SAND97-1973C

CONF-970898--

A System Safety Approach to the FAA Surveillance Process

Paul W. Werner, Ph.D. and Dave R. Olson,
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0491

Abstract

As commercial air travel grows in terms of the number of passenger miles flown, there is expected to be a corresponding dramatic increase in the absolute number of accidents. This despite an enviable safety record and a very low accident rate. The political environment is such that an increase in the absolute number of accidents is not acceptable, with a stated goal of a factor of five reduction in the aviation fatal accident rate within ten years. The objective of this project is to develop an improved surveillance process that will provide measurements of the current state-of-health and predictions of future state of health of aircraft, operators, facilities, and personnel. Methodologies developed for nuclear weapon safety, in addition to more well known system safety and high-consequence engineering techniques, will be used in this approach.

This project is concerned with Part 121 surveillance and applies system safety and high-consequence system engineering techniques and tools, including those developed by Sandia National Laboratories for assuring the safety of nuclear weapons.

Surveillance is one of the most significant duties of the FAA toward its larger responsibility of assuring air transportation (Part 121) safety. The *Process Quality Management Improvement (PQMI)* methodology was used to define the current surveillance process in order to understand the existing system, customer requirements, and system requirements. This understanding led to the conclusion that effective surveillance must be founded upon a system safety approach encompassing both surveillance of the carrier and the FAA process to certificate and to manage the certificate. A unique Sandia tool was used to center the reengineered surveillance process on safety and move it toward the new paradigm expressed in the *Gore Commission Report*.

Problem

As commercial air travel grows in terms of the number of passenger miles flown, there is expected to be a corresponding dramatic increase in the absolute number of accidents. Despite an enviable safety record and a very low accident rate, the political environment is such that an increase in the absolute number of

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

DISCLAIMER

accidents is not acceptable, with a stated goal of a factor of five reduction in the aviation fatal accident rate within ten years (Recommendation 1.1, *Gore Commission Report*).

As the aircraft fleet ages and in many cases, exceeds its intended life, age related defects are expected to occur. Also, new aircraft with new technologies create a certification and surveillance challenge.

Approach

Develop an improved and targeted surveillance process that will provide measurements of the current state-of-health and predictions of future state of health of aircraft, operators, facilities, and personnel. The approach is analysis-based and seeks to measure and predict safety related problems. This approach would evolve surveillance from the mode of routine periodic inspections to a targeted and integral part of the system design, identifying defects before actual failure and thereby reducing cost and personnel risk. Using the system surety engineering process assures the incorporation of system safety concepts and high consequence engineering tenants in the resulting improved surveillance process

Basic Concepts of System Safety

- Safety is a property of the system, not a component.
- Safety should be built into the system, not added on to a completed design.
- Accidents are not always caused by failures and all failures do not cause accidents.
- Emphasis is on identifying hazards as early as possible and then designing to eliminate or control those hazards (more qualitative than quantitative)
- Recognize tradeoffs and compromises in system design.
- System safety includes the non-technical issues.

Major Tenets of High Consequence Systems Engineering

- Validate safety requirements
- Proactively identify and analyze system failure modes and their effects (high consequences) during the entire life-cycle
- Design safety into the system to assure (through fundamental principles) safe system response in all normal and off-normal environments
- Ensure designer and user have a shared responsibility to control/reduce the consequences as well as the likelihood of off-normal environments
- Place engineered and administrative controls on safety-critical features
- Provide a forum for independent assessment

- Employ an active surveillance program throughout the life-cycle to continuously verify desired safety performance and identify timely safety upgrades
- Maintain a lessons learned database.

System Surety[1] Engineering Process

This process, depicted in Fig. 1, was developed at Sandia National Laboratories in the course of its work in high-consequence (nuclear weapon) engineering. Its development was motivated by the realization that standard engineering practices did not provide the level of safety assurance necessary for its operations with the potential for catastrophic accidents.

