AIRCRAFT MISSION AND SYSTEM FAILURE CONSIDERATIONS FOR FUNCTIONAL INDUCTION BASED CONCEPTUAL ARCHITECTURE DESIGN

Michael Armstrong, Dr. Elena Garcia, and Dr. Dimitri Mavris
Aerospace Systems Design Lab, Georgia Institute of Technology, Atlanta, GA

Keywords: *Requirements Emergence, Performance Degradation, Load Shedding*

Abstract

With current advances in system-level technologies, changes in system level aircraft requirements, and outsourcing of technology development, architecture innovation and integration have become driving differentiators between competing aircraft concepts. Revolutionary conceptual vehicle systems architectures promise additional benefits over incremental improvements achieved through technology insertion and system adaptation or evolution. However, exploration of the complex vehicle systems architecture design space introduces unique challenges in the definition and allocation of sizing critical unit and platform level requirements. Sizing critical performance requirements are infrequently derived from normal operating conditions but rather emerge from responses to system failures. This paper explores means for the identification and allocation of architecture specific off-nominal operating mode requirements through the extension of traditional hazard assessment tools, performance degradation optimization, and the propagation of function/criticality requirements through structured functional dependencies.

1 Introduction and Motivation

Current and future aerospace performance demands have increased the aerospace community's interest on enhanced vehicle systems optimization and integration. Electrical systems have been shown to provide potential for large increases in the efficiency of performance and maintenance. However, the application of high power, safety critical technologies in the aircraft subsystem architecture introduces interesting integration challenges, and requires a redefinition of the generally accepted and well understood systems relationships [21]. While much work has been done toward incremental improvement of individual technologies and subsystems, there is natural resistance to solve the problem at the whole aircraft level [4]. Complex systems design does not pose contained and well-formed problems but "messy, indeterminate situations [19]."

Next generation aircraft subsystem architecture concepts must integrate these promising technologies in order to achieve a maximum benefit. The architecture provides the framework for further development, regulates relationships between stakeholders, and manages the flow of requirements necessary to size each system and hardware. Therefore, adoption of the best subsystem architecture concept has a critical strategic importance.

In order for an architecture concept to be selected for further development, analysis must show that it proves superior to other conceptual architectural alternatives. The architecture alternatives must be sized and compared based on their effectiveness in fulfilling requirements.

As expressions from the intentional and behavioral domains, vehicle systems requirements must qualify the system's ability to achieve goals

$$\begin{array}{ll} \text{Min:} & \text{Platform Level Objective Function= } f_{Eval}(Unit_{Attr}) \\ \text{Unit}_{Attr} = \begin{pmatrix} Attr_{Unit1} \\ Attr_{Unit2} \\ \vdots \end{pmatrix} & \text{s.t.:} \quad P_{Hazard}(F) - P_{MaxLimit}(F) \leq 0 \\ \text{Load Alloc.} = \begin{pmatrix} FG1_{Alloc.} \\ FG2_{Alloc.} \\ \vdots \end{pmatrix} & \int_0^t Load_i(\tau)\, d\tau - E_{0_n} \leq 0, \qquad i = [1,n] \end{array} \tag{1}$$

and complete specified operations. However, the elicitation of sizing-critical requirements presents difficulties during non-conventional vehicle systems concept architecting. Best practices, axioms, and rules of thumb regarding the integrated sizing of high power electrical systems at the aircraft level are insufficient to warrant architecture selection. Increased component and platform complexity yields requirements which supervene due to complex behavioral relationships between the architecture's fundamental units. Many dominating requirements emerge through architecture specific sizing critical operating scenarios and unique performance degradation or load shedding strategies.

Performance requirements necessitated by exceptional operating states often prove more sizing critical than requirements imposed by the standard mission. Additionally, during architecture design, the relationship between failure causes and effects is often unclear [6]. Depending on the structure and relationships of the architecture, specific events may have vastly different operational effects at the platform level. Off-nominal scenarios performed under architecture specific load shedding strategies must be identified to predict maximum unit and system level requirements during architecture trades.

This paper explores operational emergent requirements by addressing behavioral complexity in terms of operating mode and safety/reliability. Tools and strategies are introduced which determine architecture specific performance degradation strategies during the identification and application of requirements concurrent to vehicle system concept generation and trades.

2 Vehicle Systems Emergent Requirements

Aircraft vehicle systems design can be posed as the optimization process depicted in equation 1. Designers configure the architecture by augmenting unit attributes ($Unit_{Attr}$) and allocating mission loads for each functional group (FG_{Alloc}) in a manner which can accomplish platform goals while minimizing some objective function (f_{eval} - cost, weight, etc). For this design problem, the objective function must take the form of vehicle system mission sizing, and the constraints act to limit the probability of operational hazards and ensure adequate energy on all storage elements.

Requirements definition traditionally precedes concept design and is primarily driven by designer and stakeholder intent. During the requirements definition process the "problem space [10]" is described in terms of the fulfillment of functions, the accomplishment of goals, and the solving of problems. These objectives are in turn translated into operational, functional, and physical requirements which drive concept definition.

Not all requirements, however, can be defined prior to system definition. Derived requirements cannot be specified by the stakeholder, but are the result of requirement decomposition and the application of expert knowledge and logical deduction [13, 15]. The application of domain knowledge is often sufficient for conventional design exercises. However, with the introduction of revolutionary architecture concepts, experience can fall short in the accurate prediction of unit level requirements.

Michael Sinnett, chief engineer of systems development for the Boeing 787 Dreamliner, spoke about the decision to change the cabin air pressurization method from engine bled to

electrically compressed. This single conceptual change to the aircraft architecture imposed multiple dramatic changes to the predefined or assumed relationships within the system. Sinnett said:

"When we decided on electric pressurization, it lowered aircraft empty weight 1,000-2,000 lb. and fuel burn was down several percent, but the numbers got muddied as the 787 got integrated. It's hard to say where the weight has gone [3]."

Requirements definition for revolutionary complex vehicle systems architecture is a process which can produce "counter-intuitive, seemingly acausal behavior full of unpredictable surprises [2]." As new technologies and advanced architectures are introduced, new requirements may appear which "cannot be fully explained mechanistically and functionally [8]" but require an understanding of the intent, purpose, and, to some degree, morality associated with the designs governing the derivation and application of a requirement. Ontologically, these requirements are emergent. They come into existence or become evident with specific architecture implementations.

Emergence occurs when the properties of the system or object can only be derived from the microstates or dynamics of parts of the system. These properties are not directly distinguishable from the structure property of the system/object or its parts and result from complex interactions between the parts. Flake describes emergence as "a property of a collection of simple subunits that comes about through the interactions of the subunits... Usually, the emergent behavior is unanticipated and cannot be directly deduced from lower-level behaviors [7]." Thus, emergent requirements can not be enumerated or quantified during the traditional requirements definition process, but are the result of complex behavioral relationships between units in specific architecture implementations.

