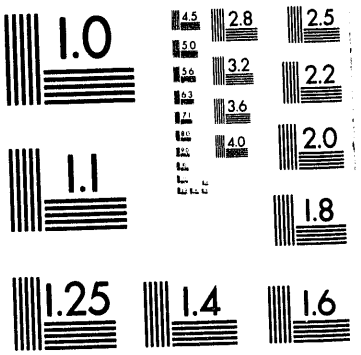
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
8.0
9.0

1 of 1

Conf-9405111--2

LA-UR-

94- 911

Title: A SYSTEMS ENGINEERING APPROACH TO AIS ACCREDITATION

Author(s): L. M. Harris and W. J. Hunteman

Submitted to: 16th Department of Energy Computer Security Group Training Conference, Denver, Colorado, May 2-5, 1994

Los Alamos
NATIONAL LABORATORY

Form No. 836 R5
ST 2629 10/91

A Systems Engineering Approach to AIS Accreditation*

L. M. Harris and W. J. Hunteman
Safeguards Systems Group
Los Alamos National Laboratory
Los Alamos, NM 87545

ABSTRACT

The systems engineering model provides the vehicle for communication between the developer and the customer by presenting system facts and demonstrating the system in an organized form. The same model provides implementors with views of the system's function and capability.

The authors contend that the process of obtaining accreditation for a classified Automated Information System (AIS) adheres to the typical systems engineering model. The accreditation process is modeled as a "roadmap" with the customer represented by the Designated Accrediting Authority. The "roadmap" model reduces the amount of accreditation knowledge required of an AIS developer and maximizes the effectiveness of participation in the accreditation process by making the understanding of accreditation a natural consequence of applying the model. This paper identifies ten "destinations" on the "road" to accreditation. The significance of each "destination" is explained, as are the potential consequences of its exclusion.

The "roadmap," which has been applied to a range of information systems[1,2] throughout the DOE community, establishes a paradigm for the certification and accreditation of classified AISs.

SYSTEMS ENGINEERING PROCESS

Systems engineering provides the ability to specify and model complex system behavior and architecture by integrating multiple viewpoints and capturing user needs. Models of the process are used to identify critical issues, system requirements and constraints, and the impact of externalities.[3]

Process Modeling

System engineers produce static functional models of a given process, frequently applying standard software engineering practices to construct a high-level, system-wide design. The models produced represent the process in a form that is suitable for human review and analysis and are also used to guide project managers in the performance of major tasks, represent relationships within the overall process, and can be used to measure both process improvement and product quality.[3] There are many approaches to process modeling; any of which can be used effectively provided the following sequence is met:

---

* Work supported by the US Department of Energy, Office of Safeguards and Security, Information Security Policy Branch.

- Identify system;
- Describe control processes and organizational groups that perform control functions (e.g. planning and tracking of resolutions);
- Describe process in terms of steps and sequences;
- Describe representations used to capture information at each step in the process;
- Describe staffing, assignments, and responsibilities; and
- Describe the review process and information under review (e.g., the documents to be reviewed at the end of each process step).

Process Modeling and AIS Accreditation

As compared to many systems, the accreditation process is a low-complexity, event-driven system in which the process steps are guided by both document development and the content of the required documents. Accreditation is essentially a management process, although its subsystems are highly technical.

Key Accreditation Concepts

The following key concepts and definitions are presented for those who may be unfamiliar with DOE computer security terminology. Each concept is fundamental to a sound understanding of the AIS accreditation process.

Certification

Certification is the comprehensive evaluation of the technical and nontechnical security features and the other security measures of an AIS. Certification occurs in support of accreditation and is used to establish the extent to which a particular classified AIS design and implementation meets the set of security requirements specified in its Security Plan. In addition, certification provides the documentation that a Classified AIS and its operational environment comply with the requirements of the DOE Classified AIS Security Program.[4]

Accreditation

Accreditation is a written, formal management decision that provides an organization with the approval and authorization to operate a classified AIS that processes, stores, transfers, or provides access to classified information. When making a decision to accredit a system, the Designated Accrediting Authority (DAA) considers the security protections of the AIS as documented in the system's security plan, the certification results, and any risk that may be involved in operating the classified AIS given its set of security protections and its operating environment. Accreditation remains in effect for three years, unless

- the classified AIS has been modified in a manner that impacts the security aspects of its environment, or
- the security requirements of the system have been changed.

