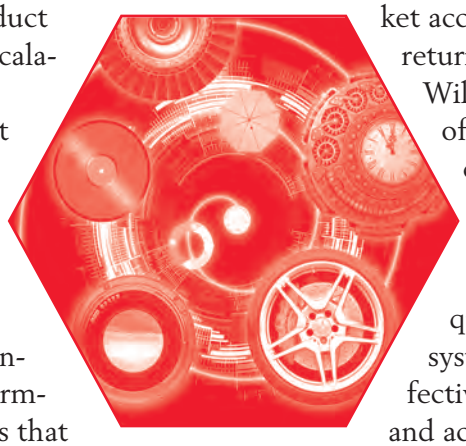
Cost, Schedule and Safety Benefits of Early System Safety Involvement

by John E. Hewitt and Daniel J. Foito
Stratford, Connecticut

System safety engineering is the application of engineering and management principles, criteria and techniques to achieve acceptable mishap risks. System safety typically reduces mishap risks through analyses that identify and address potential system failure modes. Studies indicate that when system safety is involved early in the product lifecycle, schedule slippage and cost escalation resulting from design changes can be substantially reduced. Development programs often face the dilemma of whether to apply funding to perform thorough, intensive system safety analyses in the conceptual design phase or wait until later, when designs are more complete, parts are being manufactured or testing is underway. Performing the analyses earlier consumes funds that might be needed later, while performing the analyses later increases the likelihood of expensive and time-consuming redesigns. This paper provides examples that encourage involving system safety engineering earlier in the process, by demonstrating the cost and schedule advantages, as well as the expected safety risk reduction. In addition, involving system safety earlier permits corrective actions to be implemented at a higher level in the system safety order of design precedence, which increases the effectiveness of corrective actions and reduces residual risk.



Background

System safety is defined as "the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risks within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle" [Ref. 1]. This definition prioritizes achieving "acceptable mishap risks," but also includes "the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle." In practice, there is always a desire to "achieve acceptable mishap risks" but the constraints of time and cost are ever present. This is particularly challenging during product design and development, when funding has been allocated for a new design that might not reach the market and begin generating returns for several years. During this period, program risk is high because of considerable uncertainty. For example, will the product design be completed within the allotted budget? Will the product reach the marketplace before competitors' products? Will market acceptance and product sales generate returns that will exceed development costs? Will the product enhance the reputation of the company and lead to future success? Business managers address such issues, but system safety engineering can provide support and reduce risk. To reduce risk and answer these questions, consider that "for almost any system, product, or service, the most effective means of limiting product liability and accident risks is to implement an organized system safety function beginning in the conceptual design phase, and continuing through to its development, fabrication, testing, production, use and ultimate disposal" [Ref. 2].

Thus, product development programs often face the dilemma of whether to apply funding to involve system safety engineering beginning in the conceptual design phase or wait until later, when designs are more complete, parts are being manufactured or testing is underway. Performing the analyses earlier consumes funds that might be needed later, while performing the analyses later increases the likelihood of expensive and time-consuming redesigns. Performing the analyses earlier is sometimes perceived as slowing the design phase and delaying development milestones and entry into service.

System safety engineering reduces mishap risk, often through analyses that identify potential component or system failure modes that were not discovered earlier — for example, during conceptual design, or in subsequent design and development activities. The term "system safety" applies throughout the product lifecycle, and some organizations establish subfunctions within system safety, such as development system safety, test system safety and operational system safety, which correspond to product lifecycle phases.

For clarity, this paper uses two subdivisions: "development system safety" for those system safety activities performed prior to initial production and "operational system safety" for those system safety activities performed after entry into production.

Development System Safety

Development system safety involves performing analyses that identify hazards within the design, then developing corrective actions to mitigate the risk or eliminate the hazard. Various standards, specifications, handbooks and other documents provide guidance to system safety engineers and recommend practices to be followed. In recent years, some military aviation programs have begun to use elements of both commercial and traditional military standards to identify, eliminate or mitigate system hazards and demonstrate that the system will operate with the required level of safety.