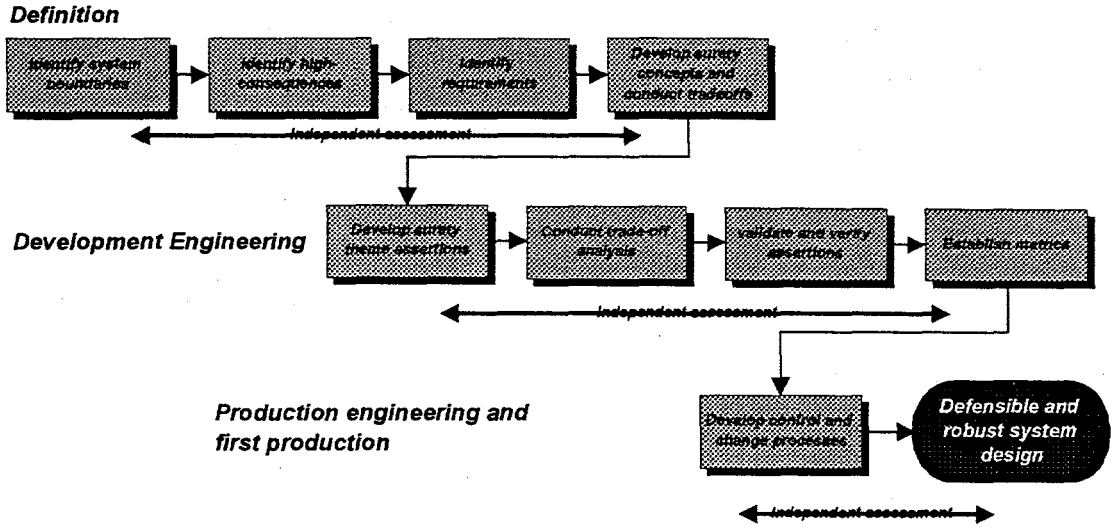

Figure 1. System surety engineering process

The process consist of the following steps, with examples of application to the FAA surveillance process provided:

1. Identify system boundaries

A clear understanding on what the extent of the "system" is. A system is an integrated set of people, procedures, equipment, and facilities that perform a specific operational task within a specific environment. The system boundaries include the interaction of this set that may contribute to the formation of hazards during the life-cycle of a system. System boundaries and interfaces will be specific to the individual system and its life cycle states. Of special importance are normal and off-normal flows of energy and information across boundaries.

---

[1] Surety is defined here as safety security, reliability, and quality.

Example: Our design space will be the FAA surveillance of Part 121 aircarriers, their aircraft, operations, facilities, maintenance, and crews. We will also include the FAA training and management functions necessary to support the surveillance process. The goal is to enhance the current surveillance process and center it on assuring the airlines operate safely.

2. Identify High Consequences: Varies with the operation and the customer, but is judged to be severe, e.g., resulting in significant loss of investment or loss of life. This is what the system design must inherently avoid.

Example: Inadequate surveillance (includes OEM, operator and FAA oversight) WILL result in aircraft accidents!!!

- Significant loss of life
- Significant financial loss
- Loss of public confidence
- Negative public perception
- Political ramifications

3. Define Requirements: Using a team with design and surety expertise, identify and integrate traceable requirements of how the system is to perform with respect to its operation, surety elements, regulations and orders, and consequences. System safety requirements are developed for both operating (normal) as well as accident (off-normal) environments. Requirements may define hazards to be avoided, credible operating and accident environments, span of operations covered, and system boundaries and interfaces. If there are many consequences/requirements, a sorting exercise is used to identify priorities.[2]

A sub-process of requirement validation is also done. We define *validating requirements* as the process which ensures that

- the set of requirements are consistent and complete.
- a real-world solution can be built that satisfies the requirements.

Requirements mat also be divided into logical groups for prioritization, e.g.:

Operational
Safety
Security
Regulatory

4. Develop Surety Concepts: Identify and integrate surety concepts that are important in the system, resulting in a surety theme. The value of the theme

---

[2] Safety culture check - safety should be the first priority in a high consequence system. If it can be done right, it can be done safely (and probably less expensively).

is that it directs design/development efforts towards meeting major requirements and provides a framework in which to communicate the various implementations (some of which, such as safety and security measures, may come into conflict). A safety theme describes in a unified fashion the goals and measures that will be used to assure safety under all expected environments.

The safety theme focuses on those elements of system design are *safety critical*. These elements must utilize engineered features that are identifiable, analyzable, and controllable. The goal is to minimize the number of system components that are safety-critical in abnormal environments. Because the safety assurance then hinges on a relatively small subset of overall system design, limited design and verification resources can be better focused to improve confidence that predictable safety will result.

Example safety theme elements for a surveillance process:

Systems Approach
Safety is an emergent property that arise when the system components interact predictably within an environment. A systems approach is necessary for improving safety.

Standardization
Management must set safety policy and goals, define priorities, detect and solve goal conflicts, and set up incentive structures. Policies, goals, requirements, and incentives must be consistent throughout the system.

Checks and balances
Independent roles and cross-checking of assessments, actions, and measurements are required for safety. Self-assessment and continuos improvement must be integral to the process. Impact of process on system must be measurable.

Communication
Information is vital for decision making. Channels for information dissemination and feedback are required, including a means for comparing actual performance with desired performance and ensuring that required action is taken.

Defined Action
The process must be able to influence the system in a desirable and predictable manner. The action may be proactive or reactive. Proactive action is emphasized. Responsibility, accountability, and authority must be clearly defined. All three must go together.

Responsibility - Who owns it?

