Development of a Regulatory-Based Safety Analysis Framework for Unmanned Aircraft Systems

Ahmet Oztekin\textsuperscript{1} and Cynthia Flass,\textsuperscript{2}
\textit{Hi-Tec Systems, Egg Harbor Twp, NJ, 08234, USA}

Xiaogong Lee\textsuperscript{3}
\textit{FAA, William J. Hughes Technical Center, Atlantic City Airport, NJ, 08405, USA}

and

Stefan Keller\textsuperscript{4}
\textit{FJ Leonelli Group, Waxhaw, NC, 28173, USA}

This paper presents a regulatory-based system-level approach to analyze the safety impact of introducing a new technology, such as unmanned aircraft systems, into the National Airspace System (NAS). The proposed framework applies the International Civil Aviation Organization (ICAO) sanctioned safety management system (SMS) principles with a particular focus on safety risk management (SRM) and safety assurance. A qualitative framework based on identifying risk controls using existing aviation rules and regulations is presented. This approach provides a systematic process to identify systems-level hazards and causal factors. It outlines a methodology to determine a safety baseline for conducting operations in the NAS.

\section{I. Introduction}

Unmanned Aircraft Systems (UAS) emerge as a viable, operational technology for potential civil and commercial applications in the National Airspace System (NAS). Although this new type of aircraft presents great potential, it also introduces a need for a thorough inquiry into its safety impact on the NAS as it will fundamentally transform aviation and its public perception. In this context, assessing the safety impact of UAS on current manned operations in the NAS will provide valuable insight on future integration of UAS into the NAS.

The research outlined in this paper presents a systems-level approach to analyze the safety impact of introducing a new technology, such as UAS, into the NAS utilizing Safety Management Systems (SMS) principles.

The primary objectives of this study are:

1) To develop a technically sound safety analysis approach for implementing Safety Management Systems (SMS) to address the integration of UAS into the NAS.

2) To provide a proof-of-concept study for the developed methodology.

\section{II. Approach}

It has been widely argued that the lack of regulations is the limiting factor against the fulfillment of the demand for unrestricted civil UAS operations in the NAS\textsuperscript{1}\textsuperscript{-3}. Notwithstanding the need for UAS specific regulations, safety concerns, or rather lack of understanding of all safety aspects, associated with future civil UAS operations are the major barrier to unrestricted, routine UAS operations in the NAS. Therefore, this study relies on the premise that understanding the safety impact of proposed UAS operations is the prerequisite to properly regulate future integration of UAS into the NAS.

\footnotesize{\textsuperscript{1} Operations Research Analyst, Hi-Tec/FAA WJHTC, Adv. A/C Sys & Avionics, AJP-6362, AIAA member.}
\footnotesize{\textsuperscript{2} Computer Scientist, Hi-Tec/FAA WJHTC, Adv. A/C Sys & Avionics, AJP-6362.}
\footnotesize{\textsuperscript{3} Manager, Structures and Avionics R&D Division, AJP-6360, FAA WJHTC.}
\footnotesize{\textsuperscript{4} Consultant, FJ Leonelli Group.}

American Institute of Aeronautics and Astronautics

Copyright © 2011 by the American Institute of Aeronautics and Astronautics, Inc. The U.S. Government has a royalty-free license to exercise all rights under the copyright claimed herein for Governmental purposes. All other rights are reserved by the copyright owner.
In order to regulate a new technology, such as UAS, without risking stifling its potential, one needs to understand existing safety criteria required to conduct safe operations. Within the context of the NAS, the existing safety criteria are the applicable aviation rules and regulations governing everyday manned flight and flight support and management operations of commercial or non-commercial nature. Aviation rules and regulations act as controls against potential risks and provide a baseline for safe operations in the NAS. More specifically, regulations are risk controls that constitute a safety baseline for all operations in the NAS. Thus, an inquiry on the regulations will provide an understanding on the current risk controls and the safety baseline.

All aircraft operating in the NAS has to satisfy requirements set by Title 14 Code of Federal Aviation Regulations (14 CFR). In that sense, 14 CFR provides the risk controls for safe operations and establishes a baseline for all prospective operation in the NAS. Understanding the risk controls as defined by the 14 CFR and outlining a safety baseline in accordance with these risk controls lie at the crux of the study presented in this paper. This study can be utilized to identify a safety baseline using 14 CFR. It introduces an approach that can be used to gain an in-depth understanding on the current safety architecture of the NAS. The proposed framework can also be applied to study the integration of any new technology into the NAS.