Table 1 provides a list of safety analyses that are typically performed during the development of an aircraft product [Ref. 3]. Many of these analyses require additional sub-level analyses to be performed, as shown in Table 2.

Figure 1 illustrates the sequencing of a typical System Safety Program Plan (SSPP) during the development of a complex new product, such as an aircraft or aerospace system. Major program milestones such as System Readiness Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR), Flight Readiness Review for aviation programs (FRR) or Operational Readiness Review for other programs (ORR), and Initial Operational Capability (IOC) are identified at the top of the figure, above the development steps. Below, the Hazard Tracking Record (HTR) Log tracks the mitigation or elimination of hazards identified throughout the design phase of the product. Detailed

Table 1 — Typical Development System Safety Analyses

Analysis	Definition/Purpose
Preliminary Hazards List (PHL)	A compiled list of potential hazards created early in development
Top-Level or System Functional Hazard Assessment (FHA)	A systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity
Preliminary System Safety Assessment (PSSA)	A systematic evaluation of a proposed system architecture and implementation based on the Functional Hazard Assessment and failure condition classification to determine safety requirements for all items
Operating and Support Hazard Analysis (O&SHA)	Identification and assessment of hazards introduced by operational and support activities and procedures; and evaluation of the adequacy of operational and support procedures, facilities, processes and equipment used to mitigate risks associated with identified hazards
System Safety Assessment (SSA)	A systematic, comprehensive evaluation of the implemented system to show that relevant safety requirements are met
Common Cause Analysis (CCA)	Generic term encompassing Zonal Analysis, Particular Risks Analysis and Common Mode Analysis
Flammable Fluids Analysis	A systematic analysis to consider interactions between flammable fluid sources and potential ignition sources, and how the potential of a fire starting and spreading has been mitigated

Table 2 — Typical Sub-level Analyses.

Primary Analysis	Sub-level Analysis
Functional Hazard Assessment	Preliminary Hazard Analysis, Top-Level FHA, System FHA
Preliminary System Safety Assessment	System Fault Tree Analysis (FTA)
System Safety Assessment	System FMEA/FMECA, System FTA

