Proceedings of IDETC/CIE 2008
ASME 2008 International Design Engineering Technical Conferences
& Computers and Information in Engineering Conference
August 3-6, 2008, New York, New York, USA

DETC2008-49656

VISUALIZATION AND VERIFICATION METHOD FOR FAILURE NETWORK ANALYSIS OF SPACE LAUNCH VEHICLES

Keiichiro Fujimoto, Akira Oyama, and Kozo Fujii
Japan Aerospace Exploration Agency
JAXA's Digital Innovation Center
3-1-1, Yoshinodai, Sagamihara, 229-8510, Japan
Phone +81-42-759-8270
E-mail fujimoto.keiichiro@jaxa.jp

Nobuyuki Iizuka and Koichi Okita
Japan Aerospace Exploration Agency
Office of Space Flight and Operations
2-1-1, Sengen, Tsukuba, 305-8505, Japan
Phone +81-29-868-5484
E-mail iizuka.nobuyuki@jaxa.jp

ABSTRACT

Comprehensive failure network analysis method was studied for liquid rocket engine development which includes failure propagation through various types of component interfaces in order to achieve exhaustive enumeration of possible failures and to identify actions to eliminate or reduce the potential failure. New failure network visualization method was developed in order to make it easier to understand complicated failure propagation mechanism among multiple system levels. Verification analysis method is developed in which it is verified all of user-specified component interfaces are contained in the failure network analysis result. The perceived component interface is specified by the analyzer and the failure propagation in the result of failure analysis is summarized in two separate N2 charts. By comparing with these two N2 charts, unperceived component interface and the unconsidered failure propagation can be found. It is found to be promising approach to achieve exhaustive enumeration especially for forgettable component interface.

Keywords: Failure mode and effect analysis, fault tree analysis, failure network analysis, component interface, failure propagation, rocket engine, N2 chart.

INTRODUCTION

From 2004, Japan aerospace exploration agency (JAXA) has initiated reliability improvement campaign for development and operations of space launch vehicles and satellites, in which current development process is aimed to be renovated by effective utilization of design engineering technologies and the information technologies.

Since main cause of the reliability degradation of space launch vehicle is generally liquid rocket engine failures, next generation expander bleed-cycle liquid rocket engine LE-X [1] is initially focused, which is under the development research phase. Since this engine is expected to be used for manned space launchers, an achievement of high reliability is essential. Liquid rocket engines consist of several hundreds of components with various types of interfaces including small parts. Operating conditions of fuel and oxidizer are extremely high temperature and pressures, so that even small parts failure mode such as fuel valve seal leakage can be resulting in the catastrophic failure, loss of crew. Failure mechanism of launch vehicles is complicated including multiple failure propagations through various component interfaces. In order to achieve high reliability, all of the possible failure modes should be extracted and comprehensively considered from the initial design stages.

In Fig. 1, schematic view of the high reliability development methodology is shown. After the vehicles' conceptual design based on the comprehensive trade-off studies, each components such as turbo-pump for rocket engine are designed and tested based on the given design requirements, if root cause of the high risk failure mode is poor design its solution should be considered in the design requirements. In reliability prediction process, all of the possible failure modes are desired to be

predicted including component failure modes, interface failure modes and interface failure propagation. In order to mitigate risk of high risk failure modes, critical components are re-designed based on the improved design requirements, or redundant system will be employed to achieve high reliability of the launch vehicle.

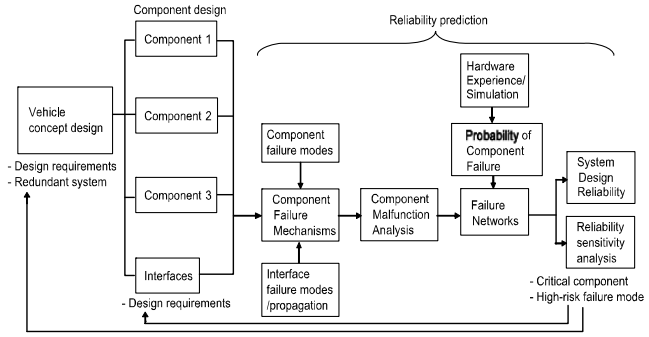


Figure 1. High reliability space launch vehicle design process.