Behavioral complexity of a vehicle systems architecture can be characterized in multiple dimensions: operating mode dependence, safety and reliability dependence, and time dependence [14]. Time and operating dependence are addressed here in the context of the aircraft mission. Additionally, designing for safety requires a complete understanding of the platform operations, consequences to functional failures, and means towards ensuring adequate reliability. Thus, safety and reliability considerations interact with mission sizing through the definition of off-nominal operations which typically dominate unit and system level requirements.

2.1 Mission Analysis

Time dependence plays a role in defining architecture requirements at multiple levels. Traditional high level aircraft platform conceptual designers, tasked with life cycle and mission analysis, apply timesteps on the order of minutes to decades. Conversely, unit and vehicle system developers must take a much finer time dependency perspective. To ensure adequate stability and power quality, power electronics and electric machine designers may consider switching and response rates on the order milliseconds or smaller. Therefore, time dependence relates to requirements emergence through multiple means.

Sizing is primarily carried out at the mission level. Here, requirements emerge which define the energy requirements of the system. Traditional mission analysis uses mission simulation to define energy storage in the form of fuel. The total block fuel requirement is the product of the integral of fuel flow throughout every likely sequence of operations. In considering the vehicle system, all energy storage requirements must be sized similarly. The amount of energy provided available from 'n' storage devices is constrained by the amount of energy available as seen in equation 2. $Load\,(\tau)$ represents mission loading and E_0 is the initial stored energy. The max energy required on the unit determines necessary mass and volumetric attributes.

$$\int_0^t Load_i\,(\tau)\,d\tau - E_{0_n} \leq 0, \quad i = [1,n] \tag{2}$$

The aircraft mission not only serves to define energy requirements for storage devices, it also

drives the magnitude of platform level requirements. An operating mode can be defined as a particular functioning condition or arrangement of a system. This includes the behavioral and physical state of a system designated in response to internal or external stimuli.

A fundamental understanding of the system level operations is critical to the identification of requirements. Requirement/specifications are derived from the behavioral domain [9]. Jacobson states, "The very first model of a complex system should be a model that describes the system, its environment, and how it and its environment are related... It should describe the system as it appears from the outside [12]." In order to determine accurate requirements, a robust understanding of the sizing critical operating conditions must be attained.

Traditional Scenario-Based Design and Model-Based Systems Engineering tools provide a framework for the definition of traditional operational scenarios. However, they fall short in addressing the emergence of requirements due to inadequate coverage. Rolland et. al. express the limitation of scenario based design techniques in providing sufficient "intentional coverage": including the capture of goal dependence, problem, responsibility, and cause. They write, "Intentional models are seldom included in scenario approaches... They are, so to speak, implicitly underlying the interfaces between the reengineering company and its environment [18]."

Furthermore, Allenby and Kelly provide more insight to these limitations. They state that "there is little guidance available for the systematic identification of either 'alternative paths' or 'exceptional courses' of events in scenario or use-case descriptions. Under these circumstances, the practitioner is left with little assurance of sufficient coverage [1]."

While ETOPS or one engine out at take-off may govern the attributes of some systems, the attributes of other units in the complex vehicle system may be more sensitive to other operational states. Deviations from the nominal mission pose sizing critical requirements on specific units [14]. As discussed earlier, requirements are directly sensitive to designer or stakeholder intent. The inability of the traditional systematic object based scenario identification tools to capture intent limits their ability to generate architecture specific emergent sizing critical scenarios.

At any point during the nominal mission there exists a probability that some deviation will occur due to internal or external changes in expected state (unit/system failure, weather, etc.). The aircraft behavioral response to this change in state represents a sequence of operating conditions branching from the nominal mission and arriving at a dissimilar final state. Furthermore, each deviation can exhibit additional changes to the internal or external state which again branch from the deviation branch. These deviations determine the form of the objective function seen in equation 1.

In addition to external relationships with the environment, the internal system relationships shape the significance of "exceptional courses" of events. The dominance of the requirements generated from each failure condition depends on the architecture implementation. Different vehicle systems architecture concepts potentially yield different paths which drive architecture requirements.

Ensuring adequate response to exceptional internal states is typically enforced through the imposition of reliability constraints. Enforcing these constraints and designing towards adequate safety requires a complete understanding of the reliability implications of each architecture architecture concept.

2.2 Safety and Reliability Requirements

In order to define the necessary reliability the designer must understand the operational impact of a failure on the environment. The detrimental impact of failures is expressed in terms of operational hazards. To specify safety requirements each hazard category assigns a probability limit to the operational effect. This is done to control risk ("the frequency of an occurrence and the associated level of hazard [22]"). Complete func-

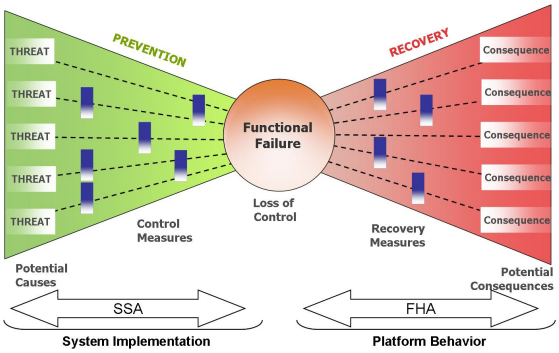


Fig. 1 Expanded Risk Bow-Tie for Functional Failures [23]

tional specification involves defining the magnitude of the the required action or capability with an associated level of reliability.

There are multiple means by which the designer can ensure that the appropriate reliability is achieved. This occurs through fault prevention or fault tolerance. Risk can be mitigated at the platform level through operational mitigation procedures. It can be additionally mitigated at the system level through "spatial and temporal redundancy [24]". Furthermore, risk can be mitigated at the equipment level by ensuring high unit reliability. This is illustrated in figure 1 . The right side of this bow-tie represents operational mitigation measures when some functional failure occurs, and the left side represents internal system controls which are implemented to minimize the occurrence of failure.

The traditional conceptual approach to aircraft hazard characterization maintains independence of the implementation and behavioral space through Functional Hazard Assessment (FHA) [22]. FHA is a systematic technique for exploring and classifying functional importance and the criticality of their impact on system operations by considering operational mitigation procedures. This process applies three guidewords in the evaluation of a function loss: loss of function, too much function, and incorrect operation of function [1]. The product of FHA is a tabular description of these discrete failure states and the associated criticality. This thereby fixes the reliability governing the fulfillment of the function. This can be expressed a constraint on the functional hazard where the probability of a given functional failure ($P_{Hazard}(F)$) cannot exceed the limit derived during FHA ($P_{Limit}(F)$).

$$P_{Hazard}(F) - P_{Limit}(F) \leq 0 \tag{3}$$

At the system level, spatial redundancy is achieved through the inclusion of multiple parallel elements capable of providing the same functionality. Temporal redundancy takes the form of replication or repair. Replication is sequential performance of some action and can achieve higher reliability in the performance of discrete task. Repair, on the other hand, is the restoration of some original capability. Total loss of thrust for a $\Delta t = 30$ seconds is much different than a total loss of thrust for $\Delta t = 10$ minutes. Allowing for engine restart can reduce hazard severity by reducing duration. With the inclusion of temporal redundancy for increased reliability, new architecture specific functions and operations must be introduced which enable functional restoration.

