2001-01-2641

The Coupling of Operational Safety and INFOSEC Assessments [1]

Marshall D. Abrams and Mark Joseph [2]
The MITRE Corporation

ABSTRACT

This paper describes an approach to integrating security and safety analysis of an Air Traffic Service (ATS) using the security assessment as an additional input to the risk management process. This approach helps address potential problems in coordinating safety and security requirements such as: different system models used for safety and security; different documentation structures for the analyses and their results; and the practice of isolating safety and security requirements processes. What motivates this approach is the overlap between security and safety considerations in the identification of hazards and associated risk management strategies.

INTRODUCTION

It is reasonable to ask whether safety assessments and Information Security (INFOSEC) analyses done for approval of an ATS can be more effectively coordinated and integrated. Both INFOSEC and Safety analyses attempt to identify potential loss or malfunction of a service. Historically safety studies have focused on Reliability, Maintainability, and Availability (RMA) based on system failures as the causes for the interruption or corruption of a service. INFOSEC analyses on the other hand have focused on a functionality or data loss, or a system malfunction caused intentionally by the action of adversarial or malicious people. Our goal is as a matter of course to link the INFOSEC analysis to the ongoing safety analysis and articulate the INFOSEC risk impact on the Safety analyses. A new methodology in use at the Federal Aviation Administration (FAA) termed the Operational Safety Assessment (OSA) facilitates this linkage.

This incorporation of INFOSEC analysis into safety analysis becomes a natural thing to do because of the nature of the OSA itself, namely that it begins with an identification of ‘operational’ hazards that are derived from the way the service is used in operation. Only after the operational hazards are classified are the causes and mitigations considered. INFOSEC attacks become another ‘cause’ in the safety analysis. The ‘naked’ hazard, that is the hazard stripped of what otherwise might be reasonable environmental assumptions, becomes at once more severe and of indeterminate probability.

There are various approaches to integrating security and safety analysis. Eames [1] investigates safety and security requirements specification methods, and proposes techniques for the integration of contrasting methodologies, employing an example of requirements specifications of an Air Traffic Control system to highlight the problems inherent in the independent approach to requirements development. Areas that can cause problems in attempting to harmonize safety and security requirements techniques include: different system models used for safety and security; different documentation structures for the analyses and their results; the interaction of safety and security requirements; and the isolation of safety and security requirements processes.

Separate INFOSEC analysis and OSA will identify most, if not all, of the same operational hazards, demonstrating considerable overlap between security and safety assessments in terms of the identification of the hazards and determination of hazard management strategies. In the recommended analytic approach, the INFOSEC analysis is used to refine the OSA by retaining events that have a low probability of occurrence when viewed as statistical failure probabilities, but a relatively high probability when viewed as deliberate attacks. Compound failures may fit this description. For example, the statistical probability of failure of communication on all channels may be considered acceptably low, but the probability that an attacker would attempt to block communications on multiple channels simultaneously cannot be dismissed. Consideration of this INFOSEC attack motivates increased attention to the operational

[1] The contents of this material reflect the views of the authors. Neither the MITRE Corporation, nor the Federal Aviation Administration, nor the Department of Transportation makes any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein. MITRE's efforts were sponsored, in part, by the Federal Aviation Administration under contract DTFA01-93-C-00001.
[2] Current affiliation: Department of Energy.

Presented at SAE Advances in Aviation Safety Conference, Seattle, WA. September 11, 2001.

hazard of total loss of communications–failure of primary communications and simultaneous failure of the backup.

BACKGROUND

INFRASTRUCTURE PROTECTION – Technological infrastructure constitutes a vulnerability that can be exploited by malicious and hostile interests. The severity of the consequence will depend on the intensity of the attack, which is closely correlated with the resources available to the attacker. As identified in *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications* [3], malicious organizations may be directly or indirectly supported by governments hostile to the United States. Presidential Decision Directive (PDD) 63 [4] mandates protection of the critical National Information Infrastructure (NII).

AIR TRANSPORTATION SYSTEM RESPONSIBILITY – The National Airspace System (NAS) is part of the NII. PDD 63 establishes Federal government policy for protecting the NII. The FAA is singled out for special responsibility in protecting air transportation systems. Office of Management and Budget (OMB) memorandum M-00-07 [2] reminds agencies of the principles for incorporating and funding security as part of agency information technology systems and architectures, and of the decision criteria that will be used to evaluate security for information system investments.

