INFORMATION SECURITY
IN
INTEGRATED AVIONIC SYSTEMS

William E. Gibbons
Naval Air Development Center
Warminster, Pa. 18974

ABSTRACT

Integrated avionic systems are being developed for application in the majority of future military aircraft. In these applications, the current technique of integrating and maintaining Information Security (INFOSEC) by using discrete electronic systems and wiring is no longer adequate. This paper defines the areas of concern and provides direction for determining the requirements to maintain INFOSEC within the integrated avionic system.

INTRODUCTION

The purpose of INFOSEC within an avionic system is to protect sensitive information as required by the operational military user and sponsor of the system. This user classifies the information at the appropriate level and requires that it be properly protected.

INFOSEC is not a new subject. It has been around as long as information, under many different names. Everyone has experienced the desire to protect some information important to themselves. Each of us determines the sensitivity of personal information, to whom it should be given and how it should be protected. Safe deposit boxes, locked file cabinets, doors and Personal Identification Numbers are INFOSEC techniques used for this purpose.

INFOSEC in avionic systems is also not new. Many sensitive data systems have been developed over the years. They have been discrete avionic subsystems employing two INFOSEC techniques where required. First, encryption is provided for all sensitive data to be transmitted through media where access cannot be controlled, such as radio broadcasts. Second, TEMPEST design is provided to prevent cross-coupling or radiation of the sensitive data to unauthorized avionics which may result in its compromise.

What is New? Integrated avionic systems such as those currently in development are new. The INFOSEC techniques previously used are insufficient to protect sensitive information in the new integrated avionics where common hardware, firmware and/or software are used for the processing of both sensitive and non-sensitive data. The following INFOSEC design areas must be addressed to provide INFOSEC in integrated avionic systems:

1. Operational/System Security Policy
2. Trusted Computing Base
3. Communication Security
4. TEMPEST
5. Internal Data Distribution

OPERATIONAL/SYSTEM SECURITY POLICY

The operational/system security policies in which an avionic system is to be developed, used and supported can both enhance the overall system INFOSEC posture and increase the INFOSEC risk of compromise. To effectively determine the INFOSEC design requirements for the avionic system the following security policies must be analyzed and understood for the development facility and system, aircraft operational environment and avionic maintenance and upgrade facility and system:

1. The classification and access restrictions of the various data to be processed by the system.
2. The clearance and authorization levels which each system operator will be granted.
3. The data access requirements of each of the system operators.
4. The system controls and access required by each of the operators.
5. The system restrictions required for each of the operators.
6. The physical security that will be supplied to the system during air and ground operations.

7. The physical security that will be supplied to the system during non-operating periods.

8. The physical security that will be provided to the system during maintenance operations on the (a) facility, (b) aircraft, (c) avionic system and (d) associated systems.

9. The clearance and authorization level which maintenance personnel will be granted at the operational, intermediate and depot maintenance levels.

10. The data access requirements for each of the maintenance levels.

11. The system control and access requirements for maintenance.

12. The system restrictions required and provided at each of the maintenance levels.

13. The security provisions of the external electronic and paper data distribution supporting the system.

14. The security provisions on the development and system support facilities.

**TRUSTED COMPUTING BASE**

The Trusted Computing Base (TCB) is the principle INFOSEC technique implemented in the integrated avionic system to provide the required security of the rapidly increasing amount of classified data processing aboard the aircraft. The security policies derived above are essential for determining the TCB requirements of the integrated avionic system. They provide the source data to be used in the computer security assessment to establish the required level of trust and trusted computer system evaluation criteria which must be fulfilled by the hardware, firmware and software of the computer system. Separate security assessments must be performed for the development, avionic and support computer systems.

The required level of trust to which the development, avionic and support computing systems must be evaluated and accredited is determined from computer security requirements tables, such as those in CSC-STD-003-85, "Computer Security Requirements", using the combination of the risk index, security environment and security operating mode as identified below:

1. The risk index is the disparity between the minimum user clearance or authorization (Qmin) and the maximum sensitivity classification and categories (Rmax) of the data processed by the computer system.

2. The security environment of the computing system can be either an Open or Closed environment. A Closed security environment meets both of the following conditions:
   a. Application developers (including maintainers) have sufficient clearances and authorizations to provide acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of the data to be processed is Confidential or less, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of the data to be processed is Secret or above, developers have at least a Secret clearance.
   b. Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications.

3. The security mode of operation can be either the System High or Multilevel security modes. In the System High security mode, the entire system, including all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored.