Accountability - Who assesses or measures the result of an action?
Authority - Who determines a course of action?

The SIP team designed a baseline process, shown in Figure 2, for surveillance based on the requirements, theme, and objectives. This was done in a team setting and resulted in several conceptual changes of the process.

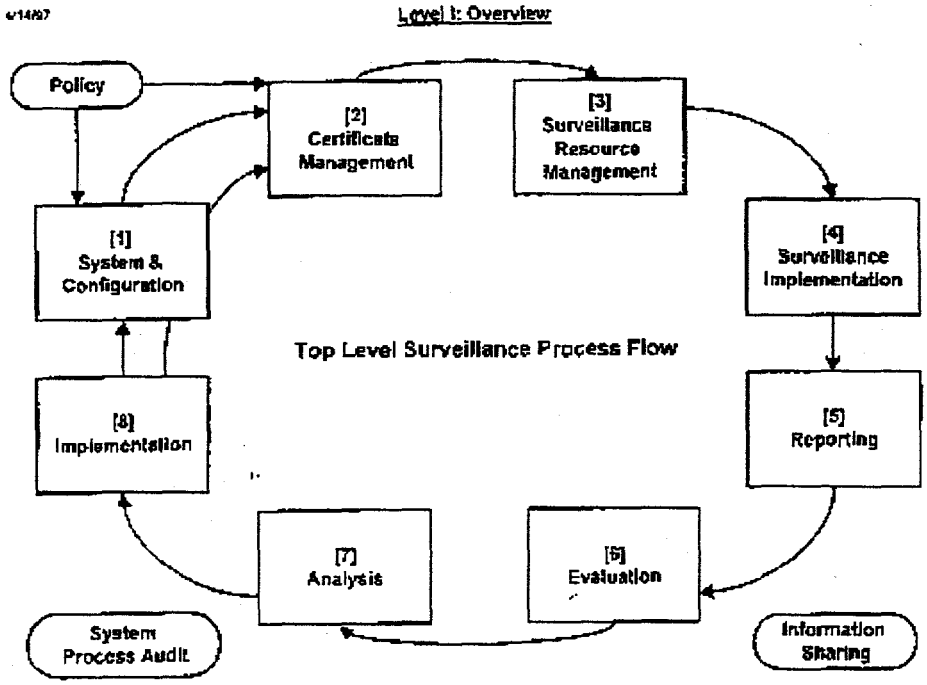

Figure 2. Level 1 surveillance system design.

5. Develop surety theme assertions

Develop surety performance assertions that are measurable and quantifiable. Develop and analyze technical alternatives for implementing the surety theme. The next level of detail is shown in Fig. 3. This was the result of developing and analyzing various alternative sub-processes.