In order to perform reliability prediction, failure mode and effect analysis (FMEA) and fault tree analysis (FTA) is conventionally used [2-4]. In order to improve the efficiency of the reliability prediction work, reliability prediction support tool was developed by which user can perform prediction based on both FMEA and FTA approaches [5]. An example of function-based failure analysis result obtained by using this method is shown in Fig. 1. As shown in this figure, allocation of failure modes to each component and their cause and actions are shown in the same way of conventional FMEA table. Failure network structure can be edited and shown in failure network view as shown in bottom of Fig. 2, thus this approach is called failure network analysis. Conventional FMEA and FTA approach including failure network analysis [2] is basically suitable for the failure mode description only for components not for interface failure modes. This is the one of the reason why the component interface failure modes and propagation is often forgotten. In addition, brain storming discussion is necessary to pursue an exhaustive enumeration and discuss actions to eliminate or reduce risk, resulting failure mechanism expressed as failure tree structure is difficult to understand because failure tree includes various failure modes of different system level components.

In this study, verification method for failure network analysis is developed to pursue exhaustive enumeration of failure modes especially for component interface failure modes and failure propagation through the component interfaces. An effective visualization method for failure network analysis result is also developed to make it easier to understand by showing failure network structures on pi-chart-like background blocks.

Component name	Deisng requirement	Failure mode	Cause	Effect	Action			Probability	Criticality	Detection difficulty	Weight
	Function			Engine System	Design /development	Production	···				
Comp A	Func A-1	FM1	FM 2					0.001	5	4	35
			FM 10					0.0015	3	3	35
Comp B	Func B-1	FM 2	···					0.002	3	3	21
	Func B-2	FM3	···					0.0013	3	3	23
Comp C	Func C-1	FM 10	···					0.0017	2	3	12
	Func C-2	FM11	FM33					0.0005	4	4	8
	Func C-3	FM29	···					0.001	5	4	9

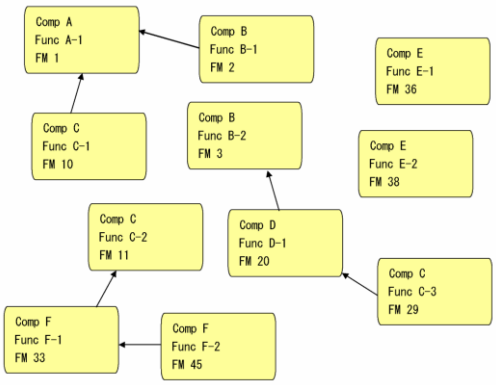


Figure 2. Failure analysis result example obtained by using failure network analysis method.

In the first section, framework of risk management system is overviewed which will be developed at JAXA. In the second section, new visualization method for failure network result is discussed. Finally, verification analysis method for failure network analysis result is discussed.

FRAMEWORK OF RISK MANAGEMENT SYSTEM

As shown in Fig. 3, this system is consists of four databases, lessons' learned database, risk item list database, risk prediction result database and technical document database. All of the risk potentials are collected and accumulated in risk prediction result database in the forms of failure network structure which will be analyzed or displayed in various types of visualization mode such as FMEA and FTA modes.

There are mainly four ways to obtain risk potential information. One is lessons' learned obtained in the past or current development experiences or in other project. It will include failure mode which is experienced during the development phase such as component cracks due to the transient heat flux or dynamic load during the development tests. Second is risk potential which is obtained by the detailed investigation of failure mechanism, which is really happened in the development activities. This risk potential information will initially be provided in the forms of risk item list database. Third is risk potential obtained by the reference and extrapolation of the past risk prediction result. Generally similar components will experience similar failure modes, and thus, past risk prediction result database vital resource of the risk potential information. As shown in Fig. 3, contents of the risk prediction result database are linked with corresponding technical documents such as detail description of measures to

fix past failures. In order not to lose this valuable development knowledge, linkage of the risk prediction database and the related technical document databases is important. Fourth is risk potential obtained by the brainstorming discussion among specialists such as development team members, experts in related fields and rocket engine component researchers. Since all of the design or development decisions such as re-design candidate critical component selection or candidate failure modes for risk mitigation campaign are based on the discussion of this types of discussion, it is the key how much valuable risk potential information can be collected. Collected risk potential information should be summarized and displayed by the effective way to understand. Development of visualization method for failure network analysis result conducted in this study is one of the efforts to encourage the effect of brainstorming discussions.