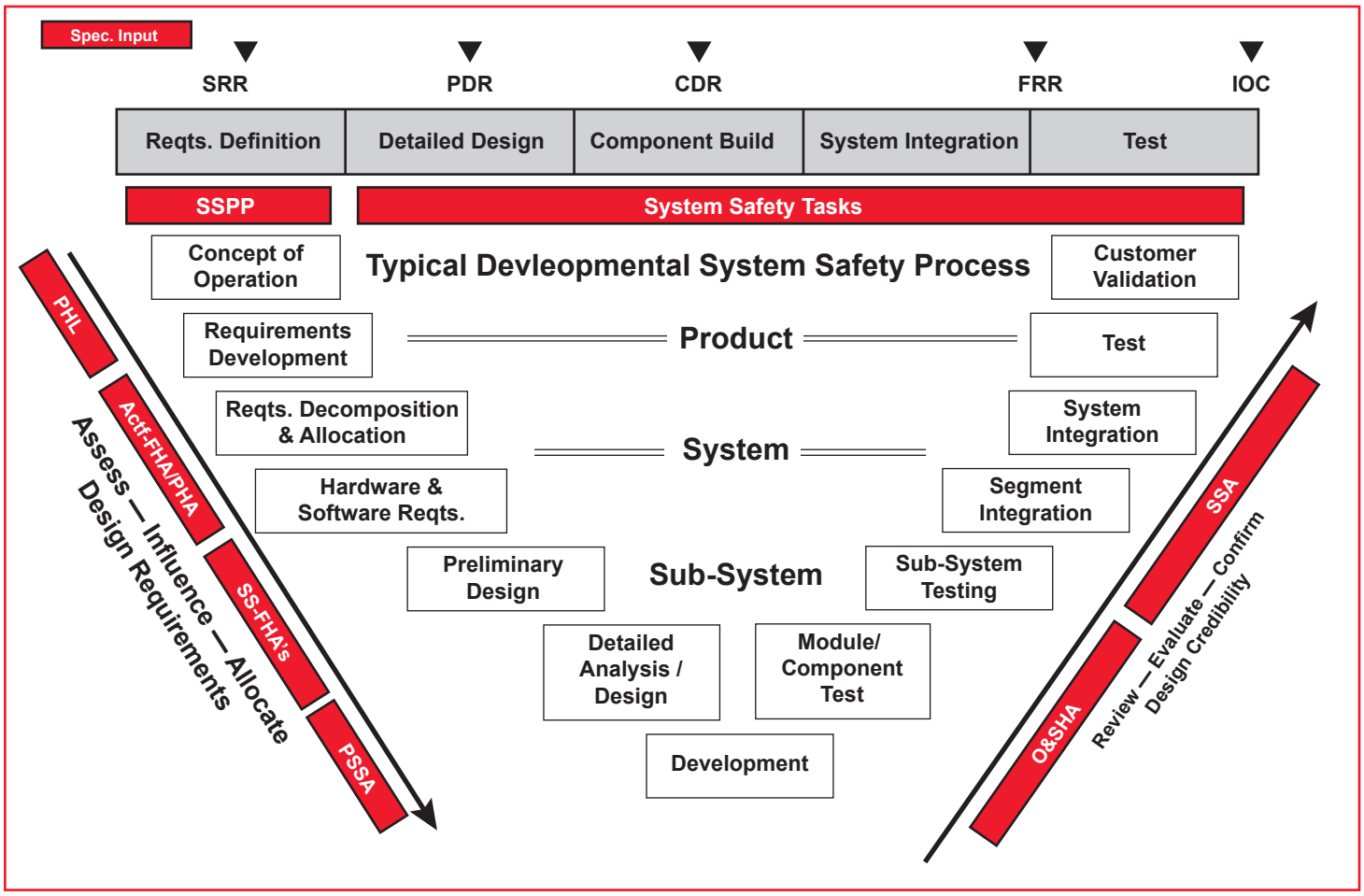


Figure 1 — Development System Safety

analyses begin on the left side of the "V," with the Preliminary Hazards List (PHL) at the start of the program, and end on the right side, with the completion of the System Safety Assessment (SSA) as the test phase is completed. A less complex SSPP would be used for a less complex product.

Operational System Safety

System safety engineering is not limited to the design and development phases of a product lifecycle. Although the design and development phase anticipates and develops mitigation for many operational hazards, some hazards are not discovered until products and systems are in service. Development system safety endeavors to contain hazards, while operational system safety addresses hazards that were not contained within the design and development phase. Hazards that are not contained can increase cost, disrupt schedules, impact resources, increase residual risk and affect the reputation of the company. In serious cases, hazards that are not contained can result in major customer dissatisfaction, withdrawal of products from service, cancelled orders and product recalls. Therefore, in operational system safety, there is an urgency to provide at least interim corrective action to temporarily mitigate mishap risk until final actions can be implemented to further mitigate the risk or eliminate the hazard.

The operational system safety process encompasses hazard identification, hazard analysis, hazard elimination, risk mitigation, residual risk control, and acceptance of risks that are not eliminated. For example, the process typically includes products in production and their associated hardware, software, firmware, operation and maintenance. The specific process varies among products and manufacturers, since complex products that benefit from system safety engineering generally must meet certain minimum safety standards or requirements. These vary depending on the product, and whether military or commercial use is intended. These requirements typically have similar approaches and processes, along with the same goal: to identify and eliminate or mitigate hazards.

