20TH INTERNATIONAL DEPENDENCY AND STRUCTURE MODELING CONFERENCE, DSM 2018

TRIESTE, ITALY, OCTOBER 15 – 17, 2018

A Failure Propagation Methodology for Analyzing Functional Models of Extremely Large Complex Systems

Leonel Akoto Chama, Oliver Bertram

Department of Safety Critical Systems & Systems Engineering, Institute of Flight Systems, German Aerospace Center (DLR), Braunschweig, Germany

Abstract: The identification of risk of potential loss of system functionality within the early stages in designing complex systems is of growing importance for risk sensitive industries. In order to enhance early design and analysis of complex system architectures using design structure matrices, this paper introduces a failure propagation index methodology for analyzing functional architecture concepts for extremely large complex systems. Unlike the classical hazard analysis techniques which become difficult to handle for extremely large complex systems, this work proposes a functional failure propagation indexing method that segments a large complex system and applies failure propagation modulating factors to estimate the criticality of the system's elements. The propagation index quantifies the relative impact of a functional failure on the overall architecture. The feasibility of the method is demonstrated using a functional model of a multifunctional actuation system architecture concept for the high-lift of a fixed wing aircraft.

Keywords: extremely large complex systems, functional failure propagation analysis, design structure matrix, system element criticality, aircraft, high lift actuation system concept

1 Introduction

The identification of risks of potential loss of system functionality during the earliest stages in designing complex systems is of growing importance (Tolga, et al., 2010). Early stage design provides the greatest opportunities to explore design alternatives and perform trade studies before costly design decisions are made. For instance, the tendency today to design the safety-critical flight control systems for multifunctionality poses many challenges (Akoto Chama, et al., 2017; Akoto Chama & Bertram, 2018). These challenges arise as a result of high safety targets and high system complexity (Sobieszczanski-Sobieski & Haftka, 1997) which may leave certain concept limitations unidentified by the designer at the early stages in development. This design process becomes even more challenging for extremely large complex systems, because classical hazard analysis techniques become more difficult to handle. On one hand, early identification and mitigation of critical design limitations are vital in designing safe and reliable large complex systems. On the other hand late identification of limitations of already established designs may require subsystem changes, which will in most cases result in changes to other parts of the subsystems, thereby increasing time and cost. Design Structure Matrix (DSM) methods (Eppinger & Browning, 2012) are widely used in generating and analyzing architectures of complex systems with a central focus on complexity management and change propagation analysis in terms of redesign or incremental development as shown in (Clarkson, et al., 2004; Giffin, et al., 2009;

Hamraz, et al., 2012; Marle & Bocquet, 2010; Fang & Marle, 2012). While these works focus on change propagation in terms of changing other subsystems in order to accommodate a change in a particular subsystem during redesign, incremental development or design for customization, they do not focus on the impact of subsystem failure on the functioning of the system (i.e. how failure of a subsystem is propagated within a complex system). Because failure of critical subsystem elements of an already established design may significantly impact the functioning of the system, their early prediction could help guide early design decisions. As a further step in enhancing the process, this work integrates preliminary safety analysis within the DSM framework by introducing a Failure Propagation Index (FPI) method for quantifying risk of potential loss of system functionality. The FPI method quantifies each functional element‘s relative failure impact on the overall architecture. The impact value is calculated from the Functional Failure Propagation Matrix (FPM) generated from the functional model. Once the distribution of the FPIs is known, valuable insights can be extracted from the architecture and early design decisions can be made to enhance or mitigate architectural concept limitations. Unlike in the aforementioned works by (Clarkson, et al., 2004; Giffin, et al., 2009; Hamraz, et al., 2012; Marle & Bocquet, 2010; Fang & Marle, 2012) which focus on how change is propagated during engineering design change, the proposed method in this work focuses on predicting how a failure of a particular subsystem element prevents other subsystems from performing their intended functions.

2 Conventional Design Approach

Typically the design of systems begins with stakeholder analysis, then requirements analysis and ends with an architecture as shown in Figure 1. Of particular importance in the process is the analysis and allocation of functions carried out after the requirements analysis and before the synthesis of the concept.