Following the characterization of functional hazards and system definition Preliminary System Safety Analysis is performed. This process validates that the defined architecture can meet the safety requirements as defined by the FHA, and establishes new safety related requirements. Additional requirements, like fail safe [5], further constrain system reliability by requiring that the loss of a single unit or connection must be assumed during fight regardless of probability. The traditional means of calculating system reliability is achieved by use of the Fault Tree and Reliability Block Diagrams. These object based tools facilitate PSSA by automatically structuring probability calculations.

System reliability is an emergent attribute. Complex behavioral attributes and relationships at the unit level determine the platform level reliability. Safety and reliability requirements originate from the operations domain and are allocated specifically to the architecture concept. These emergent requirements are imposed by the definition of necessary behavioral rules at the unit

$$\begin{array}{cc} \text{Min:} & \text{Hazard}= H_{op}(\mathbf{F}) \\ \mathbf{F}= \begin{pmatrix} fail\%_{unit1} \\ fail\%_{unit2} \\ \vdots \end{pmatrix} & \text{s.t.:} \begin{pmatrix} Req_{unit1} & 0 & 0 & \dots \\ 0 & Req_{unit2} & 0 & \dots \\ 0 & 0 & Req_{unit3} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} 1-fail\%_{unit1} \\ 1-fail\%_{unit2} \\ 1-fail\%_{unit3} \\ \vdots \end{pmatrix} \leq (1-fail\%_C)Cap_C \end{array} \quad (4)$$

level and mitigation at the system level to yield some advantageous platform level emergent behavior.

2.3 Load Shedding and Off-Nominal Operating Conditions

As discussed earlier, unit level requirements generated during off-nominal operating conditions typically prove more dominant than those applied during nominal operations even with a reduction in requirement magnitude in the presence of failure [14].

This is illustrated by aircraft vehicle systems sizing work done by Liscouët-Hanke [14]. Following a one engine or one generator failures, the peak steady state load requirement placed on the electrical machines increased approximately 15% during failure scenarios. This increased power requirement assumed a fixed load shedding strategy in the presence of these physical failures. During one generator failure the wing ice protection system (WIPS) reduced protection from anti-ice to de-ice. Additionally, during one engine failure, control loads were reduced by 50% and the environment control system functionality reduced to minimal airflow.

Load shedding, performance degradation, or demand response is the reduction of a functional requirement in the presence of adverse conditions. Load shedding attempts to reduce the maximum power required from the remaining systems by the removal of loads which are less critical to platform operations. This, thereby reduces the max load requirements from the remaining redundant devices. For electrical devices, shedding is managed by the electric load management system (ELMS) [17].

Shedding strategies must be updated when systems are modified. Hsu et. al. cite an inadequate load shedding strategy as the underlying cause for the catastrophic failure of the 1992 China Steel Corporation plant failure following plant modification and expansion [11]. With modifications to the vehicle systems architecture as necessitated by "more-electric" architecture concepts and concept trades, appropriate load shedding strategies must be identified which are architecture specific in order to appropriately predict the unit and system level requirements during off-nominal sizing cases.

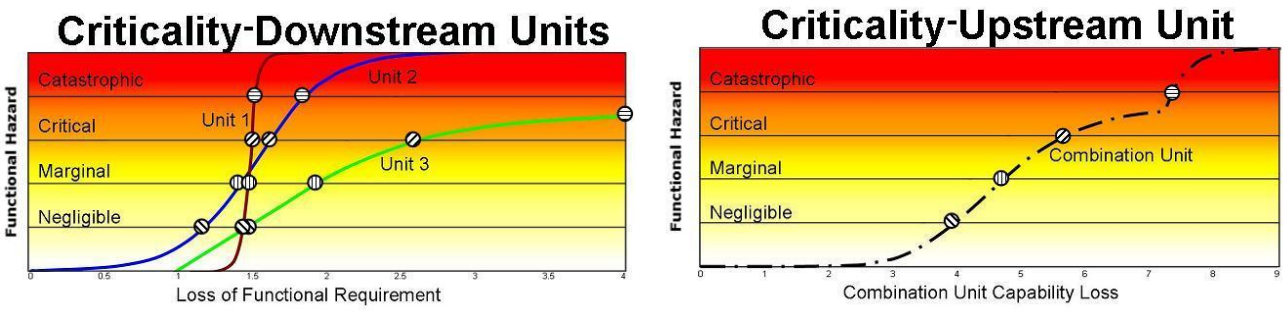
3 Optimal Load Shedding

Load shedding can be conceptualized as the minimization of operational hazards ($H_{op}(F)$) through intelligent functional degradation as depicted in equation 4. When multiple functional requirements are applied to an element or group of elements, a decision must be made as to which load requiring devices will lose support and to what degree following a loss in capability of the upstream unit ($1-fail\%_{unit1}$). The proportional loss of support is constrained by the energy available from the upstream unit.

$$\%loss_C(C_{crit}) = 1 - \frac{\sum_{i=1}^{n} max(Req_i)(1-\%loss_{Req_i}(U_{icrit}))}{Cap_C}$$

$$C_{crit}(\%loss_C) = \%loss_C^{-1}(C_{crit}) \quad (5)$$

Assuming that each element failure results in an independent effect at the systems level the associated criticality of the upstream unit becomes a min/max optimization problem. The level of hazard incurred from upstream loss coincides with equivalent hazards for each downstream % function loss. Generalizing this relationship yields equation 5, where $C_{crit}(\%loss_C)$ is the hazard associated with combining the requirements on the upstream unit.



(a) Downstream Units Function/Hazard Relationships

(b) Upstream Unit Function/Hazard Relationship

Fig. 2 'Combination' Hazard Relationship for Three Notional Downstream Units

Assuming that three units require steady state power (2 kW, 3 kW, and 4 kW respectively) from an upstream unit with a capacity of 9 kW. The functional hazard relationships for the downstream units are is given by a sigmoid function seen in figure 2a. By minimizing the criticality in a load shedding relationship, the criticality of upstream units can be directly determined as seen in figure 2b. The criticality of the loss of the upstream unit is determined by summing the magnitude of support lost for all downstream units at a specific level of hazard. Thus, a negligible hazard is seen with a loss of ≈4kW capability on the upstream unit by propagating the failure proportionally to the downstream units: negligible loss from unit 1 at ≈1.4kW, from unit 2 at ≈1.1kW, and from unit 2 ≈1.5kW ($-1.4kW - 1.1kW - 1.5kW = -4kW$). Thus, chart 2b is obtained by determining the load loss at which all downstream units incur given hazards as displayed in chart 2a.