To reiterate, accreditation is the approval for a classified AIS to operate in a particular security mode, with a prescribed set of technical and nontechnical security features, against the defined threats of a given operational environment at an acceptable level of risk.[4]

By accrediting the system, the DAA formally assumes responsibility for the system and must be prepared to accept the unavoidable residual risk of actually operating the system. The DAA must be prepared to answer whether or not the residual risk has been described adequately in the certification documentation and whether or not the risk is avoidable given implementation constraints.[5]

Protection Index

The protection index is a measure of perceived risk determined by combining the clearance level of system users, the classification level of the data processed on the AIS, and the operational environment.[4] The protection index is used to determine the appropriate system security requirements. Eight protection indices (or PIs) have been identified by the DOE; only five, however, are currently in use.

Table 1: Protection Indices

PI	Mode of Operation
0	Dedicated Mode
1	System High
2	Compartmented Mode
3	Multi-level - SRD, L/Q Users
4	Reserved
5	Multi-level, U/L/Q
6	Reserved
7	Reserved
8	Reserved

Security Plan

A Security Plan for a classified AIS describes the system, its interconnections, its security protections, and countermeasures.[4] It documents the classification levels of users and the categories of information the system will process as well as the

- system's operation,
- measures used to control access, and
- measures used to protect the AIS and its information.

The Security Plan must be reviewed and approved by the appropriate Computer Security Operations Manager (CSOM). Following CSOM approval, a copy is retained by both the Computer Security Site Manager (CSSM) and the Computer System Security Officer (CSSO). The approved security plan is used throughout the certification and accreditation process as the formal record of the AIS and its operational environment and as the basis for any inspections of the system that might occur.[4]

Security Performance Testing and the Test Plan

Security performance testing is an adjunct to the certification process. Its purpose is to assure that the AIS has been designed and is operating in accord with the security features specified in the Security Plan. The system's CSSO (with assistance from the CSSM) is responsible for writing the test plan and assuring the appropriate security tests are accomplished.

For AISs with a protection index of two or greater, an Independent Validation and Verification will be required to assure the AIS meets the security requirements of the DOE orders and "is as secure as reasonably can be attained given the circumstances and resources surrounding the AIS implementation." [5]

Key Players

Table 2 identifies the key individuals and their responsibilities.

Table 2: Responsibilities

Role	Responsibilities
CSSO	Develops Security Plan
	Writes Test Plan
CSSM	Approves Security Plan
	Approves Test Plan
	Certifies Results of Testing; Certifies System
CSOM/DAA	Approves Certification
For a PI (<=2), CSOM	Accredits System
For a PI (3), Field Office	Accredits System
For a PI (5), Field Office	Accredits System

COMPUTER SECURITY ROADMAP PROCESS

The authors have chosen a roadmap metaphor (see Fig. 1) to represent the AIS accreditation process. The roadmap identifies ten destinations and two possible side trips on the road to accreditation. The remainder of the paper discusses each destination in detail and presents possible implications from their exclusion.

It is important for system implementors to note that the process must be revised when any change to the AIS security environment occurs. Changes may occur in AIS hardware, software, administrative procedures, user clearances, installation of additional terminals, or in information access controls. The nature of the change(s) dictates the extent of the required activity. If the change is minor and does not impact the AIS security environment, little or no computer security activity will be necessary. However, a seemingly minor change, such as upgrading a software package, may have an unanticipated security impact. All assumptions modified by the upgrade must be analyzed to determine their impact on the security of the AIS.