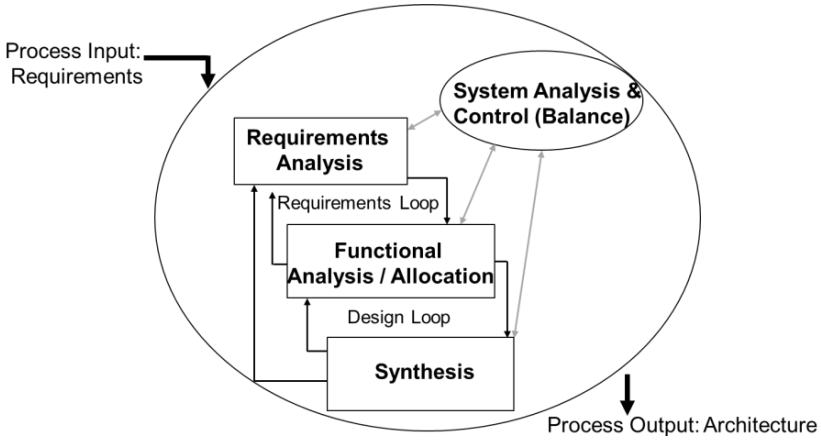


Figure 1. Classical design process

At this stage, complex systems pose many design challenges and even greater challenges for extremely large complex systems, thus methods which are also applicable to

functional networks have been developed to manage system complexity and change propagation (Hamraz, Caldwell, & Clarkson, 2012; Clarkson, Simons, & Eckert, 2004; Fang & Marle, 2012; Carlos Inaki, 1998; Thebeau, 2001). Also, within this stage, the classical hazard analysis techniques such as the Functional Hazard Analysis (Clifton A, 2005; Dalton, 1996) are performed on the system to identify potential hazardous elements in the design. While these hazard analysis techniques are sufficient, they become very difficult to apply for extremely large complex systems which may lead to potentially unidentified hazardous system elements. Thus, if design flaws are not identified and mitigated early enough, this may result in costly design changes later in the design process or even catastrophic failures during the operational phase of the system (Akoto Chama & Bertram, 2018).

3 Method

Every system is fundamentally made up of functional elements. How these elements are connected and interact with each other defines the functional architecture of the system. Understanding how these functions affect each other and how they work together to accomplish the mission of the system is vital in creating optimal system architectures. In order to identify critical system elements whose failure impact can greatly affect the functioning of the system, this work proposes a three step FPI approach with main focus on the functional failure propagation analysis that quantifies the relative failure impact of subsystem elements. The FPI method introduced in this work, has been developed to enhance the design process by reducing the risk of design flaws propagated to later stages in the design process for extremely large complex systems. The principle of the method is explained below.

3.1 Functional Model (Step 1)

The process begins by creating a functional model of the system to be designed. A functional model of a system is an abstraction that represents the system's functions and their interactions (Akoto Chama, et al., 2017; Stone & Wood, 2000; Hutcheson, et al., 2007; Chakrabarti, et al., 2011; Pahl, et al., 2007). It represents the transformation of energy, material or signal information flows as they pass through the system elements. It defines how the functions will operate together to perform the system mission. Generally, more than one functional model can satisfy the system requirements and thus a suitable functional model depends on the level of required detail that should be analyzed. In order to explain the proposed method, consider the arbitrary seven element system as shown in Figure 2. It is assumed that the elements of the system are functions, which are connected to each other as shown.