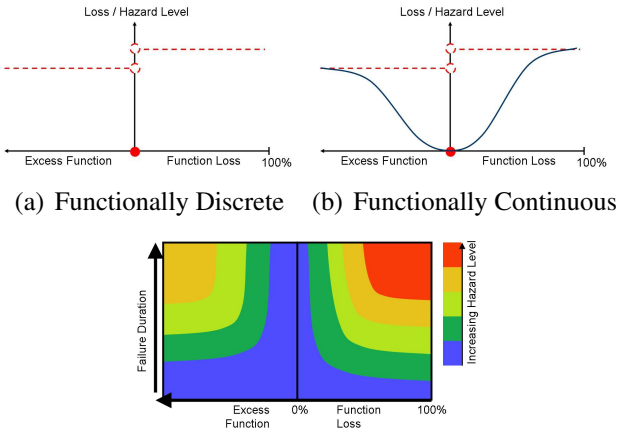
Propagating criticality requirements upstream from the platform level loads to the vehicle systems sources in the form of hazard functional relationships allows for the identification of unit level requirements which intrinsically include performance degradations considerations for specific off-nominal operational states.

3.1 Function/Hazard Relationship

In order to optimally shed loads, the relationship between function loss and operational hazard must be identified at the platform level. As discussed, the traditional FHA process has distinct limitations. Its discrete nature tends to define function/hazard relationships as seen in figure 3a. A step function of loss (adverse operational effect) in terms of deviation from the target (no failure) may be applicable for functions which take the form of discrete transactions (communication functions, actuate landing gear). However, load shedding infers a reduction in severity of effect through the elimination of functions and proportional function failure for units which can provide partial fulfillment of function.

Reliability is "the extension of quality into the time domain...[20]." Therefore, expansion of the hazard assessment methods requires expressing loss in terms of deviation from the target. To enhance the ability to optimize load shedding procedures, it is proposed that the FHA process be augmented to provide continuous relationships between operational hazard and magnitude of functional loss as notionally illustrated in figure 3b. Additionally, functional restoration has the ability to reduce the adverse effects of a failure by providing temporal redundancy. Therefore, function/hazard relationships must be defined as sensitive to failure duration as illustrated in figure 3c.

This relationship must be derived for each platform level function and combination of functions at the platform level. The hazard associated with any functional ($H_{op}(t)$) failure can be expressed as the maximum of the hazards associated with each platform level functional failure ($h_i(t)$) as shown in equation 6.



(a) Functionally Discrete (b) Functionally Continuous

(c) Continuous in Function and Duration

Fig. 3 Function/Hazard Objective Function for Load Shedding Optimization

$$H_{op}(t) = max[h_1(t), h_2(t), \cdots, h_{1,2}(t), \cdots] \quad (6)$$

$$h_i(t) = f(F_i, \tau, alt(t), M(t), dist(t), \cdots) \quad (7)$$

Each individual functional hazard relationship ($h_i(t)$) is a function of capability lost (F_i) and is scaled by the potential for recovery, as seen in equation 7. Recovery is expressed as a function of the duration of the functional failure (τ) and mission conditions (altitude, Mach number, distance from potential landing field, hazardous environments, ...). These conditions are time variant as the platform progresses throughout the mission. The operational effect of a loss in thrust for 30 seconds is much more hazardous during low altitude flight and takeoff than for higher altitude operations. A proportional loss of thrust which still yields excess power may prove catastrophic during obstacle clearance. However, a loss of thrust resulting in an inability to maintain steady level flight might be less hazardous during higher altitude operations.

Assuming independent functional hazards implies that $h_{i,j,\ldots} = 0$. Applying this assumption allows for a closed form solution of hazard in terms of upstream and downstream element attributes. However, in general, these relationships

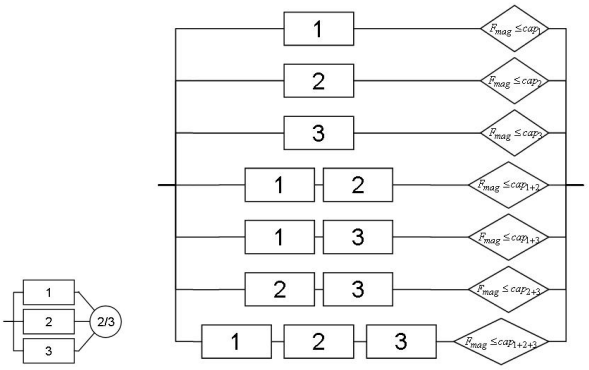


Fig. 4 Restructured Reliability Block Diagram for Proportional Load Sharing

may be developed through the optimization expressed in equation 5.

Expressing the probability constraint in terms of % functional failure significantly alters the means in which system reliability must be calculated to verify that these continuous constraints are met. Reliability must also be determined in terms of probability of proprotional functional losses. Based on traditional means, load sharing reliability is obtained through n-out-of-k relationships. In the case of proportional loading there is no assurance that a specific number of combined elements will provide sufficient functionality. In this case, the reliability of providing a functional requirement depends on the capacity of each element or combination of elements. Restructuring the reliability block diagram involves identifying all potential combinations and applying logic regarding the capability available from each parallel path as visualized in figure 4.

Assume three units with capacities of 3kW, 5kW, and 6kW with reliabilities of 0.8, 0.9, and 0.99 respectively. The maximum load sharing capacity is 14kW with decreasing reliability with increasing requirements. The reliability of this group of elements with respect to the magnitude of functional requirement is illustrated in figure 5. For requirements under 3kW any of the available systems may be used. Between 3 and 5kW, the units with 5 or 6kW devices must be operable. With requirements between 5 and 6kw, unit 3 can fulfill the requirements in isolation, or with the combination of the 3 and 5kW devices. For re-

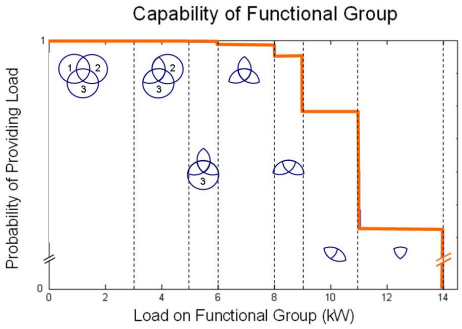


Fig. 5 Degradation of Reliability with Varying Magnitude of Functional Requirement for a Three Unit Load Sharing Group

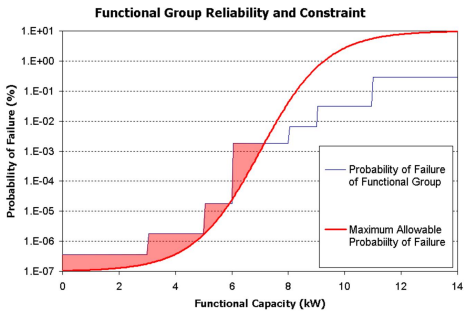


Fig. 6 Load Sharing Reliability with Criticality Constraint

quired capacities above 6kW, combinations of elements must be used to fulfill functional requirements.