Another important aspect of prospective UAS operations in the NAS is the lack of pertinent historical operational data required to apply conventional uncertainty analysis techniques on the emerging operations and on their interaction with the NAS. Probabilistic Risk Analysis methodologies are extremely popular among safety analysts to successfully model and quantify uncertainty associated with various high-risk systems. On the other hand, probabilistic risk analysis relies on quantitative tools and techniques to model and evaluate the system in question. The available data on emerging UAS operations is mostly fragmented. Some data exist on military UAS operations, but dissemination of such data for the purposes of civil/commercial studies are restricted due to its sensitive nature. Since the availability of the data on emerging UAS operations is limited, it is very difficult to perform a systems-level safety analysis of UAS using conventional quantitative safety analysis methodologies.

In this context, a new approach is needed to study the safety impact of emerging UAS operations on NAS. This new approach should not rely on historic data about the new technology. Furthermore, it should also assume a systems-level perspective while performing the safety analysis. We believe that a successful attempt to understand the safety impact of emerging UAS operations of civil/commercial nature can only be achieved through a higher, systems-level approach, which takes into account the problem domain as a whole. In this case, the problem domain in question is the NAS and it should be treated as a single complex system. Sub-systems, such as ATC, Airmen, Aircraft, Flight Operations, and Airspace constituting the NAS are interdependent and their interactions determine safety that permeates the whole system and defines minimum mandatory safety requirements for the NAS.

The defining aspect of this study is its systems-level approach to safety analysis. Traditionally, safety of a system is evaluated or quantified based on the analysis of related historical accident and incident data. However, as discussed above, such data-centric methodologies present a challenge when applied to emerging technologies. Data-centric methodologies benefit from inductive reasoning when modeling the problem domain and the system in question. Although inductive reasoning has been successfully employed for data-rich systems for which extensive collections of case-studies exist, inductive frameworks are not a good fit to understand and model new technology with limited accident/incident data.

This study adopts an approach to the problem at hand so that the limited availability of data for civil UAS operations would not hinder our efforts to fully develop a technically sound safety analysis methodology. Thus, this study adopts deductive reasoning to understand the problem domain. Deductive reasoning is a top-down approach, which puts emphasis on modeling the system based on its higher and more general components. When applied to the area of safety analysis, contrary to inductive approach where the analysis would be based on individual accident/incident cases and related data, a deductive approach will study the system as a whole and focus on its higher-level components and their interactions. Thus, a deductive approach will concentrate on understanding the safety minimums and, using an engineering term, determine the boundary conditions for conducting safe operations within the system. These boundary conditions or safety minimums apply to every seemingly independent subcomponent of the larger system, thereby constituting a safety baseline.

III. Methodology

A. Regulatory-Based Causal Factor Framework

The safety baseline concept lies at the crux of the proposed framework. Following a deductive approach, it studies the system to determine risk controls. Based on the risk controls a mandatory safety baseline is then populated. Specifically, the proposed framework uses existing regulatory structure for civil aviation as risk controls. It presents a methodology to identify hazards that are regulated by the risk controls, i.e., regulations. Following the
fundamental premises: methodology. In very broad terms, RCFF is a qualitative, systems-level approach to safety assessment based on deductive perspective, for each hazard underlying causal facts are determined. A safety baseline is populated using the identified causal factors and hazards. Consequently, potentially related causal factors underlying separate hazards governed by different risk controls are linked to construct an interconnected safety baseline. Linkages identified within the safety baseline will facilitate a deeper understanding into the interdependencies between various parts of the current regulatory framework controlling NAS.

In this text, term Regulatory-based Causal Factor Framework (RCFF) is used to refer to the proposed methodology. In very broad terms, RCFF is a qualitative, systems-level approach to safety assessment based on deductive reasoning to construct a safety baseline for operations in the NAS. The basic concept relies on two fundamental premises:

1) Title 14 Code of Federal Regulations (14 CFR) provides minimum mandatory requirements (i.e., risk controls) for safe operations in the NAS.

2) Various, seemingly unrelated regulations interact to provide risk controls for a hazard.