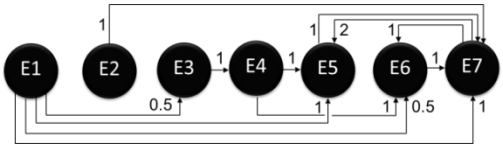


Figure 2. Functional model of an arbitrary seven element system

3.2 Design Structure Matrix (Step 2)

The DSM, also referred to as dependency structure matrix is a tool for network modeling (Eppinger & Browning, 2012). It is used to represent a system's architecture (or design structure) by mapping the interactions among the elements that make up a system. The DSM is represented as a square $\widetilde{N} \times \widetilde{N}$ matrix, with relations (or interactions) among the set $\widetilde{N}$ of system elements. One can think of a DSM as a collection of cells (e.g. E1 to E7 in Table 1) along the diagonal of the matrix as representing the system elements (Figure 2) analogous to the nodes in the digraph model (Eppinger & Browning, 2012). The diagonal cell has inputs entering from its left and right sides and outputs leaving to above and below as shown on Table 1. The corresponding marks in the off-diagonal cells indicate the sources and destinations of the inputs and outputs, analogous to the directional arcs in a digraph. The inputs to an element in a row (which are outputs of other elements) are indicated by marks in that row. The outputs from an element in a column (which are inputs to other elements) are indicated by marks in that column. For the seven functional elements system shown above, the corresponding DSM is represented as shown on Table 1.

Table 1. Design structure matrix of the functional model above

		E1	E2	E3	E4	E5	E6	E7
Element 1	E1	E1						
Element 2	E2		E2					
Element 3	E3	x		E3				
Element 4	E4			x	E4			
Element 5	E5	x			x	E5		x
Element 6	E6	x			x		E6	x
Element 7	E7	x	x			x	x	E7

3.3 Functional Failure Propagation Analysis (Step 3)

If a functional element fails, it is possible that other elements (functions) within the functional network are affected, synonymous to change propagation in (Clarkson, et al., 2004; Giffin, et al., 2009; Hamraz, et al., 2012; Marle & Bocquet, 2010) . In this section, all functions which are affected as a result of the failure of a particular function are captured. The Functional Failure Propagation Analysis (FPA) generates the information on how functional failures are propagated within the functional (network) model. For the propagation analysis the following definitions are used:

Downstream elements: Elements along the affected paths to which the output of the element under consideration goes.

Upstream elements: Elements along the affected path from which the element under consideration receives inputs.

Modulation: The change in the effect of a failure as it is propagated within the network.

For example, consider the seven element functional model as shown in Figure 2 and let the element E1 be degraded or fail. Then, there are four different failure propagation possibilities (or scenarios) within the internal network structure;

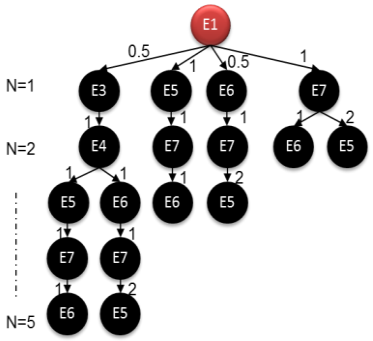
Case 1: The failure is not propagated
Case 2: The failure is propagated equally upstream and downstream across the entire network without modulation.
Case 3: The failure is propagated upstream and downstream across the entire network with modulation.
Case 4: The failure is propagated only through certain elements within the network, with or without modulation.

For extremely large complex systems, the fourth case becomes extremely challenging to handle since the elements affected must be identified for the analysis. In this work a generalized approach for capturing failure impact is presented. The failure propagation is captured within a predictive matrix called Failure Propagation Matrices (FPMs) which are DSMs whose off-diagonal cell entries represent the propagation paths and the magnitude of the effect on an element within the propagation path. The magnitude of the effect is reflected in the strength of the connection (0.5 for weak, 1 for medium and 2 for strong) which defines the relative importance of the connection within the functional network. The importance of the connection is based on its necessity for efficient system operation. A basic sensitivity analysis showed that the relative criticalities of the system elements were mostly stable to small changes in the connection strengths. Also the term "predictive" is used in describing the FPMs because the entries are based on subjective judgement and tied closely to the intended behavior of the subsystem within the system.

The propagation of the failure across different elements may differ according to the four possibilities listed above. Figure 3, shows scenarios 2 and 3 (Cases 2 and 3), where the entire network is affected, is affected. Figure 3(a) shows a failed element within the DSM and Figure 3(b) shows a tree representation of the elements affected as a result of this failure. The tree is generated using a depth first search algorithm beginning from element E1, and representing all possible paths; hence multiple elements appear in different tree branches.