A breech in the reliability constraint can occur at any magnitude of functional failure. Figure 6 shows the notional three unit shared load reliability superimposed on a maximum probability allowed as defined through continuous FHA. As seen in this figure, the system is less likely to fail in providing low levels of capability. However, providing minimal power requirements is also more stringently constrained. In this example insufficient reliability is achieved for highly critical low power requirements while adequate reliability is provided for power requirements exceeding ≈7kW. In this circumstance overrating individual units proves insufficient to providing adequate reliability at low power requirements. Solutions in this case may include the introduction of additional redundant systems, or increasing the reliability of one or more of the existing units.

This approach to hazard identification and assessment allows the conceptual designer to determine criticality associated with proportional unit failures considering architecture specific optimal load shedding strategies. Additionally, when architectures prove insufficient in meeting reliability requirements, visually inspecting the relationship between the unit reliability and constraint in this continuous fashion provides insight and motivation towards providing solutions to reliability problems (redundancy, overrating, functional restoration, increased unit reliability).

3.2 Criticality Propagation

Formulating load shedding optimization requires a detailed understanding of how functional requirements flow throughout a system. Every point in the architecture where multiple units present load requirements to a single unit or group of units necessitates the prioritization of downstream units. When generating concept architectures these points must be systematically identified with sufficient information to format function/hazard relationships for upstream systems in terms of unique shedding strategies.

Function/hazard information must be made available at all points in the architecture where these shedding decisions must be made. Additionally, all unit level continuous functional/reliability requirements must be traceable to the support of platform level functions and operations in light of optimal performance degradation strategies.

Complex unit interactions and highly interdependent structures of aircraft vehicle systems architectures pose difficulty in the traditional hierarchical flow-down of functional and reliability requirements. Therefore, a systematic means for the management of architecture relationships in the communication of requirements is necessary. This is achieved through Functional Induction.

Functional dependency relationships communicate requirements from the platform to each individual unit or groups of units. Functional induction is used to manage the implementation

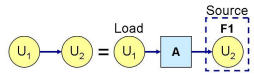
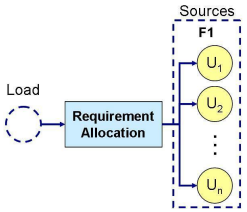
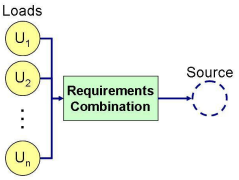
space of concept definition by requiring the specification of all dependent relationships between elements [16]. Definition of architecture implementation follows function definition. The first set of functions is provided from the operational description of the platform. These architecture independent functions are termed boundary functions. Subsequent functions are introduced following architecture implementation definition. Each decision introduces additional functions which must be fulfilled. Internal system functional relationships are termed induced functions. Redundant units providing the same functionality are termed functional groups. Defining the system through the assignment of unit dependencies provides the structure for propagating criticality throughout the architecture.

The result of system definition following functional induction is a directed graph representing the communication of requirements through functional relationships. These directed graphs use edges to communicate requirements (load, hazard) upstream and capability (reliability) downstream between nodes. Three specific types of node elements are used to propagate function hazard relationships: combination, allocation, and simple. A combination element is instantiated when multiple loads feed into a source element. An allocation element is instantiated when multiple source units can provide for requirements communicated by a single edge load (these sources form a functional group). Simple element represents a single unit providing a load to be fulfilled by another single unit. These three relationships are graphically displayed in table 1. In this table the yellow circle represents a unit, the dashed blue circle represents some undefined upstream unit or group of units, and the dashed box represents a functional group (group of elements providing the same functionality).

$$Ucrit_i(\%loss_i) = Acrit\left((\%loss_i - k_i)\frac{Cap_{Ui}}{max(Req_A)}\right) \quad (8)$$

$$k_i = \frac{\left(\sum_{j=1}^{n} Cap_{Uj}\right) - max(Req_A)}{Cap_{Ui}}$$

Table 1 Convention for Unit Requirements Relationships Relationship Types

Type	Diagram
Simple	
Allocation	
Combination	

The combination relationship was introduced before with equation 4 and generalized for independent function/hazard relationships in equation 5. The allocation/load-sharing relationship is given in equation 8. In this expression $Ucrit_i(\%loss_i)$ is the hazard failure relationship, $Acrit(\%loss_A)$ is the hazard function of the allocation element, Cap_{Ui} is the capacity of unit i, n is the number of upstream units, and $max(Req_A)$ is the maximum requirement generated from the downstream element through the allocation element. The general equation propagating criticality requirements upstream through a simple relationship is the same as for an allocation elements with one upstream unit (equation 8, $n = 1$).

Equations 5 and 8 act to propagate the function/hazard relationship through all unit functional interdependencies. Assuming that upstream element failures of a given duration impose a loss of function support of all downstream units for the same duration, these equations follow the same form but capture sensitivity to loss duration: $Ucrit_i(\%loss_i, \tau)$ and $C_{crit}(\%losses, \tau)$.

Systematically identifying the criticality requirements for individual units by considering graphical interactions enhances the architects ability to identify architecture specific operational requirements concurrent to architec-

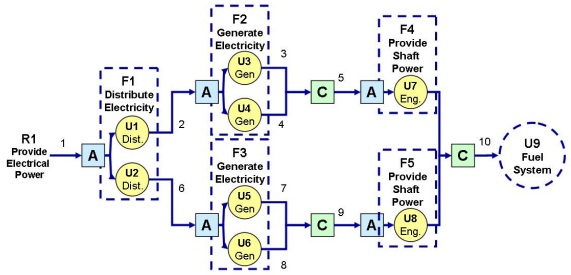


Fig. 7 Combination-Allocation Relationship for Notional System Providing Electrical Power

ture definition. This graph propagates function/hazard relationships throughout to all system elements by way of combination and allocation relationships. Each function/hazard curve acts to constrain the physical and behavioral attributes of the units according to the criticality of the functionality it provides. Once these relationships are in place, the variation in load and criticality requirements during a mission may be determined as the boundary level function/hazard relationship varies in time. Extending these relationships into the fault duration domain will also enhance the ability of the vehicle systems designer to visually inspect the benefits to temporal or spatial redundancy solutions, when reliability constraints are breeched.

3.3 Complex Allocation-Combination Relationships

As discussed in the previous sections, redundant, load-sharing relationships reduce the necessity to provide capability and reliability with a single unit. However, with complex graphs, subsequent upstream relationships may necessitate that information be made available from all downstream functional dependencies. These relationships are affected by the complexity of the system graph.