OPERATIONAL SAFETY ASSESSMENT – The OSA resulted from the work of a joint committee[3] of RTCA and European Organization for Civil Aviation Equipment (EUROCAE) to formulate an internationally harmonized method for the operational approval of ATS that use data communications. The committee has recently published guidance material [5]. Within the guidance material are definitions of processes that can be used and products that will serve as evidence of completion of objectives required by the approval authorities for entry into service. A brief summary of this method is given here, and is augmented by work done in the RTCA Certification Select Committee Working Group 2 to define a coordinated operational approval process. Note that while the RTCA SC-189/WG-53 terms of reference were crafted to exclude explicit consideration of security issues, the FAA must use the OSA in the context of a complete operational approval process including the INFOSEC, human factors, and all other operational suitability dimensions.

OPERATIONAL SERVICES AND ENVIRONMENT DEFINITION

An Operational Services and Environment Definition (OSED) is needed to initiate the safety assessment process because in general the environment in which the services are rendered affects the risks associated with the delivery of those services. The OSED has components that describe airspace characteristics, operations, and required functional characteristics. Although the SC-189/WG-53 terms of reference limited the scope of the work to the required communication characteristics in terms of derived results, the other components of required total system characteristics must be described as part of the operational environment.

An even-handed treatment of required total system characteristics is necessary within the OSED to include required navigation characteristics, required surveillance characteristics, and required control characteristics if the method is to be used on a NAS-wide basis. ‘Even-handed’ means that these characteristics are defined within the OSED, and that updates to all characteristics are possible as a result of the safety, performance, or interoperability analyses. Efforts are well underway within the FAA to use the method in this more general sense.

The OSA consists of two parts: an Operational Hazard Assessment (OHA), and an Allocated Safety Objectives and Requirements (ASOR). The OHA is the process by which the hazards associated with the OSED, or with the proposed changes to an existing OSED, are identified and classified. This is done without regard for the causes of the hazard and is therefore applicable to the INFOSEC analysis. We have used the format given in Table 1 as illustrative. Hazard ‘severity’ is assigned in accordance with the Hazard Classification Matrix (HCM) given in Table 2 [5].

The ASOR process allocates safety objectives and requirements to the aircraft, ground, and aircraft operator segments; or, more generally, to those segments identified within the OSED. It is at this step that the different causes of the operational hazard are identified and strategies are developed to cover each unacceptably likely cause. Our suggested format for an ASOR document is given in Table 3. In this table, the actions taken to manage each identified risk are presented in detail. Derived environment characteristics are fed back to the OSED to formulate an update to that document as a result of the completed and coordinated ASOR. Coordination of the ASOR with all stakeholders is essential.

Overall safety objectives are determined in accordance with the risk classification matrix given in Figure 1. This matrix assigns to each severity level an acceptable target for likelihood of occurrence of 'Probable', 'Remote', Extremely Remote', and 'Extremely Improbable'. Each combination of severity and likelihood of occurrence is considered to be acceptable, minimum acceptable, unacceptable, or minimum acceptable/unacceptable with a single point/common cause failure.

The quantitative targets for the 'likelihood' designations, such as 'Extremely Improbable,' must be agreed upon within the coordinated operational approval planning

[3] RTCA SC-189/EUROCAE Working Group 53, Safety and Interoperability of ATS Supported by Data Communications

process. These targets become one of the characteristics of the environment documented in the OSED as objectives of the airspace. Whether for safety objectives or more generally for matters of operational suitability, whenever quantitative analysis is required agreement must be reached on these matters within the coordinated operational approval planning process. Where the choice of scale is made in accordance with FAA Advisory Circular AMJ 25.1309 guidance for the aircraft segment, severity levels 1 through 5 are taken as in that FAA guidance to be 'Catastrophic', 'Hazardous', 'Major', 'Minor', and 'No Effect', with their corresponding targets for likelihood of occurrence.

SAFETY, PERFORMANCE, AND INTEROPERABILITY REQUIREMENTS

SAFETY AND PERFORMANCE REQUIREMENTS (SPR) – Requirements derived through the OSA and parallel Operational Performance Assessment (OPA) are summarized for the approval authority within the Safety and Performance Requirements (SPR) standard. Safety and performance-based requirements for the ATS, and operational or functional capability are given and the accepted risk management strategy for each hazard is enumerated for allocation in its parts to each responsible organization. The qualitative statement for each safety objective is of the form: “The “’operational hazard’ shall occur no more frequently than ‘likelihood of occurrence’”. Or, as a more explicit example, “A deviation from the cleared route of flight due to corruption of a clearance message shall occur no more frequently than Remote”.

Vulnerabilities due to human error and mitigation strategies are summarized in an appendix to the SPR. Human factors considerations are detailed along with safety assesment material in the ASOR. We suggest that the INFOSEC assessment results be documented similarly, as an appendix to the SPR, to avoid duplication and to provide easy reference to hazards that can be intentionally caused by an INFOSEC attack.

