ELEVENTH AIR NAVIGATION CONFERENCE

Montreal, 22 September to 3 October 2003

Agenda Item 2: Safety and security in air traffic management (ATM)
2.5: Safety and security of the ATM infrastructure

DEFINING A FRAMEWORK FOR SYSTEM SAFETY AND INFORMATION SECURITY TO PERFORM COLLABORATIVE RISK MANAGEMENT

(Presented by the United States)

SUMMARY

In the overall goal of building safe, secure, and efficient systems, aligning system safety and information security disciplines within a system engineering methodology can aid in achieving an effective system solution. The foundation of which lies in managing system safety and information security risk associated with the system throughout its lifecycle. A collaborative system safety and information security risk management revolves around four primary activities. Adverse event identification aids in capturing system hazards and vulnerabilities. The adverse event effect and risk level determines what undesirable situation can occur and rates the severity and probability of each adverse event item. Requirements balance resolves conflicting and overlapping requirements drawing the participants towards a consensus about project priorities. Finally, balanced requirements are incorporated into the system specification for system design and implementation.

REFERENCES

1. Gary Stoneburner, Clarke Hayden, Alexis Feringa; Engineering Principles for Information Technology Security — A Baseline for Achieving Security, NIST, SP 800-27, June 2001
2. Ronald Stroup, Warren, Naylor; Cost and Schedule — The Overlooked Hazard, International System Safety Society Conference Proceedings, September 2001
3. FAA System Engineering Manual, Introduction (February 27, 2002)
4. Harold Roland, etc.; System Safety Engineering and Management, Wiley and Interscience, 1990.
5. Ross Anderson; Security Engineering, Wiley, 2001
6. NSA, Information Assurance Technical Framework, Release 3.0, October 2000
7. NAS Modernization — FAA System Safety Management Program, May 1, 2001
8. Naylor, Warren, Everett, William; Technology Refresh Management Working Paper, 2002
9. Richard L. Baskerville, Jan Stage; Controlling prototype development through risk analysis, MIS Quarterly, December 1996
10. Military Standard System Safety Program Requirements, MIL-STD-882C, January 19, 1993
11. John H. Gibbons, Cybernation: The American Infrastructure in the Information age, July 18, 2003
12. Simon Mingay; Risk Management 2002 and Beyond; Formal and Integrated, Garter Group, 2001

1. INTRODUCTION

1.1 In these times of limited resources and an increased focus on security, a policy that encourages a comprehensive risk management strategy is essential. An effective risk management strategy must operate within the system-engineering lifecycle environment in order to achieve balance among the various engineering specialties. This paper will evaluate system safety and information security engineering principles, discuss a common risk management strategy, and address the importance of collaborative risk management system. In summary, this paper will identify the technical, programmatic, and economical benefits that can be achieved by implementing a collaborative risk management strategy.

2. DISCUSSION

2.1 Principles of system safety and information security engineering

2.1.1 Engineering principles provide a foundation in which a more consistent and structured approach to the design, development, and implementation of systems can be applied (ref. 1). Depending on the purpose of the system, the following list may represent the pertinent specialty engineering areas: safety; reliability, maintainability, availability (RMA); human factors; electromagnetic environmental effects (E^3);

quality; security; and hazardous materials. As system complexity increases, so does the risk of conflicting requirements. With the high degree of commonality between safety and information security goals, an effective means of coordinating the program specific principles is essential. These principles provide an organization with a strategy for developing and sustaining safe and secure systems.

2.1.2 Engineering principles that are applicable to both system safety and information security are (ref. 1):

a) Establish a sound safety and security policy as the foundation for design.

b) Treat system safety and information security as an integral part of the overall system design.

c) All system operations represent some degree of risk.

d) Reduce risk to an acceptable level.

e) Identify potential trade-offs between reducing risk and increasing costs and decrease in other aspects of operational effectiveness.

f) Strive for simplicity.

g) Design safety and security to allow for regular adoption of new technology, including a safe, secure, and logical technology upgrade process.

h) Do not implement unnecessary risk mitigation mechanisms.

i) Identify adverse events and prevent common hazards and vulnerabilities.

