TBD		TBD	Y		N	N		
	Data Storage	Y	TBD		TBD	Y		N	N		
	Autonomy	Y	TBD		TBD	Y		N	Y		
	Health Monitoring	Y	TBD		TBD	N		N	Y		
	HVAC	Y	TBD		TBD	N		N	Y		

Figure 1: A typical representation of a functional FMECA

1.3.2 The Functional FMECA

The functional FMECA should be performed as soon as the functional baseline has been struck in order to provide the largest value to the program and to allow for planning of the physical FMECA when the program is ready. Referencing Figure 1 above, a listing of all functions that the UxV must perform are entered into the column titled “functions”. Functions should be listed at the subsystem level such that they identify the major capabilities that the system will provide. For each function, the engineers must determine if the design solution is known or if several options are being considered. A design solution is “fixed” when a technology solution is known and no alternative is on the table. The “design fixed” column is used to indicate if the design is fixed or if alternatives are still being considered. A design may be fixed even though the specific manufacturer or the finished design is incomplete but the technical solution has been chosen. For example, the engineers have chosen an x-plane rudder configuration as the desired “steering” technology solution as indicated in the “solution(s)” column. For functions where several technologies are still being considered such as in the example of the propulsion plant or energy system, engineers then enter the alternative solution(s) being considered to support those functions. If no solution is known then a TBD is entered in the solution column.

All known Sub-Functions must be defined for each technology solution identified. Sub-Functions are all of the functions needed to enable the technology solution. For example, a gear drive and a motor are both needed to enable either a combustion propulsion system or electric propulsion system. There are other sub-functions needed for these technology solutions, however the list has been shortened for illustration purposes.

The failure mode column in Figure 1 is used to define all known failure modes associated with each sub-function. Failure modes result in the loss of specific functions of the technology solution(s) identified. Failure mode descriptions should be entered in the “failure mode” column when they are known. Failure mode numbers (1) and (2) are used in the example to simplify the spreadsheet, however detailed descriptions should be used such that each known failure mode can be identified. There may be several failure modes associated with each sub-function. For example, a gear drive may fail by corrosion, loss of lubrication, bearing failure, or fatigue of the gears themselves. All known failure modes associated with each Sub-Function should be entered in this column. When the failure modes are not known, TBD may be entered.

Mission criticality of each failure mode is marked appropriately in the column titled “Mission Critical”. Mission Critical failure modes result in the loss of those specific sub-functions which are required for the vehicle to complete independent operations and perform all required independent tasking in order to complete the mission objectives. Non-mission critical failure modes result in the loss of sub-functions which are not critical to the execution of the mission but are added to enhance performance, required for testing only, diagnostics, or features which can be recovered once the mission is complete.

Engineers will need to determine how each failure mode affects the successful completion of the mission. Failure modes that result in the system remaining fully mission capable, meaning that the failure mode will not affect the performance of the mission, are marked as “FULL Mission Capable” in the column titled “FULL/PARTIAL/NON Mission Capable”. Likewise, failure modes which result in the system becoming “partially mission capable”, meaning that the mission performance is degraded to some extent, or “non-mission capable”, meaning that if the failure mode should occur the system will be incapable of completing its assigned mission are marked accordingly.

Failure modes are also evaluated as “personnel safety critical” or “hardware safety critical”. Failure modes that are a personnel safety hazard, or would cause personal harm, are marked as such in the “personnel safety critical” column. Failure modes that may cause other hardware problems when they occur, such as an electric short resulting in damage to nearby equipment, are marked as such in the “hardware safety critical” column.

The resulting criticality of each failure mode can then be calculated by summing the values in each of the following columns as described below. The total score of adding the values is then recorded in the criticality column. In some instances a score of 0 will result and in other extreme cases a score of 5 will result.

Mission Critical (Yes = 1, No =0)
Full Mission Capable = 0, Partial Mission Capable = 1, Non-Mission Capable = 2
Personnel Safety Critical (Yes = 1, No = 0)
Hardware Safety Critical (Yes =1, No = 0)

Next, a probability of occurrence of each failure mode is determined and entered into the column titled “probability of occurrence”. Probabilities of occurrence can be qualitatively or quantitatively determined using probability levels identified in MIL-STD-882E or as shown below in Table 1. If failure rates are known or can be estimated from similarity analysis, then the probability of occurrence can be estimated quantitatively using an exponential probability function and the expected operating duration. Other probability functions may be used when the technology failure profiles are understood. However, if assuming a constant failure rate, the exponential probability function, expressed as $R = e^{-\lambda t}$, can be used where λ is the failure rate and t represents the expected operating duration. Environmental impacts on the components should also be considered and supplier estimated failure rates be appropriately adjusted. When new technologies are being developed, a more detailed analysis is needed to determine the appropriate probability of occurrence value to use. When the use of failure rates are not possible, qualitative assessments can be used in the functional analysis. The design team should meet to discuss probability estimates that are appropriate to use for each failure mode. In general, qualitative assessments will provide the results needed to allow the design to mature and for a more detailed analysis to be performed during the physical FMECA.