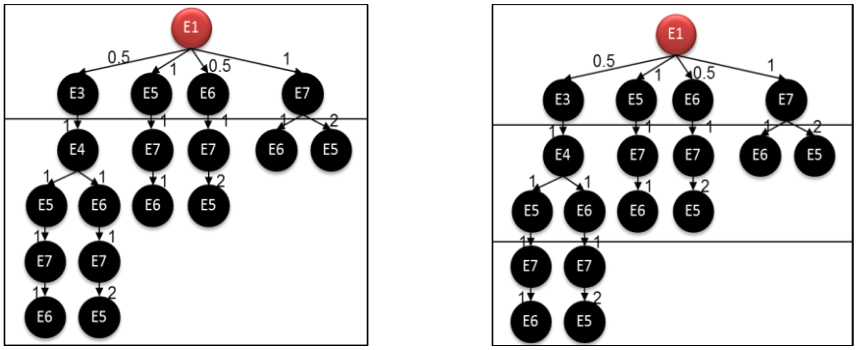
	E1	E2	E3	E4	E5	E6	E7
E1	E1						
E2		E2					
E3	0.5		E3				
E4			1	E4			
E5	1			1	E5		2
E6	0.5			1		E6	1
E7	1	1			1	1	E7

(a) E1 failed element



(b) Depth first search tree

Figure 3. An exemplary failed element and its corresponding tree



(a) Two segment partition (b) Multiple segment partition

Figure 4. Segmentation of failure propagation paths

Since E1 has no upstream elements, they are not shown. Furthermore, in order to capture propagation effect across the entire network according to scenario 3 (Case 3), the tree in Figure 3 (b) can be segmented as shown in Figure 4. The tree elements can be partitioned into two segments as shown in 4(a) or multiple segments as shown in 4(b) according to impact of the failure on them. The calculated value from the Failure Propagation Matrix (FPM) is called the Failure Propagation Index (FPI) and determines the relative criticality of the element. To obtain an element's FPI, let i and j be elements of the functional model such that when element i fails, element j is affected (i.e. j is an element that belongs to the tree generated from element i). Also let $e_{i,j}$ be the edge preceding element j, along the tree path between i and j. For a given depth N, let $S(i,N)$ be the set of elements j (in the tree of i) at depth N from i. Note from Figure 3 that the same element j may appear at different depths. Then the summed up edge magnitudes at a given depth N are:

$$P(i,N) = \sum_{j \in S(i,N)} e_{i,j} \qquad (1)$$

Each depth is assigned a modulation factor M(N). The modulation factor is chosen to reflect how an element failure may impact other elements within the network. For example, for a functional network which is designed such that distant elements are less affected, a modulation factor which is inversely proportional to the distance can be chosen. Thus, the FPI for i is the following sum:

$$FPI_i = \sum_N M(N)P(i,N) \quad (2)$$

If $\big(M(N)\big)_{N=1\ldots MaxN}$ and $\big(P(i,N)\big)_{N=1\ldots MaxN}$ are interpreted as vectors, then the FPI for i is the inner product of these two vectors:

$$FPI_i = \langle \big(M(N)\big)_{N=1\ldots MaxN}, \big(P(i,N)\big)_{N=1\ldots MaxN} \rangle \qquad (3)$$

Since failure propagation may be different for upstream and downstream elements, introducing direction on (3) yields:

$$FPI_i^- = \langle \Big(M_{up}(N)\Big)_{N=1\ldots MaxN}, \Big(P_{up}(i,N)\Big)_{N=1\ldots MaxN} \rangle \qquad (4a)$$

$$FPI_i^+ = \langle \left(M_{dn}(N)\right)_{N=1\ldots MaxN}, \left(P_{dn}(i,N)\right)_{N=1\ldots MaxN} \rangle \qquad (4b)$$