Operational system safety relies on information provided by users of the product, either directly or through the customer service organization, to operational system safety personnel. This information is reviewed and analyzed to determine if a reported

RISK ASSESSMENT MATRIX				
SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	HIGH	HIGH	SERIOUS	MEDIUM
Probable (B)	HIGH	HIGH	SERIOUS	MEDIUM
Occasional (C)	HIGH	SERIOUS	MEDIUM	LOW
Remote (D)	SERIOUS	MEDIUM	MEDIUM	LOW
Improbable (E)	MEDIUM	MEDIUM	MEDIUM	LOW
Eliminated (F)	Eliminated			

Figure 2 — Qualitative Risk Matrix from MIL-STD-882E

issue constitutes a hazard. If a hazard exists, corrective actions must be developed and implemented. Typically, a Hazard Tracking Record is entered in a Hazard Register, Hazard Tracking System or other similar tool that is used to retain all documentation and track progress toward mitigation or elimination of the hazard.

Qualitative Risk Assessment is usually performed, and a Risk Assessment Code is typically assigned in accordance with a Qualitative Risk Matrix as shown in Figure 2. Qualitative Risk Assessment provides an approximate overview of the seriousness or risk associated with a particular issue soon after it has been reported, and is used for prioritizing multiple hazards and applying resources. It is also used to establish the level of management responsible for authorizing the hazard mitigation [Ref. 1]. For example, the mitigation or corrective action, or acceptance of risk of higher-severity hazards, usually requires authorization at a higher level of management or a higher rank in the military. Operational system safety often attracts more attention from management because of the potential consequences and the financial risk to a company, compared to hazards identified during development. Quantitative Risk Assessment (QRA) is "preferable to qualitative analysis" if appropriate and representative data is available [Ref. 4]. In aviation, the FAA has been encouraging wider application of QRA since 2010. The FAA explains how to "analyze continued operational safety (COS) data and monitor safety in aircraft fleets" using the Monitor Safety/Analyze Data process, which is essentially Quantitative Risk Assessment [Ref. 4].

Impact of Later System Safety Involvement

Comparing the development system safety process to the operational system safety process initially might suggest that the former is more complex and labor intensive. However, the opposite is true because of the need to mitigate or eliminate hazards on designs that have been delivered and are operating in the field. Mishap risks identified during development are theoretical, whereas mishap risks identified in operation are actual and mishaps might occur if risks are not addressed promptly. Safety risks identified during fabrication, testing and production must be addressed and may require corrective action involving redesign, manufacturing new parts, additional testing and other activities. Manufacturers of aerospace systems and many other products are responsible for maintaining safety of the design of products that have been delivered, and corrective action is required whenever unsafe or hazardous conditions are discovered during operation. Ensuring continued operational safety can be costly. These costs can escalate rapidly depending on the number of products in service that would require corrective action to mitigate or eliminate the risk. With the rise of social media and smart technology, news of any event that may occur can spread quickly, exposing the company to public relations issues as well.

Potential hazards may be identified during maintenance or operation, or an incident or accident might occur, requiring that an investigation be conducted to determine if a hazard could exist on other products of the same design. This investigation can consist of many steps, such as interviewing operators, reviewing

maintenance manuals to understand if procedures for maintenance and operation are adequate, and reviewing records to determine if the reported event had occurred previously. For events related to a specific component, the manufacturer will generally require return of the unit for examination, analysis or testing. This could involve examination by materials failure analysts, various engineers, control systems experts or similar specialists, depending on the system affected.

The realization of a hazard in the field does not always occur immediately when an event occurs. A hazard might not be evident until multiple events have occurred, trends have been identified and investigations have been conducted. Except in extreme cases, new products continue to be delivered that are susceptible to the same hazard, adding to the number that will require corrective action. Hazards identified during the development phase are generally routine business for which staffing and funding can be planned. Hazards discovered in operation can stress the resources of the manufacturer. An unanticipated field event that is found to be a hazard can demand much attention and activity, involving many employees from many functional groups.

> "It has been suggested that earlier system safety involvement could contribute to reducing these (legal) costs — first, by reducing or eliminating the risk of mishaps and, second, by providing material in support of the defense, should a mishap occur."