The evaluation criteria for accreditation of the required level of trust (A1 through D1) are listed in DOD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria". These criteria list the security policy, accountability, assurance and documentation that will be expected of the computing system. These criteria must be analyzed together with the operational/system security policies to determine the specific requirements which must be designed into the computing system for it to be accredited. The computing system need not provide additional protection for evaluation criteria areas which...
the operational/system security policy has already adequately covered.

COMMUNICATIONS SECURITY

Communications Security (COMSEC) techniques and equipment are the only approved method for sensitive (RED) data to be treated as non-sensitive (BLACK) information. COMSEC must be included in the integrated avionic system for secure voice, secure data, transmission security, navigation security and secure identification purposes. In addition, secure cryptographic key management techniques must be incorporated to support the COMSEC applications.

The use of COMSEC techniques in avionic systems is now being expanded to protect various datalinks. COMSEC can also be used to support the Trusted Computing Base of the integrated avionic system.

At present, discrete "black-box" cryptographic equipment is included in the avionic system to provide COMSEC. Embedded COMSEC modules are now being developed to be included within the integrated avionic system. These modules require the avionic system to provide many of the internal signals, controls, power and firmware/software programs which were provided in the discrete "black-box". The avionic system designer must now understand the security procedures, design principles and interfaces involved. Design approval by the cognizant government agencies is required before sensitive information can be processed.

TEMPEST

The national policy for the control of compromising emanations requires that TEMPEST techniques be used to prevent cross-coupling or radiation of sensitive information to avionics which may result in an unacceptable level of risk of its compromise. This is relatively simple in present avionic systems because the discrete equipments and wiring can be isolated from each other where required. In integrated avionic systems this physical isolation is not possible because common hardware, firmware and software are used for the processing of both sensitive (RED) information and non-sensitive (BLACK) information. The national policy definitions of the RED and BLACK are presented in numerous TEMPEST directives, such as NASCAIM 5100A.

In the past, most of the avionics subsystems aboard the aircraft processed only BLACK information, so TEMPEST protection was provided at the equipment and wiring processing RED information. This permitted the TEMPEST analysis of the aircraft to be conducted from the viewpoint of an all BLACK aircraft with a few subsystems requiring TEMPEST protection of the RED information.

The rapidly increasing amount of RED data processing aboard aircraft coupled with the integration of former separate RED and BLACK avionic subsystems has resulted in a very cumbersome TEMPEST design when the all BLACK aircraft design viewpoint is used. Therefore, it is becoming more common to view the integrated avionics aircraft as an all RED aircraft. This allows TEMPEST design requirements to be imposed principally on the portions of the avionic system which MUST be BLACK, such as the transmitters, antennas and ground access points which must be permitted to transmit only BLACK data from the aircraft.

INTERNAL DATA DISTRIBUTION

The internal data distribution systems of the integrated avionics system present some interesting INFOSEC requirements for the design engineer. They bring together data which MUST be RED and data which MUST be BLACK. Audio and digital data distribution systems are used and both present similar design requirements.

The audio distribution system simultaneously processes the RED voice intercommunications between the crew, the RED audio communications with the secure voice systems and the BLACK audio communications with the non-secure radios. Trusted controls and TEMPEST isolation must be designed into this system.

Numerous digital data distribution systems exist within the avionic system. These systems can have the following INFOSEC architectures:

1. All BLACK - no RED data or RED data processors are connected to the system.

2. All RED - All data processors connected are authorized access to the highest data classification and compartments distributed by the system.

3. RED/BLACK Gateway - Separate all RED and all BLACK systems with a Trusted and TEMPEST protected gateway to allow necessary data to securely pass between them. This architecture can also be used when different levels of RED data must be protected.
4. RED/BLACK Composite - On a time-share basis, the system distributes both RED and BLACK data between the appropriate RED and BLACK processors. This architecture requires Trusted control and TEMPEST protection as both a RED and BLACK system. TEMPEST protection from the RED data must be provided at all BLACK access ports when the system is distributing RED data. Further TEMPEST protection must be provided at all RED data processor access ports when BLACK data is being distributed between BLACK data processors. This architecture can also be used when different levels of RED data must be protected.

Where possible data which MUST be BLACK should not be processed in the same distribution system as data which is RED. This greatly reduces the INFOSEC design requirements. For design convenience, BLACK data which is not transmitted from the aircraft can be considered RED.

CONCLUSION

INFOSEC in integrated avionic systems requires a coherent set of operational/system security policies and trusted computing base designs supported by COMSEC and TEMPEST techniques. This coherence prevents costly overkill and inadequate designs. Fulltime INFOSEC engineering from each INFOSEC technology must be included in the avionic system design from the beginning. INFOSEC cannot be added later to integrated avionic systems as is all too often required in present discrete "black-box" avionic systems.