Equation (4a) gives the calculated partial FPI (FPI_i^-) from elements affected upstream while equation (4b) gives the calculated partial index (FPI_i^+) from elements affected downstream. The multiplicative factor $M_{up}(N)$ gives the upstream dependency modulating factor as a function of the distance N. Similarly the downstream dependency modulating factor is given by $M_{dn}(N)$. The sum of the upstream and downstream partial FPIs ($FPI_i^- + FPI_i^+$), gives the FPI of the element under consideration. In matrix form, equation (4) can be written as shown in equation (5). Equation (5) represents the Frobenius inner product of the Modulation Matrix and the Propagation Matrix

$$FPI_i^{\pm} \langle \begin{bmatrix} M_{up}(1) & M_{up}(2) \ldots M_{up}(MaxN) \\ M_{dn}(1) & M_{dn}(2) \ldots M_{dn}(MaxN) \end{bmatrix}, \begin{bmatrix} P_{up}(i,1) & P_{up}(i,2) \ldots P_{up}(i,MaxN) \\ P_{dn}(i,1) & P_{dn}(i,2) \ldots P_{dn}(i,MaxN) \end{bmatrix} \rangle \quad (5)$$

For compactness, equation (5) can be written as shown in equation (6) where M represents the Modulation Matrix and P represents the Propagation Matrix.

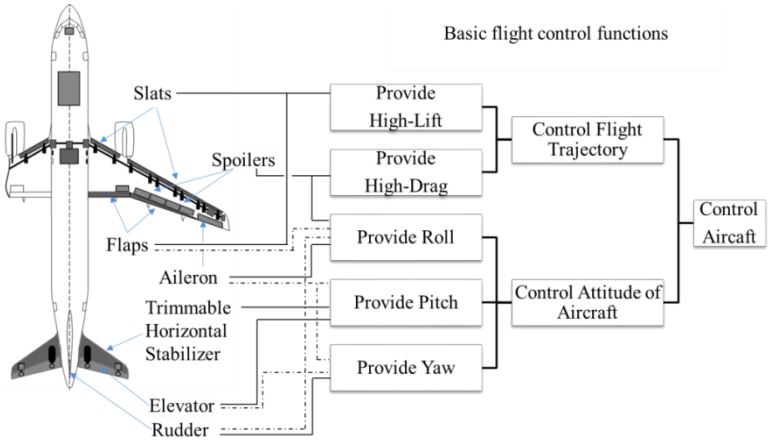
$$FPI_i^{\pm} = \langle M, P(i) \rangle \qquad (6)$$

For a tree with partitions (e.g. Figure 4), elements within the same partition can be modulated similarly while elements belonging to different partitions can be modulated differently. Such modulation is chosen to reflect potential impact of element failure on other elements (e.g. see application case in next section). In case of failure, the FPI of an element reflects the number of elements affected within the network structure of the functional model and the severity of impact. A high FPI value can be as a result of lots of affected elements with low severity or a few affected elements with high severity. Capturing this information early in the design process can be vital in optimal module formation within the function allocation stage or in making critical design decisions.

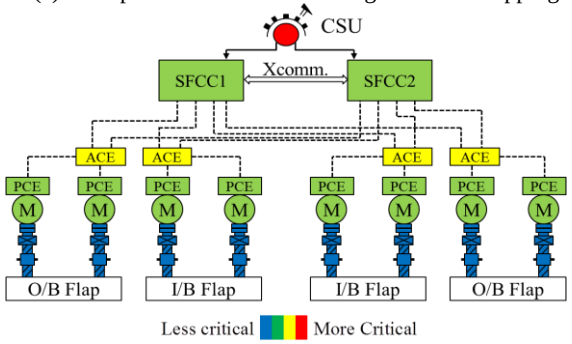
Note: The results of the analysis are influenced by the chosen values for edge (connection) strengths in the network and the modulation factors. Thus care must be taken in choosing these parameters and the resulting observations must be analyzed accordingly.

4 Application on a Multifunctional Flap Actuation Concept

Multifunctionality in flight control system presents many advantages for efficient flight which leads to reduction in fuel burn (Akoto Chama & Bertram, 2018; Akoto Chama, et al., 2017; Reckzeh, 2014; Cook & de Castro, 2004; Reckzeh, et al., 2012).