Cost

Calculating the cost benefit of investing in system safety is a perennial challenge illustrated by the common phrase, "How do you measure nothing?" This refers to determining the cost savings from an unknown number of mishaps that did not occur. In his book *Clif's Notes on System Safety*, Ericson states, "It is difficult to determine how much has actually been saved via a proactive designed-in system safety program" [Ref. 5]. The author writes, "One reason decision makers like to avoid necessary investment cost is because the results of the investment expenditure are usually not apparent or visible." Despite not being "apparent or visible" at the time of the expenditure, it can be shown that, in the long term, preventive action is less expensive than corrective action. Numerous specific and unspecific costs are incurred when mitigation of risks is required later in the product lifecycle. The approach taken here is to identify the resources (personnel) required for risk mitigation or elimination of a hazard identified in development compared to those of a hazard identified in operation, to estimate the labor cost difference and to add an estimate of the cost of any required parts. If hazards realized in the field are catastrophic, serious injury or death may occur. The costs presented are those that might be identified in typical manufacturing and customer service organizations.

Schedule

Correcting a hazard discovered in the design phase requires a redesign of the system that could involve many resources. During the conceptual design phase, a schedule slip might occur while the design is modified to correct a hazard identified by an analysis. A hazard identified later, when more of the system design has been completed, could result in a longer delay. As the design and development process continues into fabrication of parts, component testing, system testing and eventually into full-scale testing, the corrective action for identified hazards can require more and more time, leading to significant program delays and missed milestones. Beginning system safety activities early can greatly reduce the likelihood of major schedule slips.

Resources

Hazards detected after a system has been fielded require corrective action to ensure the continued safe use of that system. This can reduce productivity and impact the ability to introduce new products because employees designing new products may be redeployed to products that have moved from design and development into production and operation. In some extremes, the manufacturer may need to hire additional employees to provide the support required for this work. Implementation of corrective actions also requires resources that would not be needed if hazards were identified earlier in development. Hazards identified after numerous units have been delivered to customers and are operating in the field may require additional steps, such as recall, customer notification, logistics support and field service engineers.

Reputation

The reputation of a manufacturer can be damaged if a product fails in a manner that causes injury or death. A

tarnished reputation may reduce future sales and, more immediately, could impact the stock value of a publicly traded company. One economics master's thesis studied the effect of airplane crashes on the stock value of airlines and aircraft manufacturers [Ref. 6]. The thesis covered incidents from 1983 to 2013 and hypothesized that airplane crashes can negatively impact stock performance. This hypothesis was confirmed and showed that the stock prices of both airlines and manufacturers perform negatively after a crash, but the airline stock performance declined more than the manufacturer stock. This could discourage future purchases from that manufacturer.

Litigation

If a mishap occurs, litigation is almost a certainty, resulting in high costs regardless of the outcome. These high costs result from the many hours required for internal legal staff to prepare a legal defense, the high hourly labor rate, the high cost of outside legal professionals, expert witnesses and other supporting staff, court costs and other fees required for the defense, even if the defense is successful. Should the case be decided in favor of the plaintiff, much higher costs may be incurred, in addition to legal costs. In product liability cases involving serious injuries or fatalities, awards of tens of millions of dollars are not unusual.

It has been suggested that earlier system safety involvement could contribute to reducing these costs — first, by reducing or eliminating the risk of mishaps and, second, by providing material in support of the defense, should a mishap occur. For example, "…when considering product liability cases, courts take into consideration whether a safer alternative design exists that would not destroy the product's usefulness" [Ref. 7].

A legal distinction between inadvertent design errors and conscious design choices can be made [Ref. 8].

EFFECTIVENESS

Mitigation Method	Description
A. Eliminate hazard through design	Ideally, the risk of a hazard will be eliminated. This is often done by selecting a design alternative that removes the hazard altogether.
B. Reduce mishap risk through design	If the risk of a hazard cannot be eliminated by adopting an alternative design, design changes must be considered that reduce the severity and/or the probability of a harmful outcome.
C. Engineered Safety Feature (ESF)	If unable to eliminate or adequately mitigate the risk of a hazard through a design alteration, reduce the risk using an ESF that actively interrupts the mishap sequence.
D. Incorporate safety devices	If unable to eliminate or adequately mitigate the hazard through design or ESFs, reduce mishap risk by using protective safety features or devices. In general, safety devices are static interveners.
E. Provide warning devices	If design selection, ESFs or safety devices do not adequately mitigate the risk of a hazard, include a detection and warning system to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.
F. Develop procedures and training	Where other risk reduction methods cannot adequately mitigate the risk from a hazard, incorporate special procedures and training. Procedures may prescribe the use of personal protective equipment.