Consider the notional example displayed in figure 7. The hazard associated with the upstream Unit 9 (Fuel System) must be expressed as the combination of multiple downstream elements all supporting a similar allocation element. With total loss of U9, R1 (provide electrical power) cannot be fulfilled. Therefore, the U9 failure/hazard curve cannot be calculated directly as a function of the adjacent unit criticality. Structural information must propagate upstream all the way from the boundary requirement.

Requirements and criticality communicated through each of the edges in this directed graph must carry information regarding requirement origin and augmentation. Edge tags for the figure above are displayed in table 2. In this table, the allocation relationship is indicated by triangular brackets: e.g. $\left\langle \frac{U_i}{U1,U2,\cdots} \right\rangle$. Combinations are displayed with comma separated and parenthesized elements or allocations. Edges which stem from units in an allocation relationship are tagged by the proportion of the downstream requirement (in this case R1) provided by the unit. In order to fully characterize the sources of criticality for upstream units, criticality elements sum the requirements being received from downstream.

Table 2 Information Communicated with Graph Edges from Figure 7

Edge	Requirement Proportion
1	R_1
2	$\frac{1}{\eta_1} R_1 \left\langle \frac{U1}{U1,U2} \right\rangle$
3	$\frac{1}{\eta_1\eta_3} R_1 \left\langle \frac{U1}{U1,U2} \right\rangle \left\langle \frac{U3}{U3,U4} \right\rangle$
4	$\frac{1}{\eta_1\eta_4} R_1 \left\langle \frac{U1}{U1,U2} \right\rangle \left\langle \frac{U4}{U3,U4} \right\rangle$
5	$\frac{1}{\eta_1} R_1 \left\langle \frac{U1}{U1,U2} \right\rangle \mid \left(\frac{1}{\eta_3} \left\langle \frac{U3}{U3,U4} \right\rangle, \frac{1}{\eta_4} \left\langle \frac{U4}{U3,U4} \right\rangle \right)$
6	$\frac{1}{\eta_2} R_1 \left\langle \frac{U2}{U1,U2} \right\rangle$
7	$\frac{1}{\eta_2\eta_5} R_1 \left\langle \frac{U2}{U1,U2} \right\rangle \left\langle \frac{U5}{U5,U6} \right\rangle$
8	$\frac{1}{\eta_2\eta_6} R_1 \left\langle \frac{U2}{U1,U2} \right\rangle \left\langle \frac{U6}{U5,U6} \right\rangle$
9	$\frac{1}{\eta_2} R_1 \left\langle \frac{U2}{U1,U2} \right\rangle \mid \left(\frac{1}{\eta_5} \left\langle \frac{U5}{U5,U6} \right\rangle, \frac{1}{\eta_6} \left\langle \frac{U6}{U5,U6} \right\rangle \right)$
10	$R_1 \mid \left(\begin{array}{l} \frac{1}{\eta_1\eta_3\eta_7} \left\langle \frac{U1}{U1,U2} \right\rangle \left\langle \frac{U3}{U3,U4} \right\rangle, \frac{1}{\eta_1\eta_4\eta_7} \left\langle \frac{U1}{U1,U2} \right\rangle \left\langle \frac{U4}{U3,U4} \right\rangle, \\ \frac{1}{\eta_2\eta_5\eta_8} \left\langle \frac{U2}{U1,U2} \right\rangle \left\langle \frac{U5}{U5,U6} \right\rangle, \frac{1}{\eta_2\eta_6\eta_8} \left\langle \frac{U2}{U1,U2} \right\rangle \left\langle \frac{U6}{U5,U6} \right\rangle \end{array} \right)$

For allocation-combination graphs efficiency information must be taken into account while considering optimal load shedding. Assuming paths are shed in order of efficiency (least efficient to most efficient) the slope of the function/hazard relationship will sequentially increase as the shed parallel paths increase in efficiency. Graph tags, therefore, include information regarding the efficiency of the paths. The parenthesized groupings of elements seen in table 2 indicate that the associated criticality curve

(R_1 in the case of edge 10) must be reformed with regards to the capability and efficiencies of the parallel unit paths.

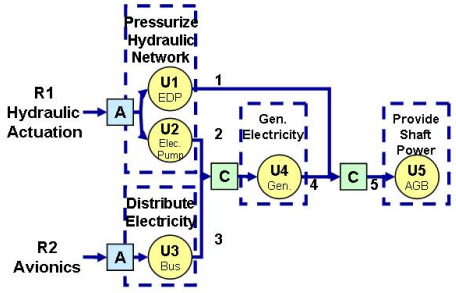
Looking at combination elements in this example, the criticalities of engines U7 and U8 are derived through an efficiency scaled simple relationship with the buses U1 and U2 respectively. Additionally, the criticality of the fuel system (U9) receiving edge 10 can be expressed as an efficiency adjusted simple relationship with the original boundary requirement to provide power R1. With total loss at U9 the requirement, R1, cannot be fulfilled.

Decomposing and propagating unit criticality in this fashion imposes reliability constraints which limit the capacity and reliability of each unit depending on its specific functional dependencies. These reliability constraints are defined with respect to architecture specific load shedding strategies generated by hazard minimization for every combination relationship which consider the support of the ultimate downstream functionality.

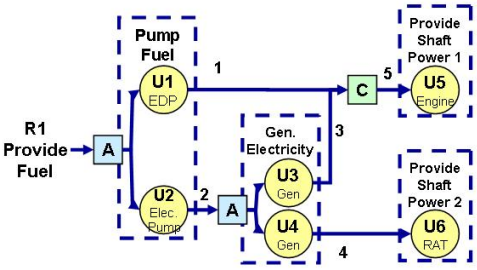
3.4 Staggered Combinations and Allocations

Load shedding optimization is further complicated when multiple boundary functions, combinations, and allocations interact simultaneously. Two staggered relationships are displayed in figure 8. In the staggered combination situation (figure 8a), U5 supports both requirements R1 and R2. However, multiple combinations are imposed. The staggered allocation relationship (figure 8b) presents an issue of combining portions of a downstream requirement which can be fulfilled by multiple sources following multiple allocations.