2.1.3 The complexity of integrated systems makes it extremely difficult to fully assess the risk. Initially, organizations perform a qualitative risk evaluation. These initial evaluations are often unstructured and misrepresent the true risk within the system. A formal assessment often occurs later in the lifecycle when cost and schedule factors become the primary drivers. When faced with cost and schedule overruns, organizations tend to circumvent standard development processes, reduce system functionality and reduce integration testing (ref. 2). Circumventing basic system engineering steps results in increased risks that become difficult to mitigate later in the lifecycle process.

2.1.4 A collaborative risk management strategy starts with integrating the safety and information security risk management processes. Before an effective risk management strategy can be discussed, some key terms must be defined to establish a common framework for the remainder of this paper.

2.1.5 *System Engineering*: System engineering concentrates on the design and application of the whole (system) as distinct from its parts. It involves looking at a problem in its entirety, taking into account all the facets and all the variables and relating the social to the technical aspects (ref. 4).

2.1.6 *System Safety Engineering*: System safety engineering is a discipline that focuses on the design and application of the system to ensure it will not endanger human life or the environment (ref. 4).

2.1.7 *Security Engineering*: Security engineering is a discipline that focuses on the tools, processes, and methods needed to ensure a system remains dependable in the face of malice, error, or mischance and to adapt existing systems as their environment evolves (ref. 5).

2.1.8 *Adverse Event*: Adverse event is a common term created for this paper to bridge similar terms with different perspectives on the same event. [A hazard is caused by a random failure while a threat/vulnerability pair can be exploited by a malicious act].

2.1.9 *Hazard*: A hazard may be defined as a potential to do harm (ref. 4).

2.1.10 *Vulnerability*: Vulnerability is defined as a weakness that can be exploited to develop an attack against the system or the type of protection that a countermeasure is to provide (ref. 6).

2.1.11 *Risk*: Risk is the composite of severity and likelihood of the outcome/effect of the hazard or vulnerability in the worst credible system state (ref. 7).

2.1.12 *Relation of Definitions*: The system engineering methodology provides a structured approach to developing a system by coordinating the efforts of all engineering disciplines pertinent to the development of that system. In using the term discipline, it tends to reflect that system safety engineering and information security engineering is a part of the larger methodology. The system safety and information security disciplines are structured approaches focused on selecting an effective solution that balances the operation of the system and the risk to that operation in achieving adequate safety and information security. An effective solution includes identifying the customer's requirements, determining the initial risk, assessing the identified risk, determining applicable risk mitigation techniques, identifying residual risk and implementing a risk management strategy. The alignment of system safety and information security principles within a system engineering methodology ensures a cost effective approach is applied in the development of safe, secure, and efficient systems.

2.2 **Risk management strategy**

2.2.1 An integrated product development system is broken down into a number of lifecycle phases, which include: Mission Analysis, Investment Analysis, Solution Implementation, and In-Service Management. Although risk management is an integral process with defined activities during each phase of development, the risk products from the various analyses will vary depending on the phase of the lifecycle.

2.2.2 *Risk Activities*: There are four activities associated with an effective risk mitigation strategy which serves to identify and assess safety and information security risk requirements for incorporation into the system specification. The activities consist of: adverse event identification, assessing the adverse event effect and risk level, achieving requirements balance, and incorporating a balanced set of requirements into the system specification as in Figure 1. The risk management process must operate as an integral part of the systems engineering environment. The prime goal of the risk management program is the early identification and continuous control of the adverse event in the enterprise. Additionally, obsolescence of new technologies occurs far more frequently than the legacy technologies of the past, which can serve as a source of risk to the system. Implementing an effective technology refresh plan is critical to ensuring the safety and security of the system throughout its projected lifecycle (ref. 8).

