



Facility Robustness: Applying Aerospace Safety Assessment Techniques to Facility Functional Resilience

Authors:

Ann Berner, Integrated Renewable Energy Senior Analyst, has over 25 years of design and analysis experience working with commercial jet transports, much of it involving accident prevention and safety analysis. She holds a bachelor's degree in Aeronautics and Astronautics from MIT.

Gary Kuhlman, Associate with Kuhlman Consulting, has over 30 years in the service, maintenance and construction of mechanical systems in commercial and healthcare facilities, focused on system reliability, quality and safety.

1 Background

In the 21st century, the built environment faces multiple environmental and physical threats and hazards, some of which have always existed and some of which are new. At the same time, human-built facilities are more likely than ever to support life critical functions, or to be required to offer security, shelter, or other safety functions to their occupants. All these challenges are being faced while increasingly efficient use of energy is required. While techniques exist to evaluate critical performance of some types of systems (such as automobiles, airplanes, nuclear power, patient care, and communications), to date there is no agreed-upon comprehensive methodology to evaluate a facility design for its ability to meet functional resilience requirements.

This white paper proposes to address this problem by adapting and applying existing System Safety Assessment (SSA) techniques currently used in the aerospace industry to evaluate airplane, system, and component designs in terms of relevant safety requirements. In order to provide functional resilience, facilities need to meet requirements for integrity and reliability, and hazards need to be minimized. In this paper, these characteristics are collectively referred to as the "robustness" of the facility.

1.1 Threat environment

A facility which is required to perform critical functions where the loss or erroneous operation of those functions could result in loss of life is subject to threats and hazards which can compromise its operation. Examples of such facilities include hospitals, nursing care facilities, power plants, government command centers, large gathering places (sports stadiums,

conference centers, etc.), schools and universities, and commercial facilities which house critical functions (communications centers for 911 services, etc.). Operation of such facilities can be affected by fire, natural disasters such as flood, wind, earthquakes, terrorism, sabotage, hardware failures, software and hardware design errors, or human error (construction, operation, or maintenance). Understanding these threats and hazards and evaluating the design against them as it evolves would help to ensure that the facility's robustness to them is maximized at minimum cost.

1.2 Facility dependencies

Critical facilities have always been dependent upon certain external infrastructures and functions, including provision of water and power, pharmacy and equipment supply, food, etc. Today, however, other dependencies are emerging as well, including off-site third party data storage for patient records and medical references, internet access, and communications with professionals who may be off-site. The method being proposed in this paper will allow analysts to account for such dependencies in evaluating facility robustness.

1.3 Applying Aerospace SSA Process to Facility Design

This paper proposes an approach to facility robustness through design assessment. Specifically, the paper describes an adaptation of proven safety assessment techniques from the aerospace industry. These techniques are detailed in SAE ARP4754 and SAE ARP4761. A previous adaptation of these techniques to Critical Control Point Patient Care is documented in "Proactive Hazard Analysis and Health Care Policy", by John E. McDonough of ECRI (reference 8). The core principles of the SAE defined safety assessment techniques have been preserved, in order to ensure completeness, thoroughness, and technical rigor. However, the examples and recommendations used in this paper have been developed specifically to address facility design.

These techniques will help designers achieve and demonstrate compliance with Executive Orders 13327, 13423 and 13514, and Energy Independence and Security Act 431, by enabling a qualitative and quantitative understanding of functional performance and resilience of various facility designs, implementations, operational schema. This will allow selection of designs which are functionally resilient, perform as required, and also comply with mandated energy requirements.

1.4 Tailoring the Approach

Appropriate tailoring of the process is required in order to ensure it is executable for the variety of needed applications, from new designs, to remodeling activities and maintenance of existing facilities. Similarly, options for scalability are described. These allow the techniques to be



applied to only certain functions, certain subsystems, or to a portion of a facility, allowing the user to optimize the analysis according to specific needs.

2 Proposed approach

2.1 Functional Hazard Assessment (analogous to ARP4761 FHA)

The first step in the process is the Functional Hazard Assessment (FHA). The FHA identifies which functions performed by the facility (or external functions upon which the facility depends) support life criticality. For all functions, the FHA will identify the severity of hazards which result when the function is lost or operates erroneously.

2.1.1 Identify functions (provide electrical power, environmental systems, provide medical gases, horizontal & vertical transportation, etc.)

The scope of the desired project will drive which functions are considered. For a “life criticality” assessment, only those functions generally considered life critical will be considered. A more comprehensive analysis may study a variety of functions which have less importance. Note that for broad functions such as provision of electrical power, it is helpful to divide the function into a life critical subcomponent and a non-critical component. This may allow savings as part of the function can be implemented at lower levels of robustness.