Applying the notation introduced in the previous section assists in propagating requirements. This notation and decomposition is applied here for the staggered combination graph. For illustrations sake linear function/hazard relationships for the boundary requirements are assumed. This assumption is not a requirement to apply this criticality propagation but is employed to simplify the visualization of the effect of allocation and



(a) Staggered Combinations

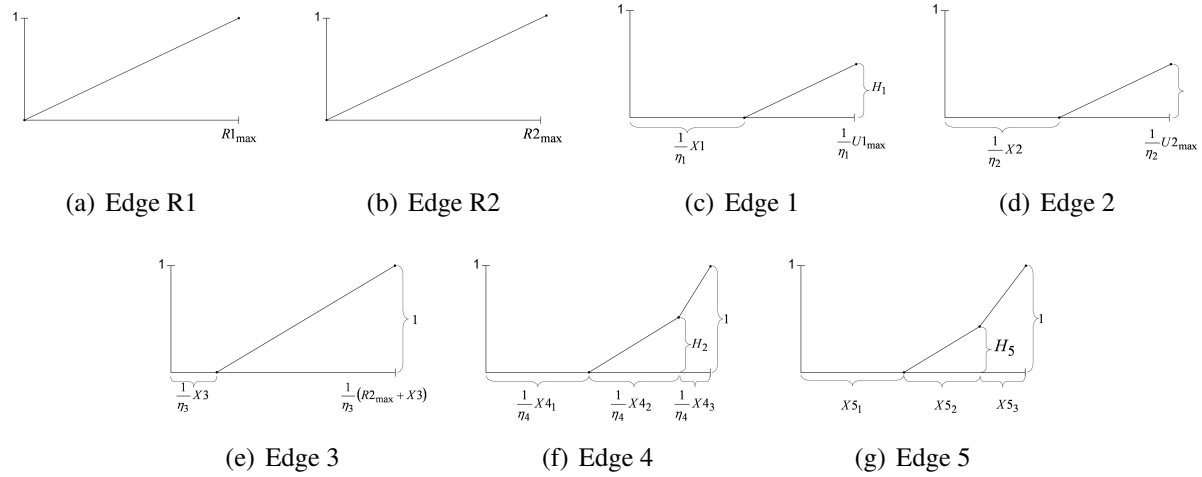


(b) Staggered Allocations

Fig. 8 Requirements Propagation with Complex Allocations and Combinations

combination relationships. Unit efficiencies are also assumed constant for this example. The criticality relationships for each of the graph edges are displayed in figure 9. The horizontal axis of these graphs represents the magnitude of capability loss of the upstream element connected by the edge. The vertical axis represents the normalized criticality (catastrophic hazard =1, no effect=0). Associated allocation-combination notation and calculated graph notations are given in table 3.

Assuming a linear relationship between function and hazard for the boundary requirements yields figure 9a and b. The loss of ability to support requirement 1 or 2 (R1, R2) yields catastrophic consequences. Edges 1 and 2 come from the allocation element upstream of R1. As shown in figure 9 c and d, loss of functionality of each redundant unit yields no hazardous effect until a threshold has been crossed. This threshold is defined by the overall capacity of the functional group. Additionally, total failure of one of the units does not mean loss of functional capability. The max hazard incurred by each independent unit failure corresponds to the capacity of the element with regard to the total functional re-



(a) Edge R1 (b) Edge R2 (c) Edge 1 (d) Edge 2

(e) Edge 3 (f) Edge 4 (g) Edge 5

Fig. 9 Function/Hazard Relationships for Edges of the Staggered Combination Graph Depicted in Figure 8a.

quirements.

Edge 3 maintains a linear relationship with a catastrophic failure for 100% loss of the upstream unit. However, this criticality is offset by the overrating of U3 and scaled by U3 efficiency.

Calculating the criticality of requirements communicated through edge 4 begins to address optimal load shedding. No hazard is seen with failures of units upstream of U4 until all overrated capability has been lost from U2, U3, and U4. The first linear increase in hazard occurs with with simultaneous failure through U2 and U3 until the max hazard for U2 loss has be seen. The steeper linear section occurs once U2 has lost all functional support and R1 has lost all possible capability through U4 failure. Therefore, this second section represents loss to R1.

Edge 5 has 4 linear sections. The first is a constant offset which includes the overrating associated with the path R2-U3-U4 and the maximum available overrating from R1-U1 or R1-U2-U4. The second section includes load shedding for the least efficient path from U1 to U5 and the path from U2 to U5. Once load has been shed from the least efficient path, the third section represents proportional losses through the more efficient path.

Characterizing the system in terms of a directed graph through functional induction relationships between elements allows criticality relationships to be propagated throughout a com-

Table 3 Propagation of Function/Hazard Relationship for the Edges in Figure 8a.

	Equations
9c.	$Notation: \frac{1}{\eta 1}R_1\left\langle\frac{U_1}{U_1,U_2}\right\rangle$ $X_1 = U1_{max} + U2_{max} - R1_{max}$ $H_1 = H_{R_1}(U1_{max})$
9d.	$Notation: \frac{1}{\eta 2}R_1\left\langle\frac{U_2}{U_1,U_2}\right\rangle$ $X_2 = U1_{max} + U2_{max} - R1_{max}$ $H_2 = H_{R_1}(U2_{max})$
9e.	$Notation: \frac{1}{\eta_3}R_1$ $X_3 = U3_{max} - R2_{max}$
9f.	$Notation: \frac{1}{\eta 4}\left(\frac{1}{\eta 2}R_1\left\langle\frac{U_2}{U_1,U_2}\right\rangle, \frac{1}{\eta 3}R_2\right)$ $X_{4_1} = U4_{max} - \frac{1}{\eta_2}(U2_{max} - X_2) - \frac{1}{\eta_3}(U3_{max} - X_3)$ $X_{4_2} = \frac{1}{\eta_2}U2_{max} - \frac{1}{\eta_2}X_2$ $X_{4_3} = \frac{1}{\eta_3}R3_{max} - \left[R_3(H2) - \frac{1}{\eta_3}X_3\right]$
9g.	$Notation: \frac{1}{\eta 4}\left(\frac{1}{\eta 1}R_1\left\langle\frac{U_1}{U_1,U_2}\right\rangle, \frac{1}{\eta 2}R_1\left\langle\frac{U_2}{U_1,U_2}\right\rangle, \frac{1}{\eta 3}R_2\right)$ $X_{5_1} = \max\left(\frac{1}{\eta_1}, \frac{1}{\eta_2\eta_3}\right)X_1 + \frac{1}{\eta_3\eta_4}X_3$ $X_{5_2} = \left\{\begin{array}{ll}\frac{1}{\eta_1} \le \frac{1}{\eta_2\eta_4}: & \frac{1}{\eta_1}U1_{max} - \frac{1}{\eta_1}X_1 + R_3(H_1) \\ o.w.: & \frac{1}{\eta_2\eta_4}U2_{max} - \frac{1}{\eta_2\eta_4}X_1 + R_3(H_2)\end{array}\right\}$ $X_{5_3} = \left\{\begin{array}{ll}\frac{1}{\eta_1} \le \frac{1}{\eta_2\eta_4}: & \frac{1}{\eta_2\eta_4}U2_{max} - \frac{1}{\eta_2\eta_4}X_2 + [R_3(H_1+H_2) - R_3(H_1)] \\ o.w.: & \frac{1}{\eta_1}U1_{max} - \frac{1}{\eta_1}X_1 + [R_3(H_1+H_2) - R_3(H_2)]\end{array}\right\}$ $H_5 = \left\{\begin{array}{ll}\frac{1}{\eta_1} \le \frac{1}{\eta_2\eta_4}: & H_1 \\ o.w.: & H_2\end{array}\right\}$

First column in reference to the graph displayed in figure 9

plex system through unit interdependencies. Supplying information regarding downstream graphical relationships to the upstream load providers allows complicated relationships to be reduced in terms of their impact on the ultimate provision of some capability demand expressed at the platform level. Propagating this information throughout the system is necessary in order to optimize load shedding for each combination relationship.