Table 1: Example Probability of Occurrence Levels

Probability Levels			
Description	**Level**	**Individual Item**	**Quantitative**
Frequent	A	Likely to occur often in the life of an item	Probability of occurrence greater than or equal to 10^{-1}
Probable	B	Will occur several times in the life of an item	Probability of occurrence less than 10^{-1} but greater than or equal to 10^{-2}
Occasional	C	Likely to occur sometime in the life of an item	Probability of occurrence less than 10^{-2} but greater than or equal to 10^{-3}
Remote	D	Unlikely, but possible to occur in the life of an item	Probability of occurrence less than 10^{-3} but greater than or equal to 10^{-6}
Improbable	E	So unlikely, it can be assumed occurance may not be experienced during the life of an item	Probability of occurrence less than 10^{-6}

1.3.3 The Functional FMECA results

Once the functional FMECA spreadsheet has been completed, the results should be plotted on a risk assessment matrix so that further actions can be taken. A typical Risk Assessment matrix is shown in Figure 2. All failure modes are plotted in the matrix using the combination of criticality and probability of occurrence for each failure mode identified in the FMECA spreadsheet. Assessed risks are expressed as a Risk Assessment Code (RAC), which is a combination of one criticality category and one probability level. For example, a RAC of 1A is the combination of a Level 1 criticality item and a "Frequent" Level "A" probability level. Figure 2 assigns a risk level of High, Medium, or Low for each RAC. For a RAC of 1A a Medium Risk level is assigned. For all Medium and High RAC failures, engineers should attempt to design in appropriate health monitoring to identify when any of those failures occur or is about to occur. Health monitoring will also advise the systems' autonomy so that the UxV can respond appropriately to those failures. Preventive maintenance should also be planned for all frequent and probable RACs as appropriate and when the technology requires some necessary preventive maintenance. Preventive maintenance may include removal and replacement of items before they fail to ensure that the end of life of high failure rate items are less likely to occur. When health monitoring is not possible for a medium or high RAC failure mode, engineers should plan to remove, inspect and replace those components that are found to have the highest failure rates during the physical FMECA. Health monitoring systems can also be used to advise maintenance activities on all corrective maintenance that will be required long before the UxV returns to the maintenance activity. NAVSEA measures readiness through Operational Availability metrics defined as Uptime divided by Uptime + Downtime. By reducing the downtime (the time to perform repairs) and increasing the uptime (the time the systems are available to the fleet) significant improvements to the UxV's operational availability is achieved.

RISK ASSESSMENT MATRIX						
		Criticality				
		0	1	2	3	4&5
Probability of Occurrence	Frequent A	Low	Medium	High	High	High
	Probable B	Low	Medium	Medium	High	High
	Occasional C	Low	Low	Medium	Medium	High
	Remote D	Low	Low	Low	Medium	Medium
	Improbable E	Low	Low	Low	Low	Medium

Figure 2: A typical FMECA Risk Assessment Matrix

1.3.4 The Physical FMECA

The physical FMECA is performed similarly to the functional FMECA, however its value is to inform the designers of which components pose a significant risk to the system's reliability and availability allowing appropriate actions to be taken. Unlike the functional FMECA that informs the autonomy design and health monitoring design, the physical FMECA assist with updating the reliability centered maintenance process or identifying those high negative impact components within the system design. A physical FMECA can also help evaluate alternatives to design modifications such as the automatic replacement of hardware before it fails in an attempt to prevent catastrophic failures from occurring in the first place. The physical FMECA can be used in conjunction with reliability block diagrams and failure predictive models to procure spares that are expected to fail. Proper staging of those spares at the appropriate locations will ensure those components are readily available when and where they are needed. It is not necessary to wait until all hardware is chosen to perform a physical FMECA. A physical FMECA may be performed in stages as the configuration matures. The most efficient approach is to complete the physical FMECA first on components that support functions identified as high and medium risk from the functional FMECA process. Completing the physical FMECA on High and Medium risk functions allows the health monitoring system design to mature quicker as the location of sensors or the method of monitoring components are chosen. A physical FMECA is not required until after the bill of materials is complete for functions identified as low risk during the functional FMECA and sparing will be the only concern for those low risk items. Unlike the functional FMECA, the physical FMECA assesses the specific hardware being used to support each function and sub-function identified in the functional FMECA. A typical physical FMECA spreadsheet is shown in Figure 3.