It is important that all functions relevant to the analysis are identified at the outset. Participants across architectural and engineering disciplines should be encouraged to identify applicable functions.

Possible life critical functions which should be considered include:

- Provision of Electrical Power
- Provision of backup mechanical and electrical systems
- Environmental control
- Provision of water
- Provision of Medical Gases
- Horizontal Transportation
- Vertical Transportation
- Laboratory Services
- Equipment Sterilization

Other functions to consider:

- Security and access control functions
- Occupant capacity
- Delivery of specific supplies required to perform critical
- Access to electronic records
- Access to medical references
- Laboratories

- Internet access
- IT Technology
- Sewage
- Solid Waste
- Hazardous Waste
- Roads and Paths
- Fire and Rescue Services
- Police
- Food
- Trans

2.1.2 Identify functional failure modes (loss of function, erroneous function)

For each function determined to be in the scope of the analysis, identify all of its functional failure modes. In general these failure modes, at a minimum, comprise “loss of function” and “erroneous function”. Loss of function failure modes are those for which the function is no longer available. For example, the provision for operating theater space pressure control, a loss of function failure mode is “failure of ventilation system resulting in loss of pressure control”. Similarly, an erroneous function failure mode is one where the function is performed incorrectly. For provision of pressurization, an example of an erroneous function failure mode is negative operating theater pressure resulting in infiltration of contaminants. Note that there may be other types of failure modes. For example, partial loss of pressurization is a failure mode that must be considered; however it is not really loss of function, nor is it erroneous function. Similarly, it is often valuable to consider whether the failure modes of some functions should be evaluated differently depending on whether warning is provided that the hazard has occurred or is about to occur. For example, if primary ventilation fails but a backup is in place and warning is provided, staff will have time to reconfigure or make corrections in order to avoid a ventilation loss. However, if the warning fails, primary ventilation could be lost and no corrective action taken, leaving the operating theater vulnerable to a complete ventilation loss should the backup fail. For this reason, consider whether to evaluate some functional failure modes “without warning” separate from those “with warning”.

It is important at this stage of the analysis to evaluate functions only. How those functions are implemented should not be taken into account. Evaluating the failure modes of the functions in the abstract ensures completeness. For example, “loss of electrical power” is a functional failure mode, whereas, “fuel leak in diesel generator” is a hardware failure mode of particular implementation (these are assessed later in the process).

2.1.3 Describe “building-level” effects of functional failure modes

For every identified functional failure mode, describe how it affects the facility. Use enough detail to allow determination of how severe the hazard may be. Describe how the operation of the facility will be compromised or limited. Be specific about possible fatalities, increased risk of injury or disease to facility occupants or to others who may be depending upon life critical functions being performed in the facility. List expected damage to the building, making quantified assessments as agreed to by the analysis participants.

2.1.4 Categorize functional failure modes by severity

In the modern aerospace industry, it is accepted practice for regulators, manufacturers, and operators to apply the following principals for determining acceptable probabilities of occurrence for hazards:

- 1) It is not possible to completely eliminate risk; therefore, every hazard has some non-zero probability of occurrence.
- 2) Current operations are, for the most part, at acceptable levels of safety from society's point of view. That is, current data can be used as a rough benchmark for setting goals for probability of occurrence. This point is qualified with the expectation that we are always striving to make an already safe system safer as time goes on.
- 3) More severe hazards should have lower probabilities of occurrence. That is, the probability of a hazard must be *commensurate* with its severity.

These same principals can and should be applied to facility design. Descriptions of severity levels and a mapping of severity to probabilities of occurrence was published by the VA National Center for Patient Safety (NCPS) presentation (reference 3) . Definitions of severity along these lines should be developed for application to analysis of facility robustness and functional resilience.:

Table 1:VA NCPS HAZARD SEVERITIES

Category	Consequences
Catastrophic (FMA rating 10)	<ul style="list-style-type: none"> One or more fatalities among occupants Equipment or facility damage equal to or greater than \$250,000
Major (FMA rating 7)	<ul style="list-style-type: none"> Multiple injuries or hospitalization of occupants Equipment or facility damage equal to or greater than \$100,000
Moderate (FMA rating 4)	<ul style="list-style-type: none"> Injury or hospitalization of an occupant. Equipment or facility damage more than \$10,000 and less than \$100,000
Minor (FMA rating 1)	<ul style="list-style-type: none"> No injuries or hospitalization of occupants Equipment or facility damage less than \$10,000 or loss of utility without adverse patent outcome

Probability Rating (Reference 3)

- Frequently – likely to occur immediately or within a short period of time (at least one time per year)
- Occasionally – probably will occur (occurs more frequently than once every 2 years, but less frequently than once every year.)
- Uncommon – possible to occur (occurs more frequently than once every 5 years, but less frequently than once every 2 years.)
- Remote – unlikely to occur (occurs less frequently than once every 5 years)

The scorecard below presents a method for weighting functional failure modes in order to give greater attention to hazards which are more severe and which occur more frequently.