(a) Simplified multifunctional flight control mapping



(b) An exemplary multifunctional flight control flap actuation system (first two O/B and I/B flaps for the left wing and the last two for the right wing)

Figure 5. Multifunctional flight control surfaces and actuation system

ACE	: Actuator Control Electronics	O/B Flap	: Outboard Flap
CSU	: Command Sensor Unit	PCE	: Power Control Electronics
I/B Flap	: Inboard Flap	SFCC	: Slat/Flat Control Computer
M	: Motor	Xcomm	: Communication Signal

Figure 5(a) shows a simplified example of the mapping between the control surfaces on the aircraft (right) and flight control functions (left). The solid lines show the classical mapping while the dashed lines show possible functionalities that could be added to the control surfaces. The underlying actuation systems that actuate the control surfaces are very complex and present many design challenges. Thus, in order to demonstrate the proposed methodology, this paper analyses the functional network of the fully distributed flap actuation system concept (Recksiek, 2009) as an application. The physical layout and possible criticality distribution of the analyzed actuation system is shown in Figure 5(b). The design problem was to design a flap actuation system that allows the flaps to perform multiple functions such as increasing the maximum lift coefficient, spanwise lift distribution as well as roll assist. Applying the three step approach described above, a functional model was created composing of 140 interconnected elements. A DSM was then created and a functional failure propagation analysis was performed. Since it was

assumed that there was no information about the type of physical system solution, the analysis was based only on analyzing the functional network structure. Here the tree was partitioned into 2 sections as shown in Figure 4(a).

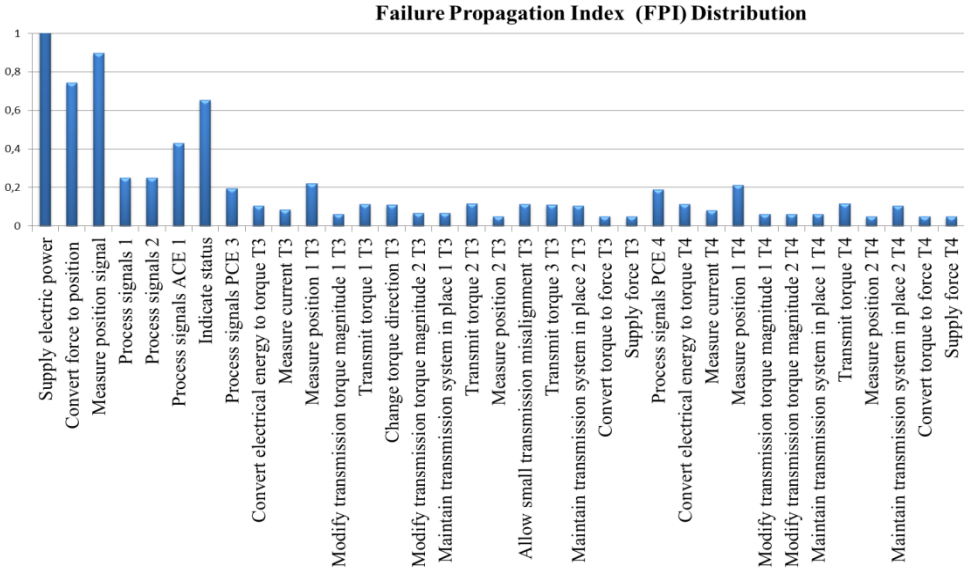


Figure 6. FPI distribution of a section of the functional architecture

The upper segment contained the failed element and elements that are directly affected by the failure without modulation. The lower segment contained elements that are indirectly affected by the failure with a distance dependent modulation of $M_{dn}(N) = 1/(2N)^2$ and $M_{up}(N) = 1/(4N)^2$ for the downstream and upstream elements respectively.