COST

Figure 3. System Safety Order of Design Precedence

“When the hazard is identified early in the design phase, the actual cost of incorporating a design change to eliminate the hazard can be less than the cost of implementing less-effective measures to mitigate risk later in the product lifecycle. Earlier completion of system safety analyses permits corrective actions to be implemented at a higher level in the system safety order of design precedence, and usually at a much lower cost.”

Inadvertent design cases may result from the design engineer not fully envisioning the implications of the various elements and failure modes of the design. Conscious design choices, however, suggest that the risk of harm from the product resulted from the conscious decision of the design engineer to trade off safety in favor of increased product performance or reduced costs [Ref. 8].

Effect on System Safety Order of Design Precedence

The Federal Aviation Administration (FAA) *System Safety Handbook* states that the “goal of System Safety is to optimize safety by the identification of safety related risks, eliminating or controlling them by design and/or procedures, based on acceptable system safety precedence” [Ref. 3]. The system safety order of precedence identifies elimination and mitigation approaches and lists them in order of decreasing effectiveness:

1. Eliminate hazards through design selection.
2. Reduce risk through design alteration.
3. Incorporate engineering features or devices,
4. Provide warning devices.
5. Incorporate signage, procedures, training and personal protective equipment, which is not to be used as the sole mitigation for a severity I hazard (generally, potential for fatalities) or severity II hazard (generally, potential for injuries) [Ref. 9].

Figure 3 illustrates conventional types of corrective action for identified hazards. As noted in the *FAA Handbook*, it is always preferred to implement the highest possible type of corrective action. Earlier completion of system safety analyses permits corrective actions to be implemented at a higher level in the system safety order of design precedence. For example, if a system safety analysis highlights the need for a redesign late in the design phase, the cost and schedule impact might drive alternative mitigation approaches which may have lower effectiveness.

Figure 3 also illustrates the effectiveness of the corrective action approach, where the cost is shown to be reduced if the corrective action is applied during the same design phase. When the hazard is identified early in the design phase, the actual cost of incorporating a design change to eliminate the hazard can be less than the cost of implementing less-effective measures to mitigate risk later in the product lifecycle. Earlier completion of system safety analyses permits corrective actions to be implemented at a higher level in the system safety order of design precedence, and usually at a much lower cost.

Case Studies

It was found that accurate data are most readily available for aircraft examples, which are shown here. However, the same principles should be applicable to other products. The examples described in this paper are based on actual cases and most are in the public domain. Some aircraft cases have been extracted from FAA records that are available to the public. However, specific product manufacturer, model, date and other identifying details are not reported here and are not relevant. The intent of this paper is to illustrate the advantages of early system safety influence for cost and schedule; those advantages are universal and apply to all products worldwide. In some cases, the current system safety process was not a civil or military require-

ment at the time of the design and development of the product. Had the product been developed at a later time when the process was required, it is likely that the issue would have been identified and the design corrected prior to production. Noncompliance with requirements is not presumed, investigated or discussed in this paper. It is presumed only that earlier discovery of system characteristics through system safety analyses would have identified the need for changes earlier in the design, development and production, which could reduce schedule slippage, cost escalation and the consequences of fleet retrofits.