Table 2: VA NCPS Hazard Score Card Matrix (Reference 3)

Probability	Severity			
	Catastrophic	Major	Moderate	Minor
Frequent	16	12	8	4
Occasional	12	9	6	3
Uncommon	8	6	4	2
Remote	4	3	2	1

2.2 Assess vulnerabilities of the facility, implementation, or design which is being assessed (analogous to ARP4761 Failure Modes and Effects Analysis (FMEA))

All electrical, mechanical, and structural components can fail in such a way that they contribute to loss of function or erroneous function for the systems they support. Some of these failures have no effect on the facility in terms of leading to hazards, some result in hazards all on their own, but most result in hazards only under certain circumstances or in the presence of other failures. In order to quantify probabilities of occurrence for hazards, the failure rates of these components are needed.

2.2.1 System by system, component by component, evaluate which failures can reasonably occur

For each major component (including complex electronics, computers, as well as mechanical, electrical, and plumbing components) list the random hardware failures which apply. For complex devices it is helpful to create functional groupings as the effects of individual component failures may be difficult, if not impossible, to discern. References 4 and 5 (RiAC parts reliability databases) can be very helpful in identifying specific failure modes for various types of components.

2.2.2 For each component failure, assess the effects at the building or facility level; and, if possible, quantify failure rates.

In order to apply the FMEA methodology to facility robustness, a combination of the above patient care format with the FMEA format called out in Reference 1 is suggested. The required elements are listed below. Reference data or SME knowledge should be used to develop the detailed FMEA. For each component, the following items must be determined:

- 1) Failure modes:
 - a. These can be determined from references 4 and 5 for components covered by those documents, and from SME knowledge for other components or structural elements.
 - b. For each failure mode develop a narrative description of its effects (alone or in the presence of certain conditions or other failures) on the subsystem and/or overall facility.
- 2) Failure Rate for each failure mode:

- a. Failure rates should be expressed as number of failures per calendar hour (as opposed to operational hour); this is because environmental conditions can lead to failures even when a component isn't operating.
 - b. RiAC documents have failure rate data for applicable components. Failure rates may need to be adapted for the appropriate environment (per Mil-Hbk 217). In addition, total failure rates may need to be broken down by failure mode; RiAC failure mode distribution data can help with this issue.
 - c. Historical facility component, system and subsystem total failure rate data and failure mode information can be used to assess risk areas.
- 3) Exposure time: this is the number of hours (statistical mean) the failure can be expected to be present before it is found. Exposure time is determined by operational factors if the failure is annunciated, by detection time if it is detected by monitoring, voting, or testing, and by maintenance intervals if it is detected by maintenance activities.
- 4) Weighting Factor from Score Card Matrix: The purpose of the hazard analysis is to develop a list of hazards that are of such significance that they are reasonably likely to cause partial or complete system failure resulting in loss of life, injury or property damage. The Hazard Score Card Matrix weighting factors accounts for the severity of the failure and likely reoccurring frequency of the define failure. Limited funds and personnel necessitate prioritizing hazards from most to least impact to life and property prior to expending resources to define and evaluate subordinate component/ process failures contributing to the Failure Mode.

2.3 Perform Common Cause Assessment

Some failures or threats compromise design features such as redundancy, separation, or partitioning by having affects in multiple parts of the facility or its supporting systems. An assessment of the likelihood of these “common causes” can be performed to ensure they are sufficiently improbable. A Common Cause Assessment (CCA) (or Common Mode Assessment, CMA) is a qualitative assessment of how expected threats may affect a design, including how they may compromise features intended to provide robustness. Its results are used to make informed design decisions about which threat scenarios will impact the facility's operation.

2.3.1 Identify Survivability and Performance Requirements

The first step in a CCA is to identify what functionality must be preserved against threats. Using the FHA, identify which functions must be preserved and to what degree they must still be

operable, or how quickly they must be restored.