INTEROPERABILITY STANDARD – The interoperability standard is a generalization of the ‘interface’ specification to include those inter-segment assumptions, dynamic behaviors, and functional allocations to segments that fully characterize the technology used in the context of ATS. Different technologies may be interoperable but have different vulnerabilities to INFOSEC attack. For example, an unusual protocol may be less well known, or more complex, and not as easily attacked. A monoclonal set of protocols could all be attacked in the same way. In the case of ATS, a protocol that has an INFOSEC flaw puts information into the system that may affect aircraft control downstream from its point of insertion. The interoperability standard is another asset to INFOSEC analysis that may be employed to thwart an attack or to gauge the avenues that might be used by an attacker.

Figure 2 depicts safety performance and interoperability assessments feeding the OSED, and the evidence of these activities of the coordinated operational approval process in the form of OSED, SPR, OSA, OPA, and Interoperability Assessment documents. [6]

INFOSEC ANALYSIS

SECURITY CERTIFICATION AND AUTHORIZATION – The FAA process for verifying the security properties of an Information Technology system and authorizing its operational processing of sensitive information is detailed in the Security Certification and Authorization Package (SCAP), illustrated in Figure 3. The coupling of the Information System Security (ISS) analysis and the SCAP documentation is shown in Figure 4. Appropriate SCAP documents may be incorporated by reference in the INFOSEC appendix to the SPR as illustrated in Figure 5 to support a coordinated operational approval process.

CONSIDERATIONS FOR THE OPERATIONAL SAFETY ASSESSMENT – One difference in the safety analysis attributable to consideration of INFOSEC attacks is in the estimation of the risk associated with the hazard since the probability of occurrence is under the control of the attacker. We can envision multiple attacks, timed attacks, and constant or high-intensity attacks, such as denial-of-service attacks, having significantly increased probability of damage than if they had occurred on a statistical failure basis. The safety analysis parameter of likelihood of occurrence is replaced in the INFOSEC analysis with likelihood of attack. The former is a statistical measure based on observation while the latter is based on analysis of intelligence data indicating whether an adversary will choose to attack in this manner. The attacker with knowledge of the hazard management strategy may in general try to find ways to defeat that strategy by attacking the countermeasures [or ‘controls’]. The attacker may target the mitigation capabilities as well as the operational capability itself.

Security issues seem to motivate more strongly some of the safety concerns identified in the safety assessment. For example, deviation from the route of flight caused by a corrupted clearance is an operational hazard that is mitigated by the airspace characteristic of low air traffic density. But we may wish to not rely on this characteristic alone because of the ability of an attacker to offset the advantage of low density through the timing of an attack.

The need for development assurance to meet safety concerns for hazard avoidance will also make more difficult intentional attack on the software. Certification requirements for third-party participants such as communication service providers or aircraft operator facilities and personnel may be more strongly indicated. OSA derived architectural considerations that ensure safety may be increasingly motivated from the security risk management point of view. In any case, the OSA-derived risk management strategies must be reviewed in the context of the INFOSEC analysis to determine their robustness in the event of an INFOSEC attack on the system.

One way of proceeding is to use the security assessment as an additional input to the risk management process. This will provide additional impetus for meeting particular safety objectives when those objectives are also needed from the point of view of the independent OSA. For example, architectural considerations that promote safety, such as end-to-end application level integrity measures, that are hard to motivate via safety alone due to cost and programmatic considerations may be reinforced from the security assessment input to the risk management process. A controller display to pilot display end-to-end integrity mechanism would be a very powerful security device. A simple message integrity mechanism such as a Cyclic Redundancy Check, Message Digest, or cryptographic-based check function, could have the added benefit of simplifying the certification of the intervening systems.

Note that safety requirements are those requirements—operational, technical, procedural, and functional—that allow mitigation or avoidance of operational hazard effects or which allow compliance to some safety objectives. This does not mean that other requirements (operational and technical) do not impact safety. All requirements impact safety as the whole safety analysis is based on them, but they impact safety in a less significant way. In case of system modification, no matter what part of the system is directly impacted by the modification, the safety (and security) analysis should be completely reviewed and new safety (and security) requirements may be identified.

Features deemed required to resolve security concerns may exhibit anomalous behavior from a safety viewpoint. The objectives of “fail safe” and “fail secure” may not be compatible. The close interaction of security and safety suggests that both security and safety analysis should be iterated in order to satisfy all objectives or to identify the need for tradeoffs.

CONCLUSIONS

INFOSEC should be considered early in the safety assessment process. Introducing INFOSEC considerations into system certification at a late stage could result in severe impact to cost and schedule. Alternatively, end-to-end integrity and availability mechanisms introduced for INFOSEC reasons at the application level might ease the certification of intermediate systems. Such protocol features and procedures that make the intermediate systems transparent to end-to-end security concerns might be highly cost-effective. For example, destination address and message integrity checking ensure end-to-end application message integrity without the need to examine intermediate systems and data paths.