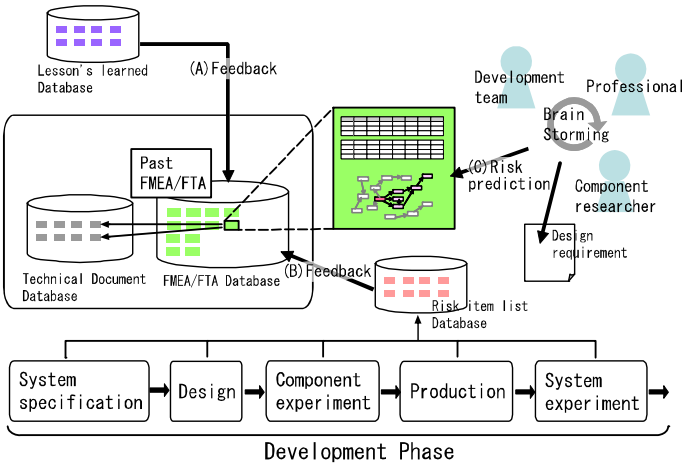


Figure 3. Framework design of risk management system.

During development process, actions to eliminate or reduce the risk potentials are identified and its progress will be monitored and managed based on its criticality, event probability and completeness of the action. Results of their risk mitigation activities are reported as technical document which is accumulated in technical document database, which each document is linked with corresponding failure or failure mode in risk prediction result database.

Most of the approaches to estimate overall launch vehicles' reliability are same as the approach conducted for Apollo project at NASA [2]. When the failure mode of major components are obtained with failure mechanisms, component malfunction analysis is performed to establish a failure network for the system which permits overall system reliability to be estimated from component reliabilities. The probability of failure modes is estimated based on the hardware experience, hardware experiments and the numerical simulations. Effective utilization of state-of-art numerical simulation technology is key issue for successful and meaningful estimation of overall system reliability. Qualitative risk assessment approach similar to qualitative risk assessment system (QRAS) [6] will be considered and developed.

FAILURE NETWORK VISUALIZATION METHOD

The failure network analysis method proposed by the present authors [5] is flexible which can be applicable for large scale systems such as overall rocket engine system. As shown in Fig. 4, rocket vehicle consists of hundred thousands of components with various types of component interfaces. Therefore, failure network analysis results will include failure modes of different system level components. Thus, it is difficult to distinguish the system-level failure propagation from the failure propagation between same system-level components. In order to make it easier to understand failure mechanism with system hierarchy information, new visualization method for failure network analysis result is conducted.

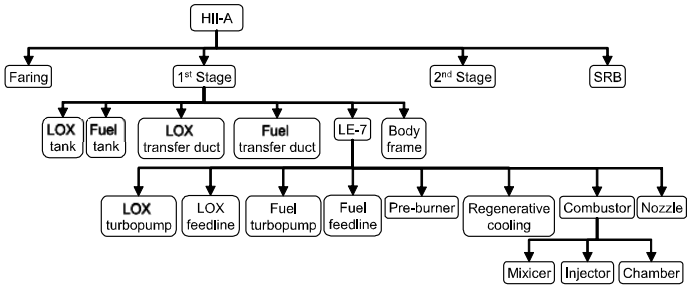


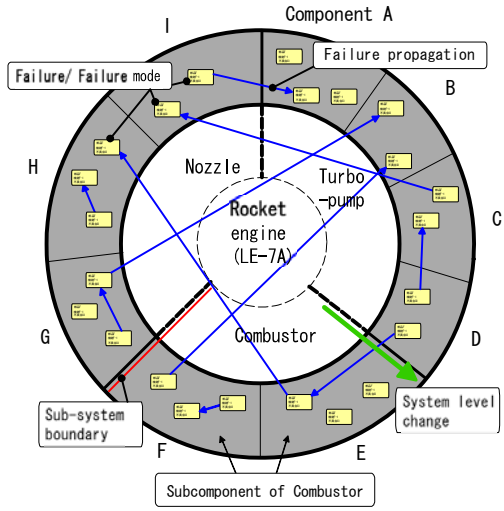
Figure 4. System hierarchy of HII-A rocket.