		Design Fixed	Technology Solution(S)	Sub-Function(s)	Manufacurer	Part Number	Failure Mode	Failure Rate	Mission Critical	FULL/PARTIAL/ NON Mission Capable	Personal Safety Critical	Hardware Safety Critical	Criticality	Probability of Occurrence	Monitored?
Functions	Propulsion	N	cumbistion	Gear Drive	X	X	1	X	Y	Non	N	Y	4	B	Y/N
							2	X	Y	Partial	N	Y	3	C	Y/N
				Motor			1		N	Partial	N	N	1	A	
							2		N	FULL	N	N	0	D	
			Electric	Gear Drive	X	X	1	X	Y	Non	N	Y	4	C	Y/N
							2	X	Y	Non	N	Y	4	B	Y/N
				Motor			1		N	Partial	N	N	1	A	
	Energy	N	Fuel	Monitoring			1		N	FULL	N	N	0	D	
				Distribution	X	X	1	X	Y	Non	Y	Y	5	B	Y/N
			Battery	Monitoring			1		N	FULL	N	N	0	C	
				Storage	X	X	1	X	Y	Partial	Y	Y	4	B	Y/N
	Steering	Y	x-plane	linkages	X	X	1	X	Y	Non	N	Y	4	C	Y/N
				controllers	X	X	1	X	Y	Non	N	Y	4	D	Y/N
	Ballast	Y	water	Valves			1		Y	Partial	N	Y	3	E	
				Tanks	X	X	1	X	Y	Non	N	Y	4	D	Y/N
	Data Sensors	N	various	various	X	X	1	X	Y	Non	N	N	3	D	Y/N
	Data Handling	Y	various	laptop	X	X	1	X	Y	Non	N	N	3	C	Y/N
	Data Storage	Y	various	hard drive	X	X	1	X	Y	Non	N	N	3	D	Y/N
	Autonomy	Y	CTR	software	X	X	1	X	Y	Non	N	Y	4	D	Y/N
	Health Monitoring	Y	CTR	software			1		N	Full	N	Y	1	D	
	HVAC	Y	MFR	Contractor	X	X	1	X	N	Non	N	Y	3	D	Y/N

Figure 3: A typical Physical FMECA Spreadsheet

Data collected in support of the physical FMECA can be added to the Functional FMECA spreadsheet. New columns added to the functional FMECA spreadsheet to support the physical FMECA include, but are not limited to, the component's Manufacturer, part number(s) if they are known, the failure rate for each component, and if the component is being monitored. Fields that will require updates include the mission critical, Full/Partial/Non Mission capable, Personal safety, hardware safety, criticality column and the probability of occurrence columns.

The manufacturer column should include the manufacturers for all of the hardware needed to support each sub-function down to the lowest replaceable parts. Figure 3 is a simplified version illustrating one component and one manufacturer for each sub-function, however, in reality each sub-function will have many components that make up the bill of materials. All components in the bill of materials need to be accounted for in the physical FMECA. Because all components in the bill of materials will be used, all of the columns for mission critical, Full/Partial/Non Mission capable, Personal safety, hardware safety, and criticality will need to be filled. During the functional FMECA these columns represented a single function, however in the physical FMECA engineers will need to determine the criticality of screws, nuts and bolts, circuit cards, and other components in a similar fashion that was used during the functional FMECA.

The part numbers column should contain part numbers for each piece of hardware and each manufacturer if they are known. If part numbers are not known, an attempt should be made to work with the design team to identify the exact component that will be used in the design.

The failure rate column should contain failure rates obtained from previous designs if available. Using failure rates from equipment already in use in a similar application will provide the highest value to the physical FMECA. If the hardware has not been used in a similar design, engineers should attempt to identify similar equipment used in a similar environment. This similarity analysis is the second best approach to predicting failure rates. When no similarity exists, a manufacturer's failure rate can be used. When manufacturers' failure rates are used, ensure that the rates are adjusted for the environment in which the equipment will be used. Many manufacturers supply failure rates based on the defects per million that the customer can expect to see, however this may not translate into a failure rate for the purpose of reliability predictions. Another alternative to using manufacturers' failure rates is to perform a physics of failure analysis, or to break the hardware down to its individual components and predict failure rates at the component level. All failure rates should be carefully reviewed and adjusted to account for potential environmental impacts. Failure to account for the environment that the hardware will operate in will result in a very conservative analysis.

The same process used during the functional FMECA is used during the physical FMECA to enter data into the "mission critical", "Non/Partial/Full mission capable", "Personnel safety", and "Hardware Safety" columns. The "Criticality" should be calculated in the same fashion such that each component is identified according to its criticality in support of the mission.

The probability of occurrence can be calculated for each component using a monte-carlo simulation software, or through other methods applied against the design's predicted operational profile. Software tools available for predicting the probability of occurrence vary widely and should be evaluated for their functionality before investments are made.