These two fundamental points require some more elaboration to clarify their meaning within the context of the proposed framework. Starting with the notion of using regulations as risk controls; 14 CFR can be considered as the culmination of efforts by the larger aviation community to provide an inherent minimum level of safety for every operation to be conducted in the NAS. This notion of minimum safety is outlined as rules and requirements by 14 CFR and aircraft in the NAS has to operate above the minimums set by this mandatory safety baseline. Thus, regulations act as minimum controls for potential safety risks associated with operating in the NAS.

However, individual regulations do not operate in a vacuum. When a specific aircraft or operation is concerned, a diverse collection of rules regulating different areas of the NAS interact to provide minimum safety requirements as they apply to the specifics of the operation/aircraft in question. For example, issues related to certification of aircraft, aircraft engine or propeller are regulated by 14 CFR Part 21, whereas airworthiness standards for aircraft and its components are outlined in Parts 21 to 33. Subchapter D of 14 CFR focuses on the issues of certification and training of airmen and Subchapter E defines and partitions airspace, within which the proposed operation is set to take place. Thus, each operation in the NAS is enveloped by a mandatory minimum safety baseline created collectively by various interacting rules regulating potential sources of various different hazards.

The notion of interactions between various parts of the 14 CFR to provide a minimum mandatory safety baseline is a simple yet powerful idea, which brings forth a new approach to understand and study safety in aviation. This intuitive idea, in fact, borrows from the fundamental principle of the interdisciplinary field Systems Analysis. Formally, systems analysis is the dissection of a system into its component pieces for purposes of studying how those component pieces interact. In complex systems such as NAS, safety is the product of these interactions. However, a closer look at various current research efforts on UAS integration would reveal that such studies rarely explore potential interactions between their respective area of interest and various other components of the NAS, in a systematic fashion.

Even tough, the modeling methodology that RCFF adopted is novel; the proposed regulatory-based approach of RCFF takes cues from FAA’s own Safety Management System (SMS) process. FAA Policy Document on SMS Guidance states that regulations will serve as risk control, if correctly applied in the context of the unique operational environments of service providers. Rule making process therefore should apply the concepts of safety risk management... They should identify hazards in the air transportation system. Compliance with the regulations would thus move beyond viewing them on as administrative requirements and into an environment where compliance entails effective control of clearly identified hazards. This would enhance the value of regulations as effective instruments of safety management. Regulations and subsequent oversight activities must be part of a strategy of risk control.

This understanding of regulation’s role coincides with the fundamental concepts that RCFF is built upon. Within the context outlined in FAA SMS Guidance, RCFF can also be used as part of an exploratory risk-based rule-making process as a future research initiative, where the impact of the current regulations as risk controls are evaluated on the safety baseline and shortcomings are identified and corrected.

RCFF is a qualitative system safety analysis framework. It adopts a deductive, top-down approach to identify systems-level hazards and associated causal factors using regulations (i.e., 14 CFR) as potential risk controls. This approach is especially a good fit for the analysis of emerging technologies, such as UAS, where limited availability of data makes the implementation of traditional quantitative safety analysis techniques difficult. RCFF also proposes a methodology to determine connections between potentially related causal factors, thereby creating an interlinked safety baseline. Ultimately, the RCFF safety baseline can be explored to understand the interactions between causal factors, as well as the dependencies between regulations (i.e., risk controls).

The outcome of the RCFF process is the safety baseline. Its context and scope is determined by the set of regulations included in the RCFF analysis. Hazards and causal factors constituting safety baseline are identified
based on risk controls outlined by these regulations. The scope of an RCFF analysis and the extent of resulting safety baseline can be adjusted both depth-wise and breadth-wise in terms of detail and coverage. The safety baseline can be constructed using only one 14 CFR Part or it can be developed based on multiple Parts to cover a larger domain. The analysis can be performed on a more detailed subsystem-level as opposed to building the RCFF safety baseline at a higher system-level. However, it is important to achieve a consistency within the safety baseline in terms of the level of detail it entails. For instance, if the RCFF analysis is performed based on the Sections of the 14 CFR Parts, the resulting safety baseline (i.e., individual hazards and causal factors) should present a level of detail, which is consistent with the information provided by pertaining 14 CFR Sections.