While calculations for this example do not extend into the time domain, these graphs can represent the projection of the hazard curve for a given failure duration (τ).

Additionally, with more complex unit requirement propagation (i.e. a requirement criticality coming out of a unit has a nonlinear relationship with incoming requirement criticality) downstream $\%loss$ must be expressed as a function of upstream $\%loss$. Therefore, to fully characterize this continuous relationship future work will explore the use of surrogate models in defining the efficiencies as a function of magnitude of requirements and other environment conditions.

4 Conclusion

Reconsidering the system optimization in equation 1, performance degradation considerations effect the architecture design by manipulation of the design constraints. Probability constraints at the unit level must consider off-nominal operating modes unique to each architecture concept. Requirements emerge in the form of sizing critical off-nominal load shedding strategies which must be optimized to minimize probability of hazard. Additionally, failure conditions pose unique energy requirements to architecture units during architecture sizing. As concept trades are performed, these emergent requirements must be identified and applied to justify architecture selection.

Designers must identify the relationship between operational hazards and the magnitude of functional requirements in the context of the platform mission. The application of fixed reliability constraints generated by FHA's traditional assumptions regarding failure states is remedied in this work by expressing hazards as a continuous relationship with the magnitude and duration of functional failure and other mission parameters. Continuous functional hazard relationships provide the objective function for the definition of requirements in terms of architecture specific performance degradation strategies. While traditional conceptual design methods make assumptions regarding the shedding of loads for vehicle system sizing, requirements are generated here which intrinsically involve optimal performance degradation through load shedding optimization.

In order to define optimal load shedding strategies, these continuous reliability/capacity constraints must be communicated to all points in the system where load shedding is feasible. Functional Induction is utilized for architecture specification (graph definition). Means were introduced which catalog complex relationships between the boundary and unit requirements and track requirements through functional interdependencies. Combination and allocation elements were introduced to manage graph complexity and logically determine optimal load shedding. Thus, the systematic identification of optimal shedding strategies is achieved through propagating function/hazard relationships throughout a system following functional dependencies and then generating upstream requirements through the minimization of hazards at all combination relationships.

With the basic framework in place, future work includes the automation of function/hazard relationship generation during graph construction. These relationships must be updated to included additional dimensions; fault duration and mission conditions. Assumptions regarding unit efficiency and the independence of platform function hazards will also be addressed.

Systematic definition of off-nominal requirements is necessary to accurately predict unit and platform level attributes. The tools and methods discussed in this paper represent initial steps in the identification and propagation of emergent off-nominal sizing requirements during the concept development of complex vehicle systems.

5 Copyright Statement

References

[1] K. Allenby and T. Kelly. Deriving safety requirements using scenarios. *Rolls-Royce PLC-Report-PNR*, 2001.

[2] J.L. Casti. On system complexity: Identification, measurement and management. *Complexity, Language and Life: Mathematical Approaches*, 16:146–173, 1986.

[3] Michael A. Dornheim. Boeing 787 technology: Massive 787 electrical system pressurizes cabin. *Aviation Week and Space Technology*, 2005.

[4] Lester Faleiro. Power optimized aircraft to change industry mindset. *Interavia Business and Technology*, 2002.

[5] Federal Aviation Administration. Advisory Circular 25.1309-1A, 1988.

[6] P. Fenelon, JA McDermid, M. Nicolson, and DJ Pumfrey. Towards integrated safety analysis and design. *ACM SIGAPP Applied Computing Review*, 2(1):21–32, 1994.

[7] G. Flake. Review of the computational beauty of nature. *AI Magazine*, 21(2), 2000.

[8] S. Funtowicz and J.R. Ravetz. Emergent complex systems. *Futures*, 26(6):568–582, 1994.

[9] D. Harel and A. Pneuli. On the development of reactive systems. *Logics and Models of Concurrent Systems*, pages 477 – 498, 1985.

[10] D.C. Hays. *Requirements analysis: from business views to architecture*. Prentice Hall, 2003.

[11] CT Hsu, CS Chen, and JK Chen. The load-shedding scheme design for an integrated steel-making cogeneration facility. *IEEE Transactions on Industry Applications*, 33(3):586–592, 1997.

[12] I. Jacobson. The use-case construct in object-oriented software engineering. *Scenario-based design: envisioning work and technology in system development*, pages 309–336, 1995.

[13] J. Lin, M.S. Fox, and T. Bilgic. A requirement ontology for engineering design. *Concurrent Engineering*, 4(3):279, 1996.

[14] Susan Liscouët-Hanke. *A Model-Based Methodology for Integrated Preliminary Sizing and Analysis of Aircraft Power System Architectures*. PhD thesis, Université de Toulouse, 2008.

[15] U. Lösch, J. Dugdale, and Y. Demazeau. Requirements for supporting individual human creativity in the design domain. *Entertainment Computing–ICEC 2009*, pages 210–215.

[16] D. Mavris, C. de Tenorio, and M. Armstrong. Methodology for aircraft system architecture definition. In *46th AIAA Aerospace Sciences Meeting and Exhibit*. AIAA, 2008.

[17] I. Moir and A.G. Seabridge. *Aircraft systems: Mecanical, Electrical, and Avionics Subsystems Integration*. AIAA, 2008.

[18] C. Rolland, C. Ben Achour, C. Cauvet, J. Ralyté, A. Sutcliffe, N. Maiden, M. Jarke, P. Haumer, K. Pohl, E. Dubois, et al. A proposal for a scenario classification framework. *Requirements Engineering*, 3(1):23–47, 1998.

[19] Schön, D.A. *Educating the reflective practitioner*. Jossey-Bass San Francisco, 1987.

[20] D.J. Smith. *Reliability, maintainability and risk: practical methods for engineers*. Butterworth-Heinemann, 2005.

[21] Vincent P. Socci. System design considerations for vehicle-based mobile electric power applications. In *Power Electronic Technology 2005/Session PET06*, 2005.

[22] Society of Automotive Engineers. ARP 4754: Certification considerations for highly-integrated or complex aircraft systems, 1996.

[23] J. Talbot and M. Jakeman. *Security risk management body of knowledge*. Wiley, 2009.

[24] I-Ling Yen, Raymond Paul, and Kinji Mori. Toward integrated methods for high-assurance systems. *Computer*, 31(4):34, 1998.