There are various visualization methods for network data, the visualization method in which pi-chart-like background block is used as shown in Fig. 5. All of failure mode blocks which belongs to the same component is located in the same background block as shown in Fig. 5. The red line shown as 'sub-system boundary' in Fig. 5(a) is the sub-system boundary by which circle is partitioned into some pieces. Each of pieces corresponds to the sub-system. Thus, two grey background blocks shown as "E" and "F" in Fig. 5(a) correspond to the subcomponent of combustor. This visualization method is suitable to visualize hierarchical structure of components in the failure network.

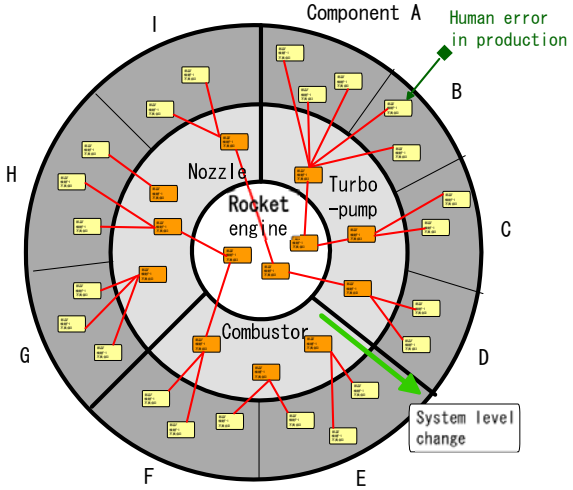
By using this visualization method, the types of the failure propagation can be understood easily at a glance. Failure propagation arrow which crosses sub-system boundary line corresponds to the failure propagation through the component interface. Failure propagation arrow started and terminated in the same background block corresponds to the internal failure propagation within the component. If there are so many failure propagation arrows going out from the background block, it means that corresponding component has many risk potentials.

The failure network basically consists of multiple FTA-like failure linkage structures as shown in Fig. 4(b).

Failure modes located in the center circle are root failures of the overall system. By tracing the propagation network from the center root failure toward the outside in the radial direction, it is easier to recognize which component failure mode can be the trigger of the system failure. In order to show the extent of the impact of another failure mode such as human error, corresponding failure mode block is located outside of the circle. This visualization method is useful to perform quick review of the failure analysis result, and is also good reference document to have brainstorming.



(a)Failure propagations within the same-system level components.



(b)System-level failure propagations.

Figure 5. Failure network visualization by using pi-chart-like background block.

VERIFICATION ANALYSIS METHOD FOR FAILURE PROPAGATION THROUGH COMPONENT INTERFACE

Rocket engines have several hundreds of components, and thus there exists various component interfaces such as fluid interface and the physical contact interface. Since operation pressure and temperature of fuel and oxidizer changes significantly during its running path, the small unexpected event can be easily resulting in the catastrophic mission failure. Therefore, from the initial stage of the design, possible failure scenario should be shared as common perceptions. And comprehensive design considerations should be done from the initial design stages. If the component interface corresponds to the output or input of the component functions such as fuel or oxidizer pressure or temperatures, this type of component interfaces tend not to be forgotten during the risk predictions such as FMEA and FTA. In other words, if the component interface is not input and output of the component function, this type of component interface tend to be forgotten. In addition, design requirements to prevent component failure for this type of component interface are also tend to be forgotten, because even without these requirements system can be designed in the early design stages. In order to achieve high reliability of the system, all of the possible failure modes should be extracted and the design requirements to prevent failure mode are identified.

In order to visualize the obtained failure analysis result, N2 chart [4] is used in this study. Although N2 chart has been used for software interface design, it is applicable also for the hardware interface. In Fig. 6, example failure network analysis result is shown in the style of N2 chart, which corresponds to the result of Fig. 2. In the left edge column and the top row, name of the components are given. Each cell stands for the component interface. For example, cell shown as “B→A” in Fig. 6 is corresponding to the failure propagation through the interface between component “A” and “B”. Blank cell means that there is no failure propagation. In order to make sure whether there is any failure propagation resulting in the failure of component “A”, 2nd column is checked. Since there are cells marked as “B→A” and “C→A”, this means that failure mode of “B” and “C” possibly result in the failure of component “A”. It implies that there is some component interface between component “A” and “B” and between component “A” and “C”. This N2 chart is named as ‘failure propagation N2 chart’ in this study.