RCFF’s hierarchy closely follows current regulatory structure. At the very top of this hierarchy, covering the entire NAS, Federal Aviation Regulations (14 CFR) provide minimum risk controls for safe operations. Thus, RCFF top-down modeling process starts with regulations, or rather, it accepts regulations as input. As the system is deconstructed according to the RCFF hierarchy, functions branch out from regulations, thereby providing context for hazards regulated by the risk controls. Consequently, groups of causal factors are identified to outline the underpinnings of individual hazards. However, unlike conventional hierarchical methodologies such as Fault Trees, the proposed framework emphasizes the interactions and connectivity, which extend beyond simple deterministic or probabilistic causality, among various components and compartments comprising the whole domain. Thus, the whole process ends with the identification of linkages between potentially related casual factors. The contents of the RCFF hierarchy are stored in a database. Although the database is constructed using a software with an interface for end-users to interact, note that RCFF is proposed as a new methodology for aviation system safety analysis and it should not be perceived as a software tool per se, pointing out explicit, ready-to-use solutions for specific inquiries.

B. Implementation of the Framework on 14 CFR
RCFF process can be implemented at different layers of the 14 CFR hierarchy to construct the framework with varying degrees of specificity. For example, it can be constructed at Parts-level, where the framework branches out from 14 CFR Parts; and hazards and causal factors represent a level of detail that is consistent with a general systems-level understanding of 14 CFR Parts. Notional representation of the RCFF hierarchy for the Part-level implementation of the framework is illustrated in Figure 2.
The scope of an RCFF model can be adjusted according to research needs and requirements depth-wise as well as breadth-wise. To increase the depth of RCFF and provide more detailed hazards and causal factors for the problem domain, one can also build the framework at Subpart- or Section-level.

Although these different RCFF hierarchies (i.e., Part, Subpart, and Section-level) provide a safety baseline for 14 CFR, when compared, they differ in terms of information quality and domain coverage that individual components constituting the baseline provide. Consider, for example, 14 CFR Section 91.113, which requires pilot operating aircraft to see and avoid other traffic as well as obstacles. This requirement provides specific risk controls for midair collision and controlled flight into terrain. Thus, the domain it covers is limited to these specific hazards and underlying causal factors. Therefore, in a Section-Level implementation of the RCFF hierarchy, hazards and causal factors under Section 91.113 should provide a detailed representation of the risks pertaining to the specific controls outlined in Section 91.113. Such hazards and causal factors, although provide detailed information, cover a relatively limited domain consistent with the coverage of the corresponding 14 CFR Section.

Now consider 14 CFR Part 91, which provides general operating and flight rules for the whole NAS. Obviously, the domain that Part 91 covers is the sum of all its Sections. Thus, in a Part-Level implementation of the RCFF hierarchy, hazards and causal factors originating from Part 91 will be broad in coverage and general, even abstract, in definition as compared to a Section-level RCFF model. This idea of varying degrees of domain coverage and information quality for part-, subpart-, and section-level implementations of RCFF on 14 CFR is illustrated in Figure 3.

IV. Components of RCFF

The preceding sections present the conceptual basis of the proposed RCFF approach for aviation system safety analysis. Starting with this section, the methodology to develop the components of RCFF and populate the RCFF database is presented. The methodology outlined below entails the construction of a proof-of-concept RCFF hierarchy and populating its database utilizing a select group of 14 CFR regulations (at Part-level) as risk controls. Thus resulting product is a Part-level implementation of the proposed framework.

In this context, the proof-of-concept study identifies the components of RCFF, namely functions, hazards, and causal factors based on existing regulatory structure of 14 CFR and hierarchical framework thereof.

A. RCFF-Functions

According to the RCFF hierarchy, 14 CFR’s domain of coverage is partitioned into functions, which define the context for risk controls and provide fidelity to conceptualize hazards and causal factors regulated by them. Since the regulations do not operate in a vacuum, the functions are intended to provide contextual characteristics for the regulations. In that sense, RCFF functions are different from operational functions. Since they are based on regulations, RCFF functions convey the point of view of regulations and risk controls, thereby defining functional areas of interest from the perspective of 14 CFR. The idea of operational functions are successfully employed to develop system engineering models for 14 CFR Part 121 air carrier operational and Part 137 agricultural aircraft operational oversight activities.