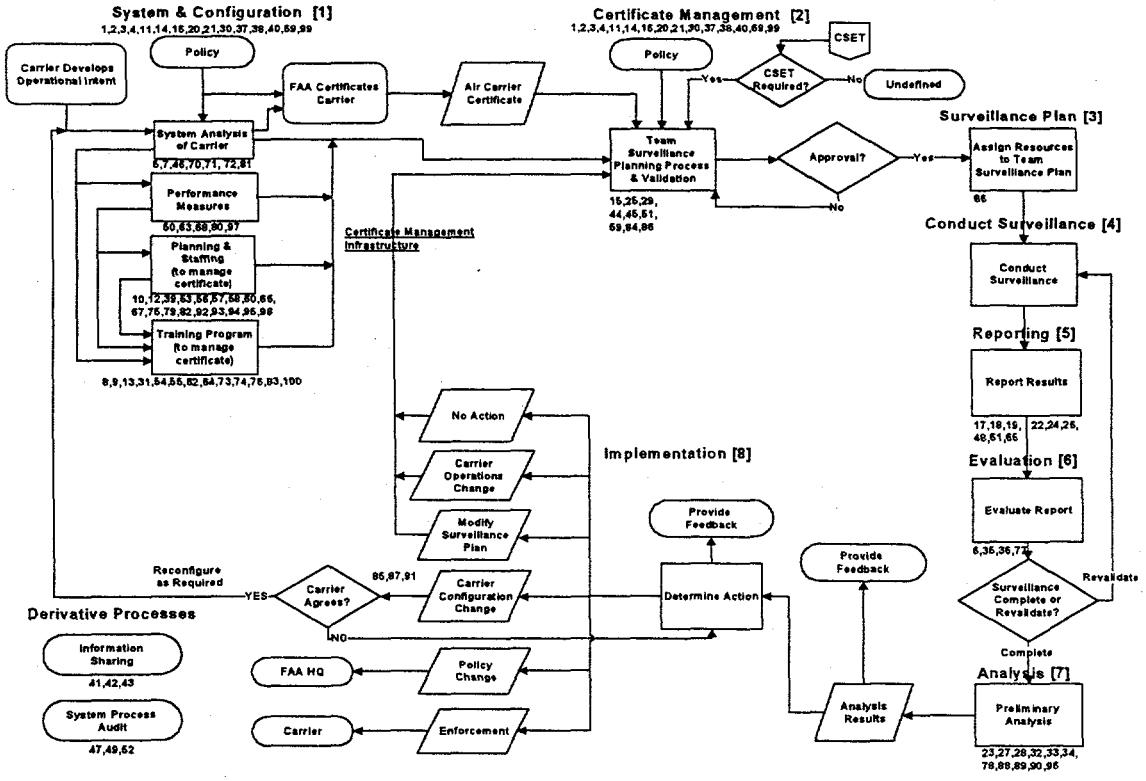

Figure 3. Level 2 surveillance system design.

6. **Conduct trade-off analysis**: Explore the interactions of the surety elements with "what if" scenarios; understand how these trade-offs affect the consequences to achieve appropriate balance and level of rigor.

   Example: The consequences of poor data quality was identified and resulted in additional QA checks and feedback channels to the information resource management function.

7. **Conduct Surety Analysis**: Perform analyses to quantify the system with: modeling and analysis; characterization of processes; and examination of procedures. The interactions between the surety elements are explored and understood.

   Example of elements comprising a surety theme for a surveillance process:

   Element - Systems Approach
   Basic concepts of system safety and high consequence systems engineering were applied by

- developing a hierarchical model for the process: Level 0, level 1, level 2, and level 3. The relationships between levels and their degree of complexity was documented;
- building an emphasis on safety into the process, not adding it on to an existing design;
- emphasizing analysis over anecdotal experience and reactive behavior;
- developing a targeted surveillance program throughout the life-cycle to continuously verify desired safety performance and identify timely safety upgrades;
- emphasizing identification of hazards as early as possible;
- ensuring carrier and regulator have a shared responsibility to control/reduce the consequences as well as the likelihood of accidents; and
- providing a mechanism for independent assessment.

Element - Standardization

We use a high level systems analysis to identify and standardize

- training
- performance measures
- options
- decision tools
- system behavior

We also identified a high-level team to enhance FAA standardization.

Element - Checks and balances

Independent roles and cross-checking of assessments, actions, and measurements are required for safety. Self-assessment and continuos improvement must be integral to the process. Impact of process on system must be measurable.

- The surveillance team actions are independent of certification.
- Analysis of the surveillance data is done by a different group.
- Quality assurance of data/report prior to analysis
- Higher level system analysis takes broader view of system
- Independent audit of surveillance process
- Preliminary analysis process validates and verifies original systems analysis and surveillance plan
- Each sub-process has a self-assessment function built-in.

Element - Communication

- Critical decisions and findings are communicated via feedback loops

- Certificate management and surveillance information sharing is inherent in the process
- Corporate knowledge is retained and communicated using the training programs.
- Critical information is directed to the action processes with minimal filtering

Element - Defined Action

- Processes and functions are clearly defined.
- We have identified the process owner, who also self-assesses the process and has authority to take action.

8. Establish metrics

Establish a method for tracking, verifying, and testing to verify system requirements are met and to continually enhance models.

9. Develop control and change processes

Surety controls assure adherence to design specifications by tracking, controlling, and testing to verify system requirements are met. Once safety critical implementations have been selected they must be controlled to validate and maintain their enduring high standards. There must also be a process to assess the total aspect of any changes and their impact on the total system design. This reevaluation must determine if any new hazards are introduced or if existing controls will be bypassed if the change is implemented. Management approval by the systems organization, the affected component organization(s), and the nuclear safety organization is required before the change is implemented.

Summary

The system surety engineering process produces a documented and traceable approach for developing a new system or process. If done correctly, it provides

- traceability from requirement to final product.
- verification of meeting requirements.
- understanding of operator, OEM, and FAA of there contributions and responsibilities for safety.

In this paper, we have shown the systematic and logical development of a new process that addresses requirements at a system level, is focused on safety, and has a documented safety approach.

Areas of identified improvement include:

- relationship of a certification and certificate management;

- linkage between system analysis and surveillance planning, staffing, and training;
- the need to use performance measures as a basis for surveillance and for self audit;
- the creation of certification management team to include the CHDO and the geographic inspectors;
- clearer linkages between training and surveillance resource management;
- identification of clear quality assurance measures for data;
- creation of a defined analytic team for certificate management; and
- relationship of the carrier in the process.

The systematic and structured approach, centered on the system surety engineering methodology, used by the team has produced a recommendation for an improved surveillance system, including the FAA training and management functions necessary for support, that will provide measurements of the current state-of-health and predictions of future state-of-health of aircraft, operators, facilities, and personnel.