In Fig. 7, an example of the component interface for 2nd staged liquid rocket engine is shown in the N2 chart. Basically, the flow parameters at the component interface such as temperature, pressure and flow rate are treated as the design variables, and the static load at the physical contact interface is treated as the design constraints. Therefore, some of the component interfaces are already known at the time when the failure analysis is started. In order to describe perceived component interfaces, N2 chart can be used as shown in Fig. 7.

This N2 chart is name as ‘perceived component interface N2 chart’ in this study.

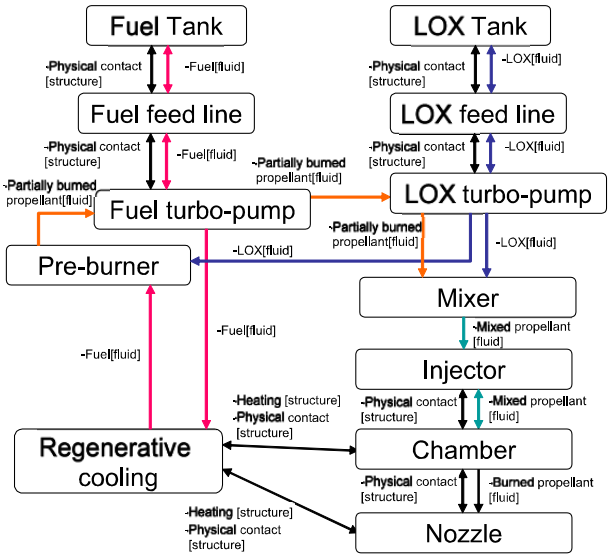
Since most of the component interfaces are known due to its importance, thus, they should be appeared in the failure scenario. In order to improve the completeness of the enumeration, verification analysis to verify that all of perceived component interfaces are considered in the failure network analysis is conducted. Its main procedures for function-based failure network analysis are shown in Fig. 8. At first, component deployment tree is generated. Secondary, ‘perceived component interface N2 chart’ is generated. Then, functions are allocated with the components and failure network analysis is performed. After finishing failure network analysis, ‘perceived component interface N2 chart’ and ‘failure propagation N2 chart’ are compared. If there is any component interface which is not contained in the failure network results and there is any failure propagation related to this component, the failure network analysis is performed again. Meanwhile, in the situation that there is any failure propagation whose corresponding component interface does not exist in ‘perceived component interface N2 chart’, that component interface is added.

This verification analysis method is useful to achieve the exhaustive enumeration of the failure modes, and also useful for the extraction of the forgettable component interface as well. If needed, design or operational considerations are conducted for the extracted component interfaces.

In addition, by using failure propagation N2 chart, it is easier to understand the extent of the influence of each failure modes. Thus, based on the failure propagation N2 chart and the corresponding failure network, the design requirements and the measurement item for the health-monitoring in the firing experiment can be discussed. This N2 chart can also be used for reference document to have quick review of failure network analysis results.

	Comp A	Comp B	Comp C	Comp D	Comp E	Comp F
Comp A						
Comp B	B→A					
Comp C	C→A			C→D		
Comp D		D→B				
Comp E						
Comp F			F→C			F→F

Figure 6. Failure network analysis result shown in N2 chart.



(a)Component interface in network.