In this context, following seven RCFF functions are identified with the help of subject matter experts (SMEs):

- A-1: Manage operations
- A-2: Perform air operations
- A-3: Performing aircraft maintenance, inspection and engineering
- A-4: Performing training
- A-5: Providing operation resources
- A-6: Provide regulatory standards
- A-7: Perform airworthiness activities (includes design, production, manufacturing, and engineering).
The definitions of the RCFF functions are provided below.

A-1: Manage Operations: This function directs, schedules, and coordinates operations (as used here, an operation consists of any set of related activities, not just flight operations) by aviation-related persons and entities, whether they are certificate holders or not. It provides directives, defines requirements and controls, establishes performance standards for the execution of those activities, and also ensures that the execution is accomplished in accordance with appropriate policies and procedures, and any required regulations for those activities.

A-2: Perform Air Operations: Air operation means any aircraft or vehicle flight activity, up to and including air transportation of passengers or cargo. This function carries out the task of flying in the National Airspace System, as well as in international airspace. This function includes preflight activities, ground operations, any customer and passenger services, and aircraft operations.

A-3: Perform Aircraft Maintenance, Inspection and Engineering: This function maintains and checks aircraft and vehicles capable of flight to prevent deterioration of the inherent safety and reliability levels of the equipment to ensure that UASs conform to their original design specification and are in a condition for safe operation. This process is usually called MIE (Maintenance, Inspection and Engineering). Here the maintenance means inspection, overhaul, repair, preservation, and the replacement of parts; the inspection refers to quality assurance and quality control, which continually check and analyze the approved inspections and other maintenance programs for performance and effectiveness; and the engineering means providing engineering support for the maintenance of aircraft and vehicles capable of flight. The aircraft and or vehicle capable of flight after this MIE process will be utilized for air operations.

A-4: Perform Training: This function plans, designs, implements, and evaluates an array of procedures, methods, and practices to improve work force capabilities to meet mission/workload requirements, and increase/maintain an individual’s knowledge, skills, and abilities associated with operations by aviation-related persons and entities.

A-5: Provide Operation Resources: This function acquires and allocates aircraft and vehicles capable of flight, personnel, parts, materials, facilities, equipment, training, automation, information infrastructure, tools, budget, publications, and any other required resources to support the execution of operations by aviation-related entities.

A-6: Provide regulatory standards: This function provides the regulatory standards mandated by the FAA that all aviation-related persons or entities must follow.

A-7: Perform airworthiness activities: This function performs any design, production, manufacturing, modification, testing, or engineering activity associated with aircraft or vehicles capable of flight (including systems and components). “Airworthiness”, as used here, is different from maintenance, inspection and engineering related to maintenance.

FCFF construction process starts with the identification of functions for risk controls. For each 14 CFR Part, SMEs determine functions that are relevant, thereby constructing the first layer of the framework and setting the context for the hazards and causal factor that follow.

B. RCFF-Hazards

Determining functions that apply to risk controls is a relatively simple process compared to identifying individual hazards and causal factors. The latter, which is essentially knowledge elicitation, requires a fairly good understanding of regulations, hence a detailed study of 14 CFRs. Thus, heavy involvement by subject matter experts is also necessary to identify hazards and causal factors. This section provides a discussion on the methodology and process utilized to identify the FCFF hazards.

FAA defines identifying hazards as an integral part of the Safety Risk Management (SRM) process and provides a good starting point for when and how to perform the hazard identification:

B. The SRM process shall be applied to:

1. Initial design of systems, organizations, and/or products;
2. The development of operational procedures;
3. Hazards that are identified in the safety assurance function; and
4. Planned changes to the operational processes to identify hazards associated with those changes.

There are two commonly used hazard identification methods:

1) Hazard identification through analysis of data derived from operational observation and
2) Hazard identification through process analysis.

In the FAA’s SRM requirements, item B.1. above corresponds to the hazard identification method based on operational observations and item B.3. refers to the method based on process analysis. In most real world applications these two methods are employed conjunctially. Due to limited availability of historical data on emerging UAS operations, it is quite difficult to perform a system safety study based on the former method, i.e.,
hazard identification through analysis of data derived from operational observations. The latter method for hazard identification will be discussed next with a particular emphasis on its applicability to the RCFF concept.