2.3.2 Develop a threat list

The first step of the CCA is to identify the types of threats which will be considered. Types of threats to consider include:

- Inadequate or deferred maintenance
- Reliability of evolving sustainability technology
- Redundancy capability
- Erroneous function
- Terrorism
- Disparate and obsolete equipment and systems
- Staff capability
- Funding
- Fire
- Earthquake
- Flood
- Wind
- Hardware failures
- Software and hardware design errors
- Production or construction flaws
- External source faults

2.3.3 For each threat, evaluate the impact on the facility

Once requirements and threats have been identified, the effects of each threat are evaluated and documented in tabular or narrative form. Recommendations on design changes may be included, but what's most important is that there is clarity about which threats pose the biggest problems in terms of facility operation so that operational plans can account for them.

2.4 Qualitative and Quantitative (probabilistic) assessment of hazards and their consequences (analogous to ARP4761 Fault Tree Analysis)

2.4.1 Identify applicable TLEs (top level events)

From the FHA (using the hazard scorecard matrix), identify which functional hazards have weighting factors high enough that a detailed evaluation of their probability of occurrence should be made. This is an area that should be tailored for each project. That is, the TLEs should be chosen by the design team in order to best support the design process without wasting time evaluating events which aren't severe enough to warrant the analysis.

2.4.2 Fault Tree Analysis

First developed for the nuclear power industry, Fault Tree Analysis (FTA) is the technique of representing failures in complex designs and computing their likelihood. These trees provide a representation of relationships among individual component and system failures using Boolean logic ('and' gates and 'or' gates), known maintenance intervals, and the failure rates and exposure times documented in the system FMEA. In general, a Fault Tree should be developed

for each TLE which is severe enough that the base reliability rate for the system doesn't support the required probability of occurrence for that hazard.

Fault Tree Analysis is usually the most difficult and time consuming part of any aerospace safety assessment, and is likely to be the same way in assessing facility robustness. Significant SME (subject matter expert) involvement is required in order to assure all relevant relationships among individual failures are captured.

2.5 Assess potential mitigations and their effectiveness against the most probable and severe hazards

2.5.1 Dissimilarity

The principal of dissimilarity provides powerful mitigation against known and unknown hazards. When functions are implemented using dissimilar hardware, software, or technology type, the overall design is protected against failures and threats which apply only to one type. For example, if a relay is controlled by software, a virus or software design error can result in erroneous operation of the relay. If it is also controlled by an independent hardware-only sensor, however, those threats are mitigated by dissimilarity.

In aerospace, dissimilarity is frequently employed in one of several ways:

- 1) By implementing critical functions using hydraulic power, electrical power, and/or mechanical controls (flight controls, landing gear, etc)
- 2) By implementing backup modes which bypass highly complex computers
- 3) By designing key systems twice, using independent design teams.

2.5.2 Redundancy

By far the most common mitigation, redundancy is an effective method for moderating the effects of random hardware component failures. In facility designs, critical systems such as power and water are often implemented with a redundant design, either with designation of N+1 or 1+1. N+1 identifies a stand-by system with an automated or manual changeover capability which is used upon primary failure. The designation "1+1" is for redundant systems operating simultaneously, often including independent external sources.

2.5.3 Integrity

Hazard mitigation can be "built into" a facility through high-integrity design techniques for construction, hardware, and software. High integrity designs have very low rates of design error, and hence the hazards which can result from such errors are unlikely to occur. In assessing how design errors can contribute to hazards, it is helpful to look at hardware and software design for each system and/or major component. The more severe are the hazards

which design errors can produce, the more rigorous a design process is required.

Integrity is built in by the use of rigorous processes which include detailed design reviews, tight configuration control, and in-depth documentation. RTCA documents DO-178b (reference 6) and DO-254 (reference 7) provide guidance on how to implement high-integrity design processes. No analogous scheme exists for facility development, so part of any hazard assessment is determining which hardware and software design techniques will be used, and where to use the most rigorous techniques.

2.5.4 Reliability

Parts or components which have high reliability provide mitigation against hazards (particularly against lower severity types of hazards) simply by making a failure sufficiently unlikely to be commensurate with the severity of the hazard.

2.5.5 Partitioning and Fortification

For threats which result in physical damage, or for critical functions where it is important to retain some functionality, or where failures can cascade through a facility, the design may need to incorporate partitioning (physical barriers which ensure that failures or damage in one partition cannot affect the functioning of another partition) or fortification (physical protection of a portion of a facility or system). Note that partitioning and fortification can be implemented at any level, from the overall facility design, to distribution of functions within buildings, to design of a particular subsystem such as electrical, plumbing, or security.