The safety-related INFOSEC analysis approach in this report was based, in part, on safety-related publications from RTCA SC-189/EUROCAE WG 53. This analysis recognized that INFOSEC concerns were excluded from the joint committee’s analysis. Some common mode and simultaneous failures that do not require hazard management strategies because their likelihood of occurrence is acceptably low should be considered in the INFOSEC analysis.

We recommend that INFOSEC analysis routinely treat the OSA as a baseline. The assumptions of the safety analysis contained in the OSED should be reexamined as part of the periodic determination of INFOSEC threats, risks, and vulnerabilities. Annual testing, including penetration testing, is a prudent and effective method of determining current adequacy.

We recommend using the safety and security assessment performed by experts to strengthen the resolve of those responsible for implementing measures to achieve joint safety and INFOSEC objectives and countermeasures. Architectural considerations that promote safety, such as controller and pilot display features, that are hard to motivate via safety alone due to the cost and programmatic issues may be considered viable when INFOSEC is considered.

REFERENCES

1. Eames, D. P. and J. Moffett, September 1999, “The Integration of Safety and Security Requirements,” *Safecomp99*, Toulouse, France.
2. Lew, J. J., February 28, 2000, *Incorporating and Funding Security in Information Systems Investments*, Office of Management and Budget, memorandum M-00-07.
3. National Communications System (NCS), 1999, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications*, also available at http://www.ncs.gov/n5_ia_hp/GovPub.html.
4. White House, 1998, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, also available at http://www2.whitehouse.gov/WH/EOP/NSC/html/documents/NSCDoc3.html.
5. *ED-78A/DO-264 Guidelines for Approval of the Provision and Use of ATS Supported by Data Communications, RTCA/EUROCAE.*
6. *Coordinated Operational Approval Process for Integrated CNS/ATM Airborne and Ground Systems*, Certification Select Committee Working Group 2 (CSCWG2) (draft material prepared 11/2000)

ACRONYMS

ASOR	Allocated Safety Objectives and Requirements
ATS	Air Traffic Service
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
HCM	Hazard Classification Matrix
INFOSEC	Information Security
ISS	Information System Security
NAS	National Airspace System
NII	National Information Infrastructure
OHA	Operational Hazard Assessment
OMB	Office of Management and Budget
OPA	Operational Performance Assessment
OSA	Operational Safety Assessment
OSED	Operational Services and Environment Definition
PDD	Presidential Decision Directive
RMA	Reliability, Maintainability, and Availability
SCAP	Security Certification and Authorization Package

CONTACT

Marshall D. Abrams, The MITRE Corporation, 7515 Colshire Drive, McLean, VA 22102-7508, abrams@mitre.org, 703-883-6938, fax 703-883-1397

Table 1 Operational Hazard Matrix Form

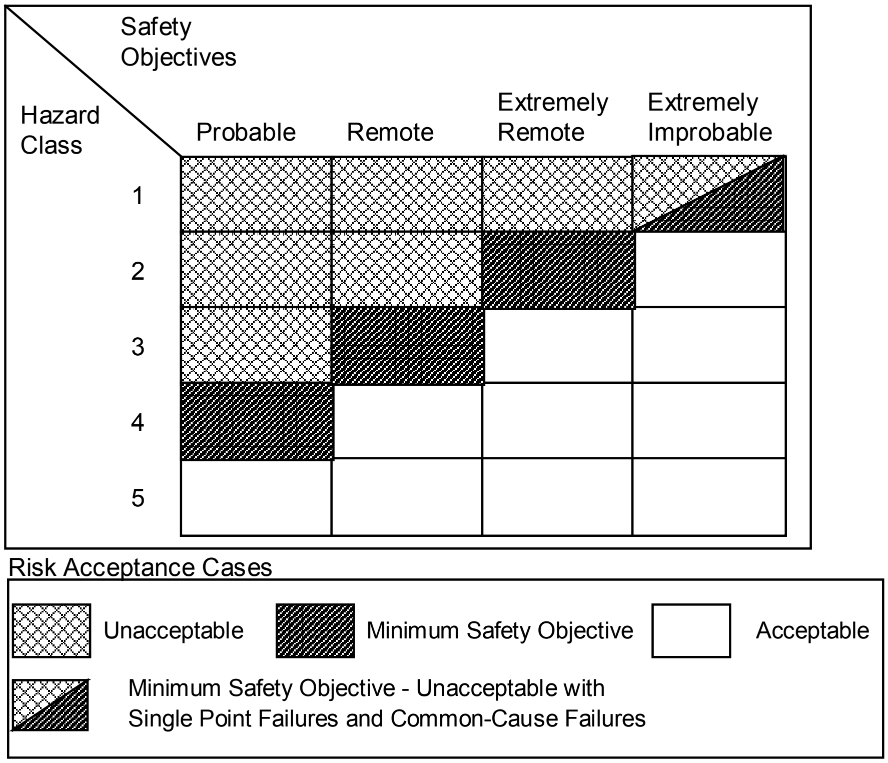
Operational Hazard	**Effect On Operations**	**Severity**	**Assumptions** **[Environment Characteristic]**
1.0 Service or Service change covered **Summary:** Summary of identified hazards and their severities.			
1.1 Hazard description	Effect of hazard on operations	Levels 1...5	Assumption made in the assignment of severity that is an assured characteristic of the operational environment. They may be airspace, procedural, or functional characteristics.