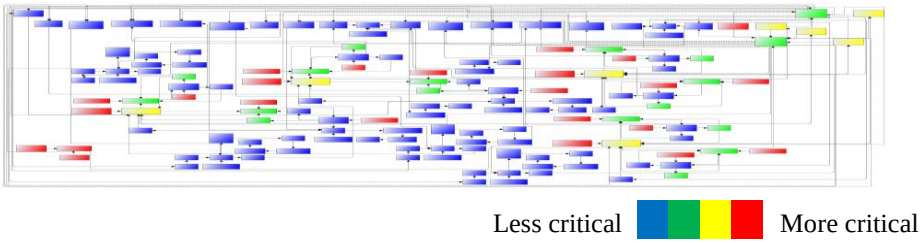


Figure 7 FPI color distribution of the complete functional model

These modulation factors were chosen in this way because it was assumed that the greater the distance between elements the lesser their dependency on each other and also that dependency for upstream elements reduces faster than that of downstream elements. For this work all connection strengths where chosen as unity for preliminary analysis and because no information was assumed for the technical solution of the functional model. Figure 6 shows a section of the FPI distribution for the elements in the model. For symmetry purposes, only a section of one wing of the entire architecture is shown. Figure 7 shows the color distribution of the complete functional model of the flap actuation

system. This color distribution was created according to the magnitude of the FPI generated using equation (4), with normalized distribution as follows: $Blue \leq 0.2$, $0.2 < Green \leq 0.4$, $0.4 < Yellow \leq 0.6$ and $0.6 < Red$. As expected, the distribution showed that more highly connected elements are more critical than less connected elements. Because the FPI of the electric power supply is extremely high, a potential early design decision would be to introduce a second power supply. Also, another enhancement decision could be to introduce redundant "Process Signals ACE" function due to the high FPI. The general observation made from the functional architecture is that highly connected elements with many downstream elements are more critical than those that are less connected with fewer downstream elements. Also functional elements with electrical inclined solutions (e.g. Supply Electric Power) which are highly connected have higher criticality values than those which are not (e.g. Measure Position 2 T4). On the other hand the two green boxes on the top right of Figure 7 represent the SFCCs, though highly connected, they are less critical because of redundancy. This equally shows the effect of redundancy using the FPI method.

4 Conclusion and Further Recommendations

Designing extremely large complex systems is a challenging task, especially when dealing with hundreds or thousands of interacting elements. This makes it difficult to identify high risk elements without prior knowledge in the design. As shown in this work, the Failure Propagation Index can therefore be used as a tool to help with the identification of such elements which may otherwise go unnoticed by the designer. If such elements are not identified early in the design process, this may lead to costly design changes or even catastrophic failures in the operational phase. The index formulation presented in this work serves as a systematic way to identify high risk elements in order to improve on the initial concept. The index can either be applied within the concept development phase, as shown for the functional model of the multifunctional actuation concept or for assessing existing design concepts. The FPI methodology uses segmentation of extremely large complex systems and modulation for modulating the failure as it is propagated within the network structure. The FPI method determines the internal impact of the element failure, by capturing its effect within a particular architecture network. With this method, only element connections, connection weights, and distance weights are needed to capture preliminary system element failure impact during concept generation. This aspect is especially useful for extremely large complex systems because of the huge challenges in capturing and processing their complex system behavior. Though this method can be used as a first step in understanding element network impact for extremely large complex systems, a possible enhancement could be by modifying the modulation factor to depend not only on the distance but also on the failed element. Another enhancement could be by introducing multiple connections of different types between system elements, which gives more detail to the functional network and thus, allows the possibility for further analysis on the system architecture. Nevertheless, as a first step in capturing element failure impact, the FPI method has been successfully demonstrated.

References

Akoto Chama, L., & Bertram, O. (2018). Identifying Enhancement Potentials of Actuation Systems Using a Criticality Index. 8th International Conference on Recent Advances in Aerospace Actuation Systems and Components. Toulouse, France: 8th International Conference on Recent Advances in Aerospace Actuation Systems and Components,INSA.

Akoto Chama, L., Bertram, O., & Schumann, H. (2017). Generation of Potential System Architectures by Applying a Stochastic Clustering Algorithm in the High-Lift Actuation Preliminary Design Process. 19th International dependency and structure modeling conference, DSM 2017. Espoo, Finland: 19th International Dependency and Structure Modeling Conference, DSM 2017.