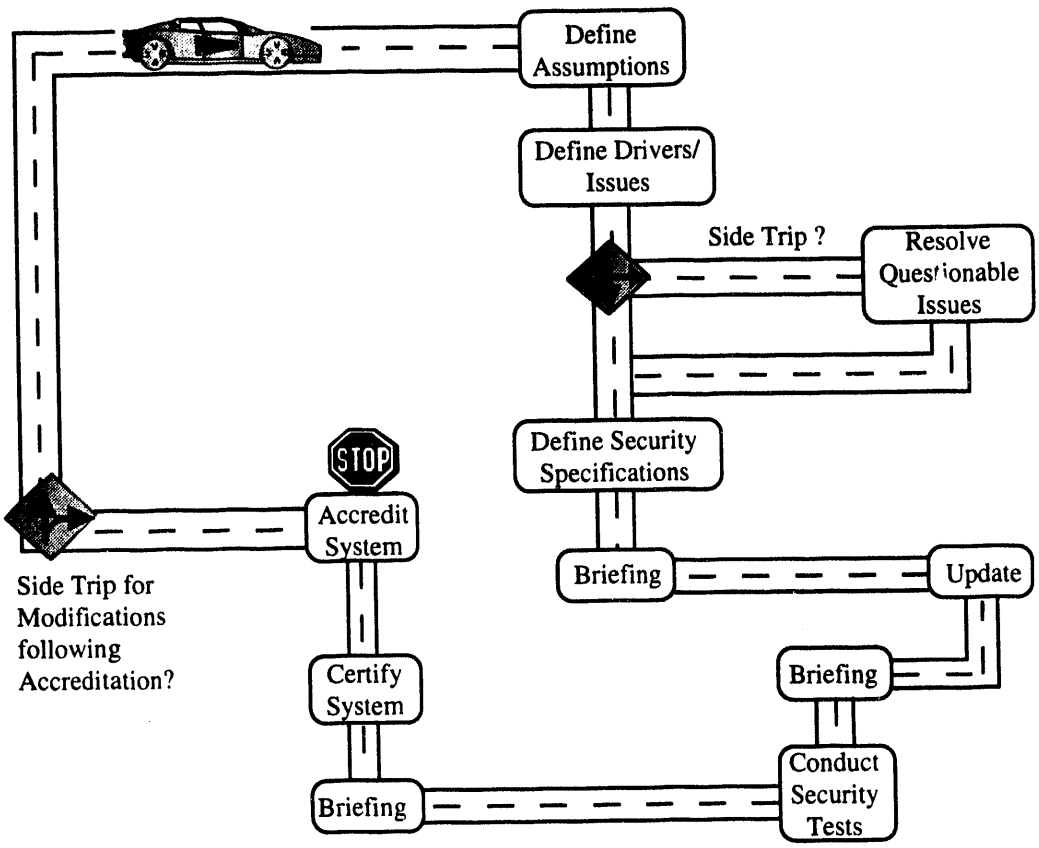

Fig. 1. The computer security roadmap.

Destination 1. Establish Assumptions

Developing new (or updating existing) assumptions establishes the security "architecture" for each specific version of the AIS. This "architecture" is the basis for determining the security requirements and includes definitions of the hardware and software architectures, determination of the information access controls, identification of the physical security controls for the AIS, if any, and definition of the administrative procedures and security requirements.

Hardware Architecture

The hardware architecture assumptions include all hardware components of the AIS system or the AIS network. These assumptions must address each unique hardware system as well as all communications components.

Software Architecture

Software architectural assumptions must include all software components used anywhere in the AIS system or network. Software descriptions should be organized according to each unique computer system and communication system used in the AIS. For example, the software used on each unique PC configuration must be identified as a group. Similarly, the

software used on each unique server configuration must also be identified, but as a separate group. Software grouping is necessary to clearly state the relationships between the different software components so security dependencies or interactions can be identified.

Information Access Controls

Any change to the requirements for granting access to information in the AIS has a significant impact on the AIS security environment. Two fundamental assumptions for information access control are that all AIS users have a clearance equal to or greater than the highest classification of data on the network and that formal access approvals will not be required to access any data.

The operating assumption is that all data access will be controlled on a need-to-know basis. The addition of any data requiring formal access approvals, or the addition of a user who does not have the proper clearance, requires a complete reassessment of the computer security requirements.

Physical Security

Any change to the physical security provided for all the AIS hardware, software, and data at any site may have a significant impact on the AIS security environment. Such a change typically occurs when a computer system is moved or when a new site is added to a wide-area network.

Administrative Procedures

Several administrative procedures, such as configuration control and password management, are essential to the security of AIS hardware, software, and data. If these procedures are modified, either because of changes in the AIS systems or data or because of administrative needs, the impact on the security of the AIS must be assessed before the change is implemented.

The administrative procedures in Table 3 must be specified and documented for the personal computers, servers, and network components in the AIS.

Security Requirements

Any change to the AIS security environment may result in a change to the security requirements that the AIS must meet. Current DOE orders on computer security arrange computer security requirements in an hierarchical manner. The components (protection indices or PIs) are arranged such that a PI of 0 is the lowest level of security and a PI of 5 the highest. As the PI level increases, new requirements are added to the list, which always includes all of the requirements from the lower PI levels. The specific requirements are identified in the DOE Order for Classified Computing for each PI.

A change in the AIS security environment may increase the PI required for the AIS and, thereby, substantially increase the security requirements. To minimize the impact on the AIS security environment, a careful security analysis of all proposed changes must be performed before committing to the changes. Although the changes may be necessary, their impact on security must be understood to allow adequate time for developing the appropriate changes in security functionality or in documentation, or both. Failure to analyze and prepare for changes in the security environment will delay the operational use of the AIS.