	LOX Tank	LOX feedline	LOX Turbo pump	Fuel Tank	Fuel feedline	Fuel Turbo pump	Pre-burner	Mixer	Injector	Chamber	Nozzle	Regenerative cooling
LOX Tank		-LOX[Fluid] -physical contact										
LOX feedline	-LOX[Fluid] -physical contact		-LOX[Fluid] -physical contact									
LOX Turbo pump		-LOX[Fluid] -physical contact					-LOX[Fluid] -Partially Burned[Fluid]	-LOX[Fluid] -Partially Burned[Fluid]				
Fuel Tank					-Fuel[Fluid] -physical contact							
Fuel feedline				-Fuel[Fluid] -physical contact		-Fuel[Fluid] -physical contact						
Fuel Turbo pump					-Fuel[Fluid] -physical contact		-Fuel[Fluid] -Partially Burned[Fluid]	-Partially Burned[Fluid]				-Fuel[Fluid] -physical contact
Pre-burner			-LOX[Fluid] -Partially Burned[Fluid]			-Fuel[Fluid] -Partially Burned[Fluid]						
Mixer			-LOX[Fluid] -Partially Burned[Fluid]			-Partially Burned[Fluid]						
Injector										-Mixed[Fluid] -physical contact		
Chamber									-Mixed[Fluid] -physical contact		-Burned[Fluid] -physical contact	
Nozzle										-Burned[Fluid] -physical contact		-Heat flux -physical contact
Regenerative cooling						-Fuel[Fluid] -physical contact	-Fuel[Fluid] -physical contact				-Heat flux -physical contact	

(b)Component interface in N2 chart.

Figure 7. Example of the component interface for 2nd staged liquid rocket engines.

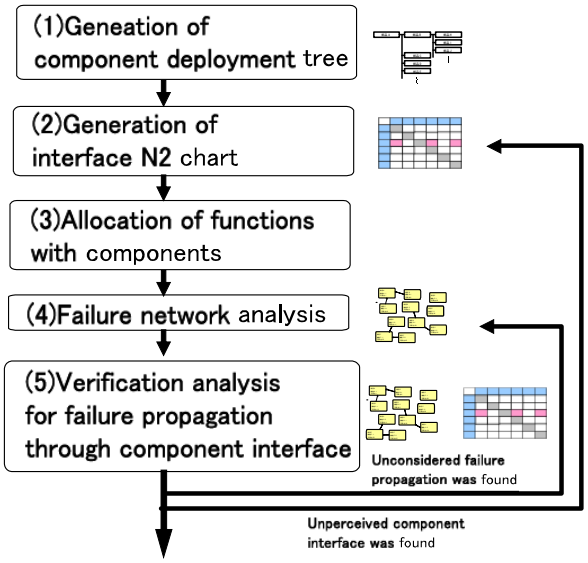


Figure 8. Failure network analysis process including verification analysis for failure propagation through component interfaces.

CONCLUSIONS

Comprehensive failure analysis method was studied for liquid rocket engine development which includes failure propagations through various types of component interfaces in order to achieve exhaustive enumeration of possible failures and to identify actions to eliminate or reduce the potential failures. Framework design of JAXA's risk management system was overviewed in which all of the information of failure potentials are obtained in the practical rocket engine development and accumulated in the risk management database.

New failure network visualization method was developed in order to make it easier to understand complicated failure propagation mechanism among multiple system levels. In addition, verification analysis method is developed by which it is verified all of expected failure propagation through perceived component interface is contained within the failure analysis result. By using N2 diagram to specify perceived component interfaces and to visualize obtained failure analysis result, this method is found to be promising to achieve exhaustive enumeration especially for forgettable failure propagation through component interface.

REFERENCES

[1] Kurosu, A., Yamanishi, N., Tani, N., Okita, K., Ogawara, A., Onga, T., and Atsumi, M., 2006, "Study of Next Booster Engine LE-X in JAXA," AIAA-2006-4700.

[2]General Electric company, "State-of-the-art Reliability Estimate of Saturn V Propulsion Systems," NASA CR-55236.

[3]Science Applications International Corporation, "Probabilistic risk assessment of the Space Shuttle", Space shuttle catastrophic failure frequency final report, 1993.

[4] Shishko, Robert, "NASA Systems Engineering Handbook," NASA SP-6105, 1995.

[5]Fujimoto, K., Iizuka, N., Oyama, A., Kado, Y., Fujii, K., Nanri, H., and Okita, K., "Visualization of design interface information based on detailed failure mode effect analysis data," Proceedings of the 17th JSME Design & Systems Division Conference, pp. 205-208, Sendai, Japan (in Japanese).

[6]Fayssal, M. S and Rebecca, L. B., "NASA New Approach for Evaluating Risk Reduction Due to Space Shuttle Upgrades", Proceedings of Annual Reliability and Maintainability Symposium, 2000.