Table 2 Operational Safety Assessment Hazard Classification Matrix

Hazard Class	1 (most severe)	2	3	4	5 (least severe)
Effect on Operations	Total loss of flight control, mid-air collision, flight into terrain or high speed surface movement collision. Normally with hull loss.	Large reduction in safety margins or aircraft functional capabilities.	Significant reduction in safety margins or aircraft functional capabilities.	Slight reduction in safety margins or aircraft functional capabilities.	No effect on operational capabilities or safety
Effect on Occupants	Multiple fatalities.	Serious or fatal injury to a small number of passengers or cabin crew.	Physical distress, possibly including injuries.	Physical discomfort.	Inconvenience
Effect on Air crew	Fatalities or incapacitation	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload.	Slight increase in workload.	No effect on flight crew.
Effect on Air Traffic Service	Total loss of separation.	Large reduction in separation or a total loss of air traffic control for a significant period of time.	Significant reduction in separation or significant reduction in air traffic control capability.	Slight reduction in separation or slight reduction in air traffic control capability. Significant increase in air traffic controller workload.	Slight increase in air traffic controller workload.

Table 3 ASOR Detail Format - Example

Operational Hazard/ Safety Objective/ Cause(s)	Allocated Safety Requirements Detail	Risk Management Strategy
Entry For each Hazard Number: Hazard description as given in the OHA hazard classification table. All classified hazards are listed. **Safety Objective:** Likelihood of occurrence target that is acceptable based on the severity of the hazard identified. **Cause(s):** Enumeration of known causes of operational hazard	**Airspace Characteristic:** Identified airspace characteristics that have the potential to reduce the severity of the hazard or its probability of occurrence. For example, separation minima, throughput restriction. **Aircrew Procedure:** Identified aircrew procedural requirements **Aircraft/Avionics:** Identified aircraft or avionics functional requirements **Ground System:** Identified ground system functional requirements. **Controller Procedure:** Identified controller operational procedures. **Other Segment:** Other segment allocated requirements. [e.g., Communication Service Provider, Airline Operations Center]	**Implementation:** Agreed strategy for risk mitigation from the potential functional and procedural possibilities. [Indicates stakeholder agreement to a particular set of ASOR detail elements.] **Means of Compliance:** Agreed means of compliance, or qualification of the required procedures, functionality, or other characteristics, the evidence of which is presented for operational approval. **Monitoring:** Agreed monitoring requirements supporting the Operations and Monitoring process. [Provides for operational validation of safety analysis assumtions and continued validity of the OSED.] **Human Factor considerations:** Identified vulnerabilities to human errors. Note is taken of need for fault tolerant approach and of potential for functional mitigation of human error. [A particular implementation may facilitate or render more difficult the mitigation of human error.] **Current system comparison:** Summary of relative risk due to proposed implementation with respect to this identified hazard and its likelihood of occurrence. [Necessary to prevent over specification of a system and their components.]



Hazard Class \ Safety Objectives	Probable	Remote	Extremely Remote	Extremely Improbable
1	▨	▨	▨	◩
2	▨	▨	■	□
3	▨	■	□	□
4	■	□	□	□
5	□	□	□	□

Risk Acceptance Cases

▨ Unacceptable ■ Minimum Safety Objective □ Acceptable

◩ Minimum Safety Objective - Unacceptable with Single Point Failures and Common-Cause Failures