Table 3: Administrative Procedures	
Waste, Fraud, and Abuse	Personnel Security
Visual Access Controls	Configuration Management Program
Remote Maintenance and Diagnostic	Escort Procedures
Computer Security Incident Procedures	Authorization and Authentication
Virus/Intrusion Detection	Clearing and Sanitization Procedures
Back Up	Auditing Procedures
Continuity of Operations	Software Certification Procedures
Hardware Maintenance Removal	Security Incidents
On-Going Testing	Physical Access Control Procedures
Document Accountability Procedures	Protected Distribution System
Marking of Classified Output	Removable Media Handling and Marking
Printer Media	

Destination 2. Define Drivers and Issues

Drivers are the major events or requirements that dominate the resources or schedule of activities. Identification of these items will allow the appropriate assignment of resources and will ensure that the accreditation of the AIS version can be completed in a timely manner.

Resolve Driver Issues

Any issues arising from the analysis of proposed changes to the AIS security environment must be resolved before further work on the changes can be undertaken. These issues should be identified and resolved through coordination between the AIS security personnel, the AIS management, and the appropriate technical teams and personnel.

Most of the issues are expected to have minor impacts on the AIS security environment, but some issues could have a significant impact. For example, a decision to require formal access approvals for some of the AIS data would automatically increase the AIS PI from 1 (system-high mode) to 2 (compartmented mode). The security requirements for a PI of 2 would probably require a major restructuring of the AIS software architecture and a significant increase in the security functionality that the software must support.

Determine Established Milestones

A determination of required milestone dates or events is part of the process for determining required security activities. These milestones will determine the resources and dates for completing any security activities necessary to achieve accreditation.

Several computer security activities must be completed and some of the activities may overlap (such as briefing computer security personnel). In general, however, an activity must be completed before the next can begin. These activities, in their expected order, are

- Define/update security specifications,
- Brief the appropriate computer security personnel,
- Update the AIS Security and Test Plans,
- Brief the appropriate computer security personnel,
- Conduct computer security tests,
- Brief the appropriate computer security personnel,
- Certify the AIS, and
- Accredit the AIS.

Destination 3. Define/Update Security Specifications

This activity develops an updated set of security specifications from the data obtained during the development and analysis of the assumptions and security requirements. These specifications are intended to document the detailed requirements necessary to ensure the AIS conforms to DOE orders and regulations and to support reviews and discussion with the AIS personnel, such as the AIS developers.

Destination 4. Brief Computer Security Personnel on Security Specifications

Once the security specifications are developed and accepted by the AIS project developers, the appropriate computer security personnel must be briefed on the security features and environment for the AIS. Depending on the magnitude of the change, the briefings may range from informal telephone calls to formal presentations of the changes. Personnel who must always be briefed include

- the CSSM,
- the CSOM, and
- depending upon the PI level, the DOE/OSS Computer Security Program Manager (CSPM).

These individuals must concur with the proposed changes in the security specification before any further computer security activities may proceed. Current DOE orders do not explicitly require this concurrence; however, failure to obtain concurrence and support at this stage may create difficulties in later activities when the DOE officials ask for changes to the specifications before accrediting the AIS.

If the AIS crosses more than one CSOM boundary, other individuals who must be kept informed of the changes, but may not require full briefings, include

- CSOMs of the DOE Operations Offices (responsible for oversight of the facilities containing the AIS data and terminals) and
- CSSOs for the AIS at each site.

Destination 5. Update Automated Information System Security and Test Plans

The AIS Security Plan and the AIS Security Test Plan must be updated to incorporate changes in the security environment and specifications. Depending on the nature of the change, the update may range from letters informing the cognizant personnel of the change to a complete rewrite of the documents. A minor change, such as changes in the versions of already approved software, would require only written notification of the software changes. A change from system-high mode to either compartmented or multi-level mode would require a complete rewrite of the documents.

Destination 6. Brief Computer Security Personnel on AIS Security and Test Plans

Once the updated AIS Security and Test Plans are developed and accepted by the AIS project implementors, the appropriate computer security personnel must be briefed on the changes in the documents. Depending on the magnitude of the change, the briefings may range from informal telephone calls to formal presentations of the changes.

The personnel who must always be briefed include

- the CSSM,
- the CSOM, and
- depending upon the PI level, the DOE/OSS CSPM

These individuals must concur with the proposed changes in the documents before any further computer security activities may proceed. Current DOE orders do require this concurrence.

If the AIS crosses more than one CSOM boundary, other individuals who must be kept informed of the changes, but may not require full briefings, include

- CSOMs of the DOE Operations Offices (responsible for oversight of the facilities containing the AIS data and terminals) and
- CSSOs for the AIS at each of the sites.