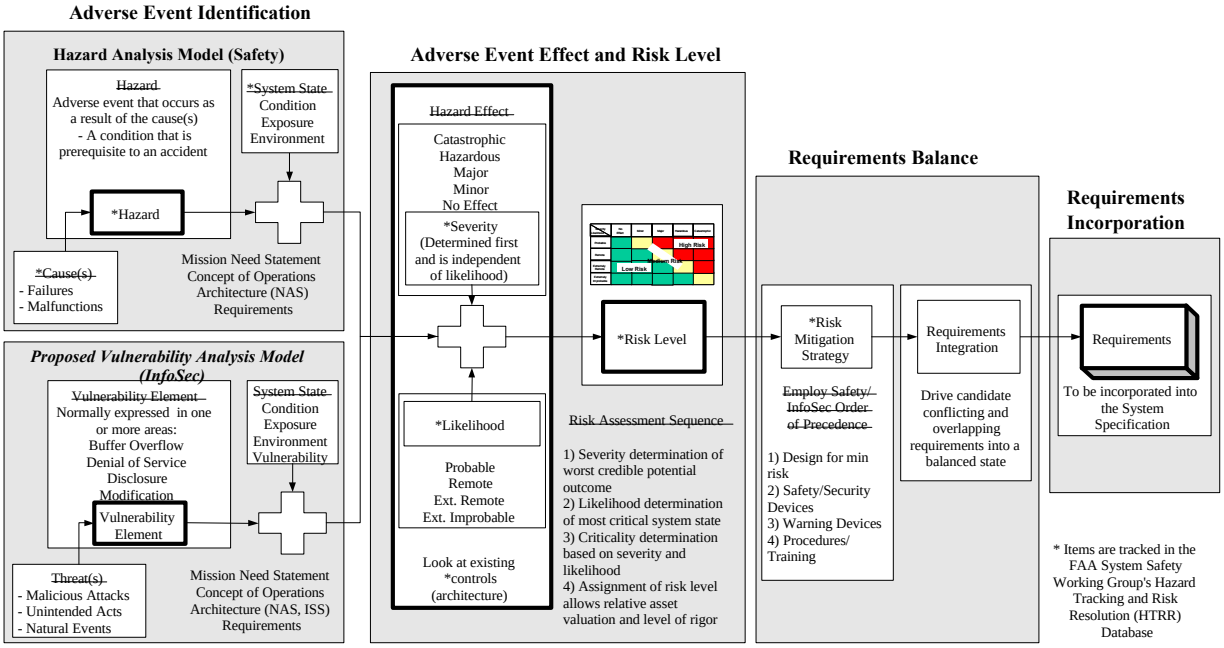

Figure 1. Risk management strategy

2.2.2.1 *Adverse Event Identification*: With the ever-increasing complexity of systems, incident analysis can require an extremely detailed process to thoroughly understand the what, why and how of system failure or compromise. Adverse event identification starts with an evaluation of the Mission Need Statement, Concept of Operations, System Architecture, and operational environment. A hazard exists regardless of whether it is from a safety or security perspective. Modeling of the processes behind incidents and accidents is an effective means of defining the relationship between causes, threats, hazards, vulnerabilities, system states, and effects for the purpose of managing risk. The potential outcome describes an effect, which is the first component in making an evaluation of risk. The system safety and information security should agree on those hazards that are common and unique to their disciplines.

2.2.2.2 *Adverse Event Effect and Risk Level*: Specifying the consequences of a hazard will allow the group to consider what undesirable situation could result if the hazard occurs and prepares the team to rate the severity and probability for each hazard item (ref. 9). Varying degrees of effect or severity can occur which may take the form of death, injury, loss of mission capability, damage to property, or damage to the environment. For the evaluation of the severity to be of value, severity must be determined in the worst credible system state at a minimum. The second component of risk is the likelihood of occurrence of the severity being realized. Each hazard has its own likelihood of occurrence. Based on various analysis methods, the worst-case hazard effect is determined. The combination of hazard severity and likelihood of occurrence results in that risk rating. Once all risks have been assigned to the risk index, management can clearly see those risks that pose the greatest threat to the program. System safety and information security must agree on the risk rating for those hazards that are common.

2.2.2.3 *Requirements Balance*: The system safety and information security professional's focus is on the engineering processes. The goal is simple: ensure a safe, secure, and efficient development and deployment of a system using an agreed upon order of precedence (ref. 10). The recommended order of precedence is:

a) Design for minimum risk.

b) Incorporate safety and security features.

c) Provide safety or security warning devices.

d) Develop procedures and training.

2.2.3 Based on this process a set of candidate requirements will be developed that mitigate each risk. However, in large complex systems there may be hundreds of risks with multiple requirements. This may result in conflicting and/or overlapping requirements.