Figure 1 Hazard Class Versus Safety Objective

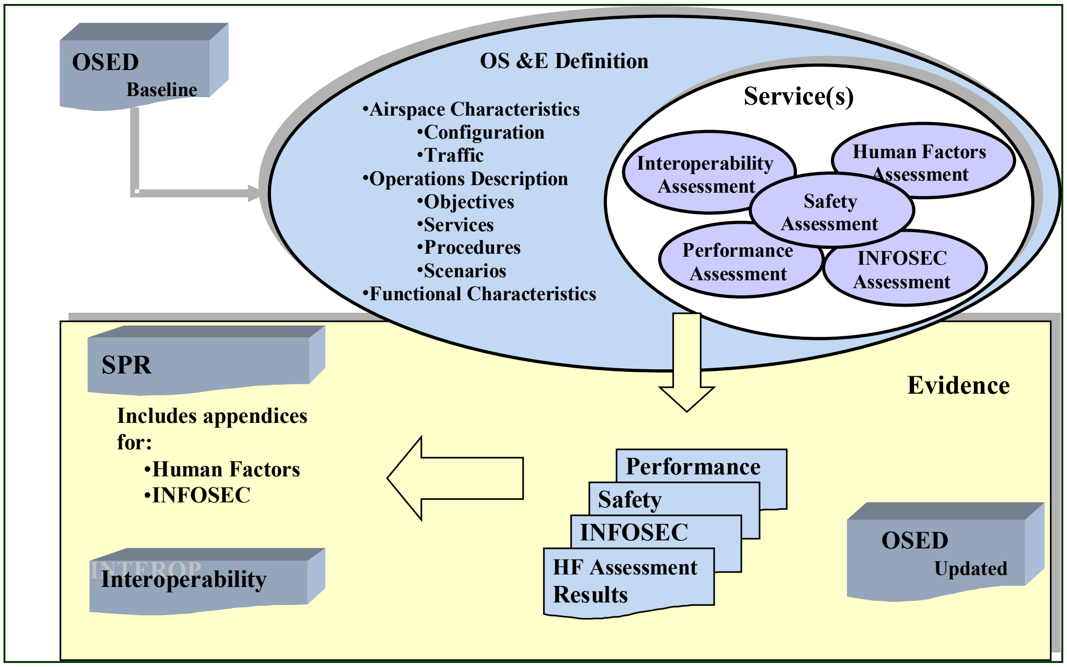


Figure 2 Coordinated Requirements Determination Including Safety and INFOSEC Considerations