Cost estimates in these case studies have been developed as described in the Cost section. The labor rate could vary widely depending on many factors, such as the country where the work is performed, local economic and employment conditions, the availability of specialists in the particular field, and other factors. Therefore, a labor rate of $100 USD per labor hour was applied for all engineers, technicians, managers, pilots, and other technical and administrative workers as a reasonable average. Where corrective action was mandated by an FAA Airworthiness Directive, the cost of performing the work on the product was based on the methodology used by the FAA. It is important to be aware that the costs presented are estimates, based on experience, and are useful only for comparative purposes to illustrate the advantage of early system safety influence in the rotorcraft design. Actual costs would be different. Also, the cost of corrective action might be borne by the manufacturer, the customer, a branch of the U.S. military or foreign military, or a combination of parties. This is not relevant, and no attempt has been made to associate any cost with any entity.

Case Study 1: Effect on Control of a Helicopter Leading to a Large Increase in Crew Workload

In this case an aircraft was in the development phase and a System-Level Functional Hazard Assessment (FHA) had been created for the design. During the development system safety process, the FHA identified two hazards for the flight control system affecting the Stability Augmentation System (SAS). The SAS assists the pilot in maintaining control of the aircraft during interaction with outside forces, such as wind. Fault trees were created for hazard verification and the fault tree analyses revealed that the system did not meet reliability requirements for the criticality of the system. Both hazards could affect control of the aircraft, leading to a large increase in crew workload to regain control. The architecture of the system was redesigned to improve reliability. Identification of this hazard within the development process prevented the original design from being implemented on a fielded aircraft. The estimated cost of corrective action is $40,000.

Case Study 2: Aircraft Lack of Electrical Distribution Redundancy to Critical Components

A potential loss of electrical power to critical components was discovered during flight testing. It was determined that there was a lack of redundancy, so the hazard elimination required significant modification to the electrical distribution system, along with adding an additional power supply and other changes to add the required redundancy. This resulted in significant redesign, development, testing, certification, fleet retrofit labor and fleet retrofit parts for a small number of aircraft. The cost estimate includes the small number of aircraft that required the modification, the labor hours required for the modification, and an approximation of the parts cost, although the actual parts cost is unknown. The estimated cost of corrective action is $417,600.

Case Study 3: Loss of Electrical Power

This case resulted from discovery of a hazard in an aircraft electrical system on aircraft in the field. It was determined that loss of primary electrical power could occur if two generators were to fail. Loss of primary electrical power could result in loss of control of the aircraft. The electrical distribution system was redesigned and modification of aircraft in the field was necessary. Numerous resources would be involved in developing the corrective action. The cost estimate is also based on the number of aircraft that required the modification, the labor hours required for the modification and an approximation of the parts cost, although the actual parts cost is unknown. The estimated cost of corrective action was $2,768,320.

Case Study 4: Aircraft Mechanical Flight Control Single-Point Failure

In this case an aircraft design had been in service for many years and had accumulated several million hours on several thousand aircraft. A loss of yaw control was reported, and an investigation revealed that a mechanical part in the control system had fractured. Operational system safety determined that fracture of the subject part constituted a single-point failure and that corrective action was necessary. In addition, a derivative model using a similar design also required corrective action. The short-term mitigation was a field inspection and the hazard elimination required a straightforward