Reiterating, at the crux of the RCFF lies the assumption that regulations provide a safety baseline in terms of controlling and managing hazards and consistent with this hypothesis, current aviation regulations are considered as the minimum controls that are used by RCFF methodology to derive hazards and causal factors. In this context, the hazard identification process relies on the interpretation and extraction of these controls as defined by the regulatory text. At first glance, this novel approach for hazard identification may seem substantially different than and, in some cases, incompatible with the traditional methodologies. However, a closer inspection would reveal that these controls can be considered as part of the safety assurance function mentioned above in item B.3. and hence the hazard identification method employed by the RCFF is basically a variation on hazard identification through process analysis.

To perform the hazard identification task within the RCFF, numerous knowledge elicitation sessions were conducted with a diverse group of subject matter experts who have extensive background on regulatory oversight. During this process, for each 14 CFR Part included in this study, SMEs were advised to identify hazards, within the context defined by the pertaining function, while keeping the level of detail and coverage at a Part-level understanding of the regulatory text. This approach gives rise to a hazard set, where individual hazards represent a systems-level risk with broader coverage of UAS, its components and operations. An illustrative example is provided below to make the mechanics of the proposed hazard identification procedure employed by the RCFF more transparent to the reader.

Consider 14 CFR, Subchapter F, Part 91 – General Operating and Flight Rules. Functions A-1 to A-6, were identified by the SMEs as the six functions covering the domain of Part 91. Then, for each function, a set of potential hazard sources was named based on a high-level reading of the Part 91’s content. Within this context, for Function A-1, SMEs identified “Operational Information”, “Aircraft Airworthiness”, and “Required Authorizations” as potential hazard sources. Whereas potential hazard sources for Function A-2 are identified as “Collision Avoidance” and “Environment”. Identifying potential hazard sources rather than individual hazards themselves fits perfectly to the system-level approach of RCFF using a Part-level analysis of the regulations.

C. RCFF-Causal Factors

Determining causal factors that are potentially related to the hazards sources constitutes the next step in building the framework. Although basic concept entails a similar qualitative approach involving SME knowledge, causal factor identification process differs from hazard identification in detail and execution. In particular, individual causal factors are identified through the combination of two components: keywords and modifiers. When a keyword is paired by a modifier a causal factor is created. Keywords and modifiers are determined independently by the SMEs for each hazard source based their interpretation of 14 CFR Parts. Consequently, the pairing of a keyword and modifier is done automatically by a computer script. The resulting list of causal factors is then verified by the SMEs for relevance and accuracy. All possible pairs are used during the process to create a list of preliminary CFs.

Once identified according to the process outlined above, automatically generate list of causal factors needs to be reviewed by the SMEs to verify that individual causal factors presents a level of generality consistent with the intended systems-level perspective of the Part-level RCFF model. For 62 FAR Parts, functions, hazards, and causal factor keywords and causal factor modifiers had been identified as part of a Phase 1 RCFF study. However, considering thousands of prospective part-level causal factors generated for these Parts, it was decided to further limit the scope of the Part-level RCFF model. Consequently, among the 62 Parts, the following 13 Parts representing various important areas of interest in the NAS were selected as basis for the Part-Level proof-of-concept.

List of 14 CFR Subchapters and Parts included in the Part-Level RCFF proof-of-concept model:

Subchapter C – Aircraft:
- Part 21 – Certification Procedures for Products and Parts
- Part 23 – Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes
- Part 25 – Airworthiness Standards: Transport Category Airplanes
- Part 27 – Airworthiness Standards: Normal Category Rotorcraft
- Part 33 – Airworthiness Standards: Aircraft Engines
- Part 34 – Fuel Venting and Exhaust Emission Requirements for Turbine Engine Powered Airplanes
- Part 43 – Maintenance, Preventive Maintenance, Rebuilding, And Alteration

Subchapter D – Airmen:
- Part 61 – Certification: Pilots, Flight Instructors, and Ground Instructors
- Part 65 – Certification: Airmen Other Than Flight Crewmembers

Subchapter F – Air Traffic and General Operations:

American Institute of Aeronautics and Astronautics
Note that the Parts listed above are some of the most prominent Parts among the regulations that constitute Chapter I of 14 CFR, providing broad coverage in terms of risk controls for the whole NAS. Once the scope of the proof-of-concept study was determined, causal factors that had been generated for them were reviewed by SMEs and a final set of Part-level causal factors was compiled.