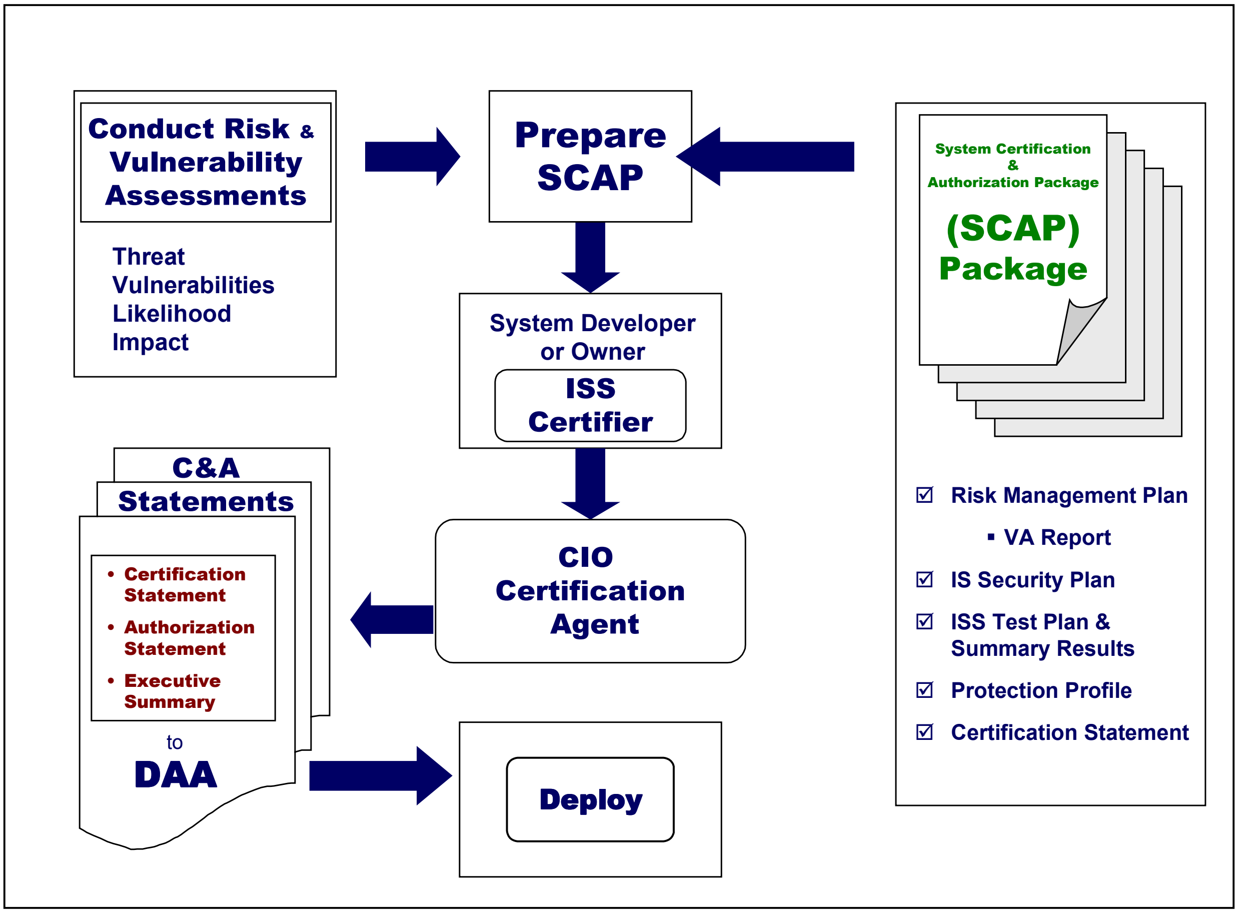

Conduct Risk & Vulnerability Assessments
Threat
Vulnerabilities
Likelihood
Impact
Prepare SCAP
System Developer or Owner
ISS Certifier
System Certification & Authorization Package
(SCAP) Package
☑ Risk Management Plan
▪ VA Report
☑ IS Security Plan
☑ ISS Test Plan & Summary Results
☑ Protection Profile
☑ Certification Statement
C&A Statements
• Certification Statement
• Authorization Statement
• Executive Summary
to
DAA
CIO Certification Agent
Deploy

Figure 3 Security Certification and Authorization Process

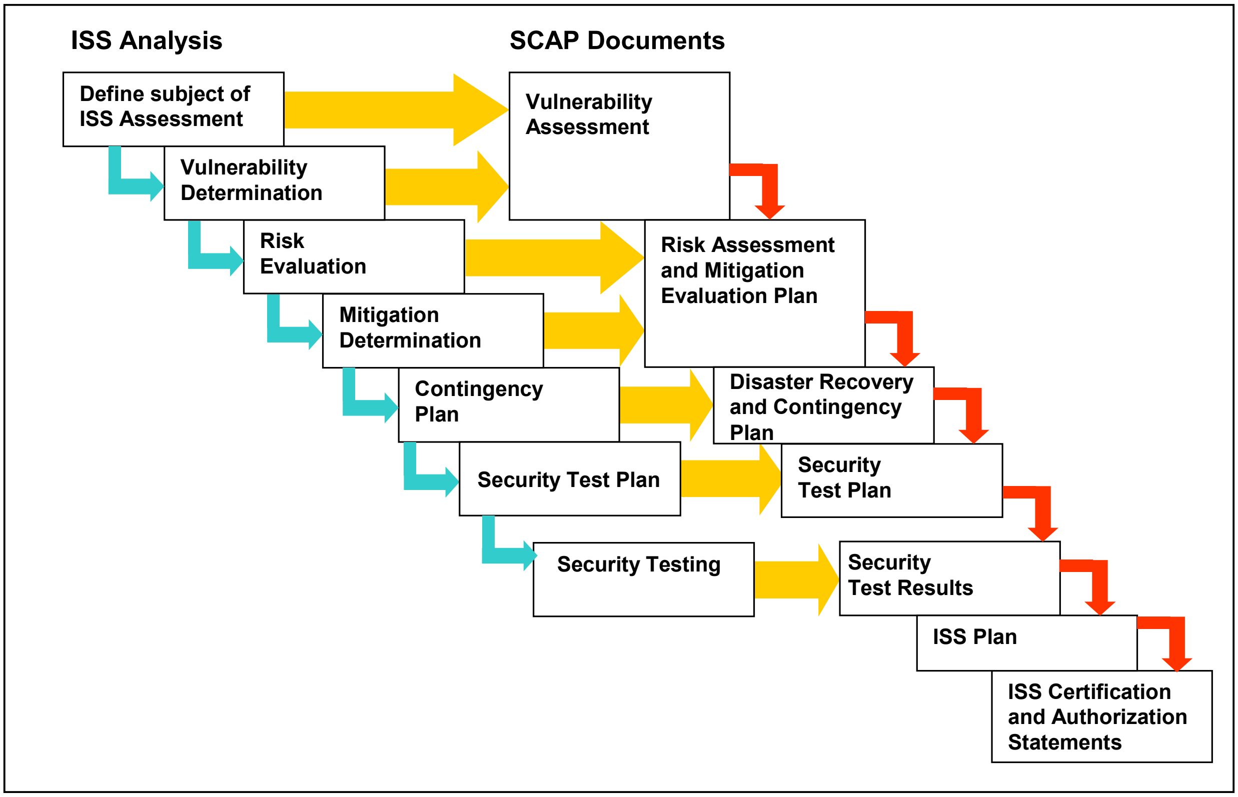

ISS Analysis
SCAP Documents
Define subject of ISS Assessment
Vulnerability Determination
Risk Evaluation
Mitigation Determination
Contingency Plan
Security Test Plan
Security Testing
Vulnerability Assessment
Risk Assessment and Mitigation Evaluation Plan
Disaster Recovery and Contingency Plan
Security Test Plan
Security Test Results
ISS Plan
ISS Certification and Authorization Statements