2.6 Assemble all component analyses into overall facility assessment

Review the entire analysis to ensure all hazards have been addressed and quantified probabilities of occurrence are numerically and analytically consistent with the reliability and failure rate estimates which drive them. Have appropriate SMEs assess fault trees to ensure they are logically coherent and quantitatively correct.

If any fault trees were built, a summary table should be included of TLEs and their probability of occurrence.

Finally, summarize any findings where design changes are warranted, or where specific trade studies should be conducted in order to make key design decisions.

3 Potential Incorporation Approaches

The techniques described in this paper can be applied during various phases of a facility's life cycle. Some techniques, such as applying design rigor to ensure desired levels of hardware or software integrity, can only be fully applied at the time of original construction, but qualitative

and quantitative assessments can be used to ensure upgrades and remodels best mitigate against severe/likely hazards, and to implement appropriate maintenance and monitoring even when no facility changes are planned.

Funding, disruption to ongoing operations (including occupants, staff, and the public), are challenges when upgrading any infrastructure. When a facility analysis identifies deficiencies, obsolete equipment, critical systems which need upgrades or significant design changes in order to address identified hazards, there is no one right way to implement the needed changes. New construction, renovation, system upgrades and ongoing maintenance are all possible avenues to get these changes incorporated. . Non-new construction approach to upgrading systems and correct defined deficiencies in an existing building may be the best use of scarce funding. The analysis will identify problems and severity of the deficiency, but decision-makers then need to factor this information into construction or upgrade plans, subject to available funding.

3.1 Ground up new development

New construction of a state-of-the-art facility, whether standalone or connected to an existing center, provides a facility that meets current safety and construction standards, incorporates sustainability measures and provides critical system redundancy improving overall infrastructure reliability and functional resilience.

Applying a facility analysis to new construction is fairly straight forward in terms of the analysis itself, since there is flexibility in how the design will be implemented. In this case, however, schedule presents a big challenge. The assessment must be performed simultaneously with the top level and detailed design work. Otherwise the results will come too late in the process to influence the design. It's important that the analysis is performed as early as possible, and that design SMEs are involved in reviewing the results.

3.2 Identify strongest potential improvements/interventions and perform a dedicated remodel

The facility assessment identifies and ranks system deficiencies and gaps in system functionality providing managers an overview of system condition and risk. Available funding for capital projects will drive the development of project scope ranging from replacing a high risk component to a system upgrade. The infrastructure evaluation provides facility and risk managers information to assist with annual capital budgeting and long term planning. The interdependency of various systems may dictate that defined failure points, equipment problems and system upgrades be bundled as a single project for logistic and capital funding purposes.

3.3 Incorporate improvements into regular facility improvement schedule

For an existing facility with no planned major remodel, the results of the facility assessment can still be useful. Ongoing maintenance work, component replacement, and facility operation can all be used to make improvements in the facility's robustness to a variety of threats. An example is the identification of a single point failure at a relay or junction box which could be eliminated with a simple wiring change.

The facility assessment will find some items which are operational issues and can be corrected by the facility engineering group and/or service provider. The identified issues could be related to staffing, maintenance processes, operational procedures and pending component failures. The ranking of the failure points will assist the facilities group with prioritizing annual corrective work and provide supporting documentation for the annual operational budget process and long range planning.

4 Conclusion

Applying an adapted and tailored version of established System Safety Analysis techniques can provide facility planners and developers with robust designs which maximize efficiency by identifying an optimal design early in the design process. These same principles are also well suited to analyze existing facilities when renovations are planned or review of maintenance and staffing practices are being conducted. The key to Facilities Robustness lies in timely and appropriate application of the methods and techniques outlined in this paper by qualified experts and decision makers.

5 References

1. SAE ARP 4754, Certification Considerations for Highly-Integrated Or Complex Aircraft Systems
2. SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
3. "The Basics of Healthcare Failure Mode and Effect Analysis", United States Veterans' Affairs Center for Patient Safety
4. RiAC Nonelectronic Parts Reliability Database
5. RiAC Electronic Parts Reliability Database
6. RTCA DO-178b, Software Considerations in Airborne Systems and Equipment Certification
7. RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware



8. "Proactive Hazard Analysis and Health Care Policy", by John E. McDonough of ECRI.

6 About the Authors

Ann Berner has over 25 years of design and analysis experience working with commercial jet transports, much of it involving accident prevention and safety analysis. She holds a bachelor's degree in Aeronautics and Astronautics from MIT.

Gary Kuhlman has over 30 years in the service, maintenance and construction of mechanical systems in commercial and healthcare facilities, focused on system reliability, quality and safety.