The methodology employed to determine this final set of Part-level causal factors, in essence, is a qualitative process where expert judgments determine the outcome. Therefore it is essential to setup a structured process to make sure that the outcome is repeatable and the knowledge elicitation process is transparent.

When dealing with subjective data, such as expert judgments, repeatability is always a major issue. However, expert judgments are indispensable within the context of system safety analysis especially when data required for analysis is limited or unavailable. If the problem domain dictates, aviation safety studies use expert knowledge successfully. Therefore, it can be confidently argued that using expert judgments is not necessarily a drawback if implemented according to a well defined, structured and repeatable protocol. In this context, SMEs involved with the review process were provided with a structured protocol, which establishes guidelines to identify Part-level RCFF causal factors among the preliminary list generated automatically for the included Parts.

D. RCFF-Linkages

Final step of the RCFF construction process is the phase where potential interactions among causal factors within the RCFF safety baseline are identified. Ultimately, this will lead to an interconnected safety baseline and help facilitate a deeper understanding of some important potential dependencies between regulations controlling separate domains of the NAS.

A linkage between two causal factors indicates a potential qualitative correlation or dependency, which extends beyond the linked causal factors to their respective risk controls (i.e., regulations). Identifying this potential dependency between various seemingly unrelated parts of regulations is an intriguing prospect that we are very much interested in. In this context, the safety baseline and associated linkages constitute the outcome of an RCFF analysis.

Within the proposed framework of RCFF, it is conceptualized that these interactions (or linkages) are to be determined by identifying semantic similarities between causal factors. To determine a potential dependency based on a semantic connection, additional information is need for each causal factor. This additional semantic information is composed of two components;

1) a short text describing the causal factor, and
2) a set of keywords and/or phrases representing important aspects of the context of the causal factors.

Connections between two potentially related causal factors are established based on textual similarities that exist between their respective descriptions. More specifically, textual similarities are determined by conducting word/phrase searches within the descriptions of causal factors. To that end, Boolean operators, such as AND and OR, are used to formulate a simple query expression for each causal factor using their respective set of keywords. Then, based on the query expression, a search is performed in the descriptions of all other causal factors in the RCFF safety baseline. A match during the search is indicative of potential linkage between the causal factor whose keywords are searched for and the causal factor whose description contains those keywords as defined by the query expression.

We used PolyAnalyst, a commercially available software package from Megaputer Intelligence, to perform Boolean searches in the causal factor definitions. PolyAnalyst is a data mining tool. For the purposes of this study, we mainly utilized its text-mining functionality. In simple terms, PolyAnalyst seeks out similar keywords and key phrases within the definitions of the causal factors. Based on predefined criteria, it determines similarities and suggests linkages between CFs.

In more technical terms, PolyAnalyst provides the user with the ability to perform the operations such as categorization, clustering, prediction, keyword and entity extraction and more. This software determines which causal factors are related to each other and stores this information in a database. PolyAnalyst accomplishes this through categorization functionality. A taxonomy is created in PolyAnalyst where each causal factor becomes a category with the associated keywords put into a query. The query will consist of a string of words separated by Boolean operators (e.g., AND, OR, NOT). A thesaurus is used to improve search accuracy by including searches for
synonyms. PolyAnalyst then calculates which categories match which records using the query and create links between the causal factors.

Table 1 provides a sample data entry in the RCFF database, which includes CF Descriptions and keywords employed to identify potential interdependencies between causal factors in the safety baseline.

### V. Concluding Remarks

The integration of UAS to the NAS could arguably be the most challenging problem that the aviation community in the United States is currently facing. The premise of integrated UAS operations in the NAS not only requires technology solutions for complex issues, such as “sense and avoid” or “control and communications”, but also necessitates a systems-level understanding of UAS’s safety impact on existing controls and current operations.

This paper presents a regulatory-based integrated approach to system safety and risk analysis of the UAS operations and their interaction with the current NAS and the future Next Generation (NextGen) Airspace. The proposed framework applies the International Civil Aviation Organization (ICAO) sanctioned safety management system (SMS) principles with a particular focus on safety risk management (SRM) and safety assurance. The framework establishes a SMS approach based on the FAA regulatory requirements to support the safe integration of UASs into the NAS. It is intended to provide guidance and direction to move forward while integrating new and complex technologies in the NAS and meeting the FAA SMS mandates.