Two types of failures can be expected in a design, A-Mode and B-Mode. A-mode failures are those failures that are predictable and fail at a constant failure rate. A-mode failures are generally corrected by removal and replacement of the same part when they occur. B-mode failures are those failures, which are unpredictable and fall outside the estimated failure rate identified in the physical FMECA. B-mode failures are environmentally induced failures such as unexpected humidity level, high or low temperature environments, extreme vibrations or electromagnetic effects. B-mode failures cannot be introduced into the FMECA spreadsheet and will be dealt with during testing and the use of a Failure Reporting, Analysis and Corrective Action System (FRACAS). Unpredictable B-mode failures are a result of the absence of rigorous engineering and analysis that might have identified deficiencies in the design during the design phase. How many B-mode failures occur will depend on how well systems engineering is applied, the number of manufacturing defects, or any unexpected environmental issues affecting the equipment. For these reasons, planning for and implementing a closed loop FRACAS is critical when entering the test and evaluation phase of a program. As mentioned previously, the physical FMECA has other valuable uses and should not be ignored.

Once all data is entered into the physical FMECA spreadsheet, with the exception of hardware monitoring, the analysis can be completed in the same manner as the functional FMECA. All failure modes are assigned RAC values and entered into the Risk Assessment Matrix as shown in Figure 2. Once complete, engineers can then determine if all high and medium risk equipment are being monitored for failure. Decisions on the need to monitor each component can then be made based on their ranking in the risk model. In some cases when a high risk component cannot be monitored, predicted periodic removal, inspection or replacement should be planned.

2.0 CONCLUSION

Functional and physical FMECAs are critical design tools necessary to support the design of UxVs or any equipment where performance and health monitoring is being considered. The functional FMECA should be accomplished prior to preliminary design so that the results can inform the design of the system's autonomy, such that the vehicle is capable of responding appropriately to all system failures. Some failures may require little to no action during the mission, while other failures may require a deviation of the mission objectives or a complete abortion of the mission. Also, a functional FMECA must inform the design of the health monitoring system such that appropriate failure modes are detectable to support autonomy and to direct preventive and corrective maintenance activities.

A physical FMECA is used during initial design to inform the reliability centered maintenance process to help develop and manage the fleet's preventive maintenance tasking. The intent of reliability centered maintenance is to formulate failure management strategies that allow assets to continue operating at the desired levels of performance and availability. After fielding, a health monitoring system will inform updates to the reliability centered maintenance process to improve preventive maintenance tasking. Reliability data is used to determine what preventive maintenance should be performed to improve the reliability of systems. Preventive maintenance systems inform maintenance activities on existing or potential failures occurring in the fleet in real time, or prior to the hardware arriving at a maintenance activity. A physical FMECA is also used during

design to inform the CBM+ process. The CBM+ process uses health-monitoring systems to inform what corrective maintenance is required and to expedite corrective maintenance on systems.

Functional and physical FMECAs are not the only tools necessary for maintenance optimization. The FMECA is the backbone required to mature the design, but engineers must be proficient in many other aspects of reliability & maintainability engineering to produce a valuable FMECA that will inform the design appropriately. As alluded to in this paper, engineers must be proficient in performing many of the activities listed in the References for the FMECA process to serve its full purpose.

REFERENCES

[1] DOD-HDBK-791 17 Mar, 1998 Maintainability Design Techniques

[2] DODM-4151.22M 30 Jun, 2011 Reliability Centered Maintenance

[3] MIL-HDBK-189C 14 June, 2011 Reliability Growth Management

[4] MIL-HDBK-470 4 Aug, 1997 Designing and Developing Maintainable Equipment

[5] MIL-HDBK-472 12 Jan, 1984 Maintainability Predictions

[6] MIL-HDBK-781 1 Apr, 1996 Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development, Qualification, and Production

[7] MIL-HDBK-2155 11 Dec, 1995 Failure Reporting, Analysis and Corrective Action Taken

[8] MIL-HDBK-2164A 19 Jun, 1996 Environmental Stress Screening Process for Electronic Equipment

[9] OPNAVINST 3000.12A 2 Sep, 2003 Operational Availability of Equipment's and Weapons Systems

[10] OPNAVINST 4442.5A 15 Aug, 2011 Readiness Based Sparing

[11] OPNAVINST 4700.7L 25 May, 2010 Maintenance Policy for United States Navy Ships

[12] OPNAVINST 4790.4F 27 Oct, 2014 Ships Maintenance and Material Management System

[13] OPNAVINST 4790.13B 23 Sep, 2014 Maintenance of Naval Electronic Equipment

[14] OPNAVINST 4790.16B 1 Oct, 2015 Condition Based Maintenance (CBM) and CBM Plus Policy