Destination 7. Conduct Computer Security Tests

Depending on the magnitude of the change in the security environment and specifications, the testing activity may range from no testing to a complete testing of all security functionality by independent personnel. When testing is performed, it must always be conducted in accord with the Security Test Plan developed with the AIS Security Plan.

For example, if an upgrade is made to a different version of already approved software, then no testing is necessary. If the changes have a minor impact on the AIS security, then only the modified components must be tested. If the changes have a significant impact on the AIS security, the entire AIS must be tested.

Destination 8. Brief Computer Security Personnel on Security Test Results

Once the computer security tests are completed, the appropriate computer security personnel must be briefed on the results of the tests. Again, depending on the magnitude of the change in the security specifications, the briefings may range from informal telephone calls to formal presentations of the test results.

The personnel who must always be briefed include

- the CSSM,
- the CSOM, and
- depending upon the PI level, the DOE/OSS CSPM.

These individuals must concur with the test results before any further computer security activities may proceed. Current DOE orders do not require this concurrence; however, failure to obtain concurrence and support at this stage may create difficulties in later activities when the DOE officials ask for changes to the specifications before accrediting the AIS.

If the AIS crosses more than one CSOM boundary, other individuals who must be kept informed of the changes, but may not require full briefings, include

- CSOMs of the DOE Operations Offices (responsible for oversight of the facilities containing the AIS data and terminals) and
- CSSOs for the AIS.

Destination 9. Certify the AIS

Once the computer security tests are completed, the AIS must be certified by the local CSSM. The certification decision is based on the content of the AIS Security Plan, the AIS Security Test Plan, and the results of the computer security tests.

Destination 10. Accredit the AIS

After the new AIS version has been certified, the system must be accredited before operation with classified information may begin. The accreditation is based on the content of the certification package, which includes the certification statement and the security documentation. The security documentation package contains the AIS Security Plan, the AIS Security Test Plan, and the security test results.

Accreditation is performed by the AIS DAA. The individual who acts as the DAA is determined by the PI of the system (see Table 2). The DAA will typically ask for concurrence by the CSOMs who have responsibility for sites where the AIS terminals or data are located.

SUMMARY

The roadmap model provides a vehicle for communication between the system implementors and the certifying and accrediting officials, which is accomplished by presenting the system security features and architectures in a somewhat standardized, organized form. The model also provides system implementors with a detailed picture of the security function and capability of their system, while maximizing the effectiveness of participation in the accreditation process by making the understanding of accreditation a natural consequence of applying the model.

REFERENCES

1. W. J. Hunteman and L. M. Harris, "Proliferation Information Network System Computer Security Roadmap," Los Alamos National Laboratory, Safeguards Systems Group Draft Report (February 28, 1994).
2. L. M. Harris, "LANMAS Security Requirements Document," Los Alamos National Laboratory, Safeguards Systems Group Draft Report (February 1, 1994).
3. "Manual of Security Requirements for the Classified Automated Information System Security Program," Department of Energy Draft Document DOE M 5639.6A-1 (January 14, 1994).
4. S. White (Chair), "Systems Engineering of Computer-Based Systems," State of Practice Working Group of the IEEE Computer Society Task Force of ECBS, IEEE Computer, November 1993, pp. 54-65.
5. "Criteria for Verifying the Security and Assurance for Compartmented Mode, Secure MultiLevel Mode and MultiLevel Mode Operation in Department of Energy Automated Information Systems," Prepared for the Department of Energy, Office of Safeguards and Security, Information Security Policy Branch by the Safeguards Systems Group, Los Alamos National Laboratory, September 30, 1993.

ADDITIONAL SOURCES

J. Brule and A. Blount, *Knowledge Acquisition* (McGraw-Hill Book Company, New York, 1989).

R. de Nuefville, and J. Stafford, *System Analysis for Engineers and Managers* (McGraw-Hill Book Company, New York, 1971).

M. Peterson, D. Lundberg, and A. Elk, *Knowledge Engineering—System Design in Diffuse Domains* (Telelogic, Sweden, 1990).

S. Shinners, *Guide to Systems Engineering and Management* (D. C. Heath and Company, Lexington, Massachusetts, 1976).

B. Werbell, and R. Gibson, *Structured Analysis and Design of Information Systems* (McGraw-Hill Book Company, New York, 1984.)

I. Wilson and M. Wilson, *From Idea to Working Model* (John Wiley & Sons, Inc., New York, 1970).

DATE
FILMED
5/2/94
END