Carlos Inaki, G. F. (1998). Intregration analysis of product architecture to support effective team co-location. Massachusetts: Massachusetts Institute of technology.

Chakrabarti, A., Shea, K., Stone, R., Cagan, J., Campbell, M., Hernandez, N. V., & Wood, K. L. (2011). Computer-Based Design Synthesis Research: An Overview. Journal of Computing and Information Science in Engineering, 11.

Clarkson, P. J., Simons, C., & Eckert, C. (2004). Predicting Change Propagation in Complex Design. Transactions of the ASME, Journal of Mechanical Engineering, 126, 788-797.

Clifton A, E. (2005). Hazard Analysis Techniques for System Safety. New Jersey: John Wiley & Sons, Inc.

Cook, M. V., & de Castro, H. V. (2004). The Longitudenal Flying Qualities of a Blended-Wing-Body Civil Transport Aircraft. The Aeronautical Journal, 75-84.

Dalton, J. (1996). Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment - ARP4761. Pennsylvania: SAE - International; The Engineering Society for Advanced Mobility Land Sea Air and Space.

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

Fang, C., & Marle, F. (2012). Dealing with Project Complexity by Matrix-Based Propagation Modelling for Project Risk Analysis. Journal of Engineering Design, Taylor & Francis.

Giffin, M., de Weck, O., Bounova, G., Keller, R., Eckert, C., & Clarkson, P. J. (2009). Change Propagation Analysis in Complex Techmical Systems. Transactions of the ASME, Journal of Mechanical Design, 131.

Hamraz, B., Caldwell, N. H., & Clarkson, P. J. (2012). A Multidomain Engineering Change Propagation Model to Support Uncertainty Reduction and Risk Management in Design . Transaction of the ASME, Journal of Mechanical Design, 134.

Hutcheson, R. S., McAdams, D. A., Stone, R. B., & Tumer, I. Y. (2007). Function-Based Systems Engineering (FUSE). Paris: International Conference on Engineering Design, ICE'07.

Marle, F. V.-A., & Bocquet, J.-C. (2010). Interaction-Based Risk Clustering Methodologies and Algorithms for Complex Project Management. International Journal of Production Economics, 142, 225-234.

Pahl, G., Beitz, W., Feldhusen, J., & Grote, K. H. (2007). Engineering Design, A Systematic Approach (Third Edition ed.). London: Springer-Verlag.

Recksiek, M. (2009). Advanced High Lift System Architecture with Distributed Electrical Flap Actuation. Workshop on Aviation System Technology. Hamburg: Technische Universität Hamburg-Harburg.

Reckzeh, D. (2014). Multifunctional Wing Moveables: Design of the A350XWB and the Way to the Future. 29th Congress of the International Council of the Aeronautical Sciences. St. Petersburg, Russia: ICAS.

Reckzeh, D., Bernhard, S., Andreani, L., & Sutcliffe, M. (2012). Patentnr. US 8,336,829 B2. United States of America.

Sobieszczanski-Sobieski, J., & Haftka, R. T. (1997). Multidisciplinary Aerospace Design Optimization Survey of Recent Developments. Springer-Verlag.

Stone, R. B., & Wood, K. L. (2000). Development of a Functional Basis for Design. Journal of Mechanical Engineering, 122, 359-369.

Thebeau, R. E. (2001). Knowledge management of system interfaces and interactions for product development. Massachusetts : Massachusetts Institute of Technology.

Tolga, K., Irem Y, T., & Jensen, D. C. (2010). A Functional Failure Reasoning Methodology for Evaluation of Conceptual System Architectures. Springer-Verlag, 209-234.

Contact: L. Akoto Chama, German Aerospace Center (DLR), Safety Critical Systems & Systems Engineering, Lilienthalplatz 7, 38108, Braunschweig, Germany, Tel: +49 531 295-2841, Fax: +49 531 295-2647, e-mail: leonel.akoto@dlr.de