Figure 4 Information System Security (ISS) Analysis and SCAP Documentation

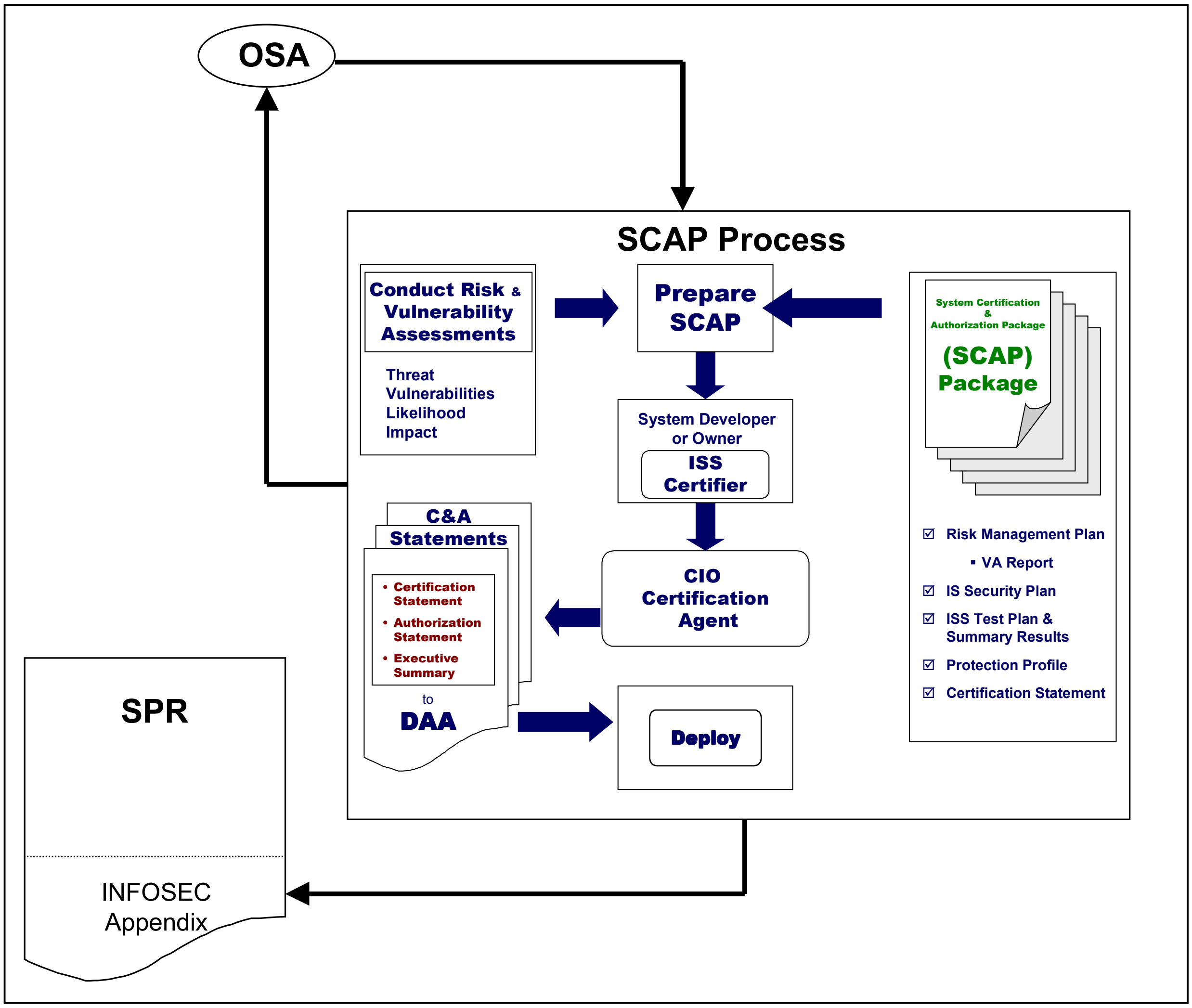


Figure 5 Coordinated Safety and INFOSEC Products