The proposed approach is a systematic process for the identification of systems-level hazards and causal factors that are derived from existing controls such as the regulations governing the NAS (i.e., 14 CFR). It provides a qualitative means of identifying a safety baseline on the NAS.

Future integration of UAS into NAS suggests potential system-wide impact large due to UAS’s unique design and mission needs. These UAS-specific requirements along with limited operational knowledge and lack of historical data make the application of conventional quantitative safety risk analysis tools and techniques difficult.

This paper presents an outline of the concepts and methodologies utilized to construct a Part-level RCFF study. This study entails a systems-level implementation of the proposed safety analysis framework based on the risk controls that currently exist in the NAS and are provided by the 14 CFR. In this context, a systems-level implementation of the proposed framework was achieved by constructing the RCFF hierarchy at the level of 14 CFR Parts.

The proposed framework is applied to a set of Federal Aviation Regulations (FARs) selected to represent existing hazard controls for various main components of the NAS. Using this representative set of regulations a baseline set of systems-level hazards and causal factors are determined. Then, for each causal factor identified, textual descriptions are developed by a group of subject matter experts with diverse aviation background.

---

Table 1. Sample entry in the RCFF database which includes Part-Level RCFF causal factor descriptions and keywords.

<table>
<thead>
<tr>
<th>Part #</th>
<th>Part Title</th>
<th>Function</th>
<th>Hazards (related to)</th>
<th>Causal Factor</th>
<th>CF ID</th>
<th>CF Description</th>
<th>Notes</th>
<th>CF Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Certification procedures for products and parts</td>
<td>A-7:</td>
<td>Instructions for Continued Airworthiness (ICAs)</td>
<td>inadequate manufacturer’s manuals</td>
<td>8082</td>
<td>Manufacturer fails to provide adequate manuals, which include detailed instructions and guidance for continued airworthiness.</td>
<td>Manufacturer’s manuals developed and published by the type certificate holder do not include detailed instructions for continued airworthiness in accordance with Part 21 of 14 CFR. Such instructions include the drawings and specifications necessary to define the configuration and the design features of the product, information on dimensions, materials, and processes necessary to define the structural strength of the product, an airworthiness section, a special inspection and preventive maintenance program.</td>
<td>(Manufacturer AND manual) OR (Instruction AND phrase(continued airworthiness))</td>
</tr>
</tbody>
</table>
Consequently, text mining tools and techniques are used to identify interactions and interdependencies between potentially related causal factors.

As a result of this study, the following conclusions are surmised:

1) RCFF provides a technically sound system safety analysis framework to investigate the safety impact of introducing a new technology, such as UAS, to the NAS.

2) The proposed framework, unlike many other methodologies, determines a minimum mandatory safety baseline for the domain that it investigates. This mandatory safety baseline applies to all operations and platforms and identifies a set of minimum -but not necessarily sufficient- risk controls for conducting safe operations within that particular domain.

3) The notion of a mandatory safety baseline has tremendous potential when studying the safety impact of Unmanned Aircraft Systems whose platform diversity and operational complexity present a challenge for the NAS unlike any other technology before.

4) The mandatory safety baseline not only provides a set of casual factors and associated hazards; it also links them back to a set of risk controls mandated by exiting regulations and presents the results within a top-down hierarchy.

5) Ultimately, RCFF concentrates on potential interactions and dependencies within the mandatory safety baseline. Once identified, these connections can be used to study dependencies between regulations and to determine potential gaps in the regulatory structure that need to be address to control safety risks associated with new technology, such as UASs, to be integrated in to the NAS.

**Acknowledgement**

This research outlined in this paper is supported by Federal Aviation Administration under contract number DTFACT-04-D-00003. The authors are appreciative of the technical expertise provided by the FJ Leonelli Group, Inc. in the knowledge elicitation sessions. The contents of this paper do not necessarily reflect the official view or policy of the Federal Aviation Administration.

**References**

15. Federal Aviation Administration, Order - Safety Management System Guidance, 8000.369, September 30, 2008

American Institute of Aeronautics and Astronautics