2.2.4 Integrated risk resolution provides a collaborative mechanism that draws the participants toward a consensus about project priorities (ref. 9). Conflicting and overlapping candidate requirements will be driven to a balanced state for incorporation into the system specification. A set of risk mitigation objectives should be used to identify potential conflicting and overlapping requirements. The expertise needed to carry out the process activities will come from systems engineering, safety engineering, security engineering, and domain experts. During this activity the team must consider not only the cost of the various requirements, but also the impact on performance (ref. 6), interoperability, and maintainability.

2.2.5 In order to balance risk mitigation requirements, an organization must normalize the risks across the safety and information security disciplines. This normalization can be done through the use of well-known security services; but for the sake of integration, this paper will identify them as risk mitigation services. The risk mitigation services consist of confidentiality, integrity, availability, and accountability (CIA^2). The process evaluates the various mechanisms to be applied and attempts to define a single set of risk management requirements for the project team. These mechanisms are broken down into the basic services or combination of services that are needed. For example, the safety organization has identified a requirement for the system to employ a checksum to ensure the integrity of critical information. At the same time, the information security organization has identified the requirement for encryption of the same information to ensure the confidentiality and integrity of the information.

2.2.6 Risk mitigation services allow a common ground to be established for the safety and information security organizations to have informed discussions. In the example, the process should result in the safety requirement being removed in favor of encryption, which would provide the required integrity as well as confidentiality. This process would remove the difficult task of determining which conflicting or overlapping requirements to implement or not from the program manager to a risk management group. The output of this process would be a single set of risk management requirements to complement the system functional and interoperability requirements.

2.2.7 *Requirements Incorporation*: The balanced set of risk management requirements would be considered in the initial program baseline. At this point, the program manger can focus on implementing all the requirements rather then trying to determine which requirements are not affordable. Initial and derived requirements can be identified in this manner during the various stages of the system lifecycle.

2.3 Importance of integrated risk

2.3.1 Different domains of risk should not be seen or managed in isolation; they are interrelated and potentially affect the enterprise's stakeholders (ref. 12). The events of September 11, 2001 revealed the need to accelerate the evolution of integrating the system safety and information security disciplines on managing risk to build greater resilience into their operations.

2.3.2 For any risk management effort to succeed there must be a commitment on the part of management. There must be mutual confidence between the program and risk management organization. Program managers must have confidence that risk decisions are made with professional competence. Risk management and engineering must know that their actions will receive full program management attention and support. System safety and information security personnel need to have a clear understanding of the risk management tasks along with the authority and resources to accomplish the tasks.

2.3.3 An approach that seeks to manage risk by weighing cost, performance, and reliability tradeoffs along with the likelihood and severity of specific hazards or vulnerabilities is the most sensible (ref. 11). Decision-makers need to be fully aware of the risks they are accountable for when they make their decisions. What needs to emerge is a unified framework to manage risk across multiple domains and ensure the enterprise is not taking on unacceptable risk (ref. 12) knowingly or unknowingly.

3. CONCLUSION

3.1 The collaboration of system safety and information security throughout the system development lifecycle is advantageous for the following reasons. First, system development goals can more effectively be achieved when system safety and information security issues are resolved and risk mitigation requirements are implemented during the design. Second, it is less expensive and obtrusive to integrate risk mitigation requirements in the design than to force them at the end. By leveraging the engineering principles, the foundation of managing system safety and information security risk can effectively pursue adequate levels of system safety and information security.

3.2 The benefits to be achieved can be significant. The technical perspective can result in reduced complexity in system designs and a balanced set of risk mitigation requirements. The programmatic perspective can result in better alignment with the system engineering lifecycle and simplified management by the program regarding the implementation of risk mitigation requirements. The economic perspective should yield a more accurate program baseline, reduction in significant late requirements, and a higher probability of maintaining cost and schedule targets. This also allows for phased or spiral development, which may increase the likelihood that safety and security requirements are implemented. (NOTE: it is a rare program that can fund all the safety/security requirements at "proof of concept" phase or during early deployments. Safety/security requirements should be prioritized based on risk mitigation strategy, even IF requirements are fully funded.)

3.3 System safety and information security disciplines are critical elements in the system lifecycle. These disciplines should be incorporated and addressed from the mission analysis phase through in-service management of the system. Without proper attention, an organization's development process can become a source of significant mission risk. Failure to understand the system hazards upfront and develop mitigating requirements, places your organization in a reactive mode to which it may not achieve the desired level of safety or security and almost always doom it to cost and schedule overages for its lifecycle.

— END —