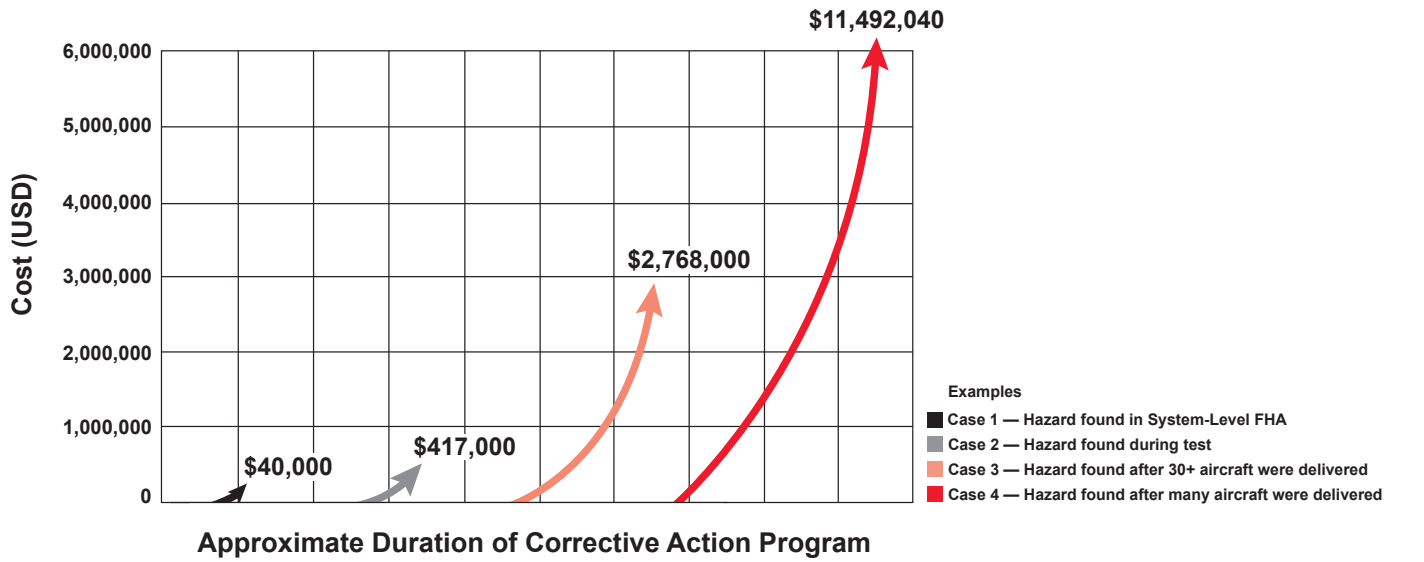


Figure 4 — Estimated cost of later system safety involvement.

design change. Retrofit of all aircraft, including derivative models, is included in the estimated cost. The cost of each part is estimated to be the same as for the original design, and the estimated total cost of corrective action is $11,492,040.

Figure 4 illustrates the estimated cost of each case and the relative duration of the corrective action program.

Conclusions and Recommendations

1. Early system safety influence in the product design process can prevent cost escalation and schedule slippage that could result if risk mitigation or hazard elimination is required later in the product lifecycle.
2. Early system safety influence also can prevent mishaps that negatively impact the reputation of the manufacturer, which could lead to additional negative consequences, such as decreased stock performance.
3. Early system safety influence in the product design process may reduce the possibility of litigation costs.
4. Early system safety influence in the product design phase can permit corrective actions to be implemented at a higher level in the system safety order of design precedence, which increases the effectiveness of corrective actions and reduces residual risk.
5. It is recommended that system safety analyses begin as early as possible in the conceptual design process and should use techniques such as colocation and close working of system safety engineers and designers.

References

1. U.S. Department of Defense. Military Standard MIL-STD-882, "Standard Practice for System Safety," 1969.
2. International System Safety Society. "The System Safety Concept," http://www.system-safety.org/about, retrieved March 28, 2018.
3. Federal Aviation Administration. *FAA System Safety Handbook*, 2000.
4. Federal Aviation Administration. FAA Order 8110.107, "Monitor Safety/Analyze Data (MSAD)," 2010.
5. Ericson II, Clifton A. *Clif's Notes on System Safety*, CreateSpace, Inc., Charleston, South Carolina, 2012.
6. Homar, Ambrož. *The Effects of Airplane Crashes on Stock Performance of U.S. Airlines and Airplane Manufacturers between 1983 and 2013*, Master's Thesis, University of Ljubljana, Slovenia, September 2015.
7. Rottenstein Law Group. "What is a 'Design Defect'?" http://www.rotlaw.com/legal-library/what-is-a-design-defect, retrieved June 1, 2018.
8. Twerski, A.D., A.S. Weinstein, W.A. Donaher and H.R. Piehler. "The Use and Abuse of Warnings in Products Liability-Design Defect Litigation Comes Of Age," *Cornell Law Review*, Vol. 61, No. 4, April 1976.
9. U.S. Department of Defense. Military Standard MIL-STD-882E, "Standard Practice for System Safety," 2012.