Adapting the ISO 27000-Series Security Framework to Space Missions

Craig T. Biggerstaff[1]
Lockheed Martin, Houston, Texas

and

Howard Weiss[2]
SPARTA, Inc. (A Parsons Company), Columbia, Maryland

Space systems and operations support systems bear a striking similarity to industrial control systems, environments in which security countermeasures designed for generic information technology computing are often unavailable or poorly suited to operational needs. This mismatch does not relieve agencies and organizations from the policies and laws (e.g., FISMA) requiring them to implement security controls from frameworks designed for generic IT computing systems. This paper discusses the recent development of a security guide for space mission planners aimed at helping them develop the management, operational, and technical security controls appropriate to the value of their system and the information processed in it. It is intended to tailor the generic security framework and controls of the ISO 27000 standards to the specific needs of spacecraft and space mission support facilities.

I. Introduction

THE proliferation of computer system security breaches and known exploits, along with the vast increase in ordinary computing power available to wage such attacks, have led to a heightened awareness of the risks present in all types of systems. Several highly-publicized security attacks (e.g. the so-called 'Stuxnet' Trojan-horse attack) against supposedly well-protected industrial control systems have made it obvious that even the 'air gap' (i.e., no direct connections at all) is no longer a sufficient defense against the possible threats. When discussing the risk of attack, however, there is a widespread perception that such sophisticated attacks are unlikely to be experienced by any real organizations, and are largely plot matter for spy movies. Since the majority of attacks go completely unpublicized, it is difficult to combat this perception; there is therefore a burden on information security engineers to educate and advise system designers and operational line organizations about the threats they face, and how to plan for an achievable means of protecting their assets.

Space systems and operations support systems bear a striking similarity to industrial control systems, environments in which security countermeasures designed for generic information technology computing are often unavailable or poorly suited to operational needs. This mismatch does not relieve agencies and organizations from complying with policies and laws (e.g., the Federal Information Security Management Act, or FISMA) requiring them to implement security controls from frameworks designed for generic information technology (IT) computing systems.

This paper discusses the recent development by the Security Working Group of the Consultative Committee for Space Data Systems (CCSDS) of an informational guide for space mission planners aimed at helping them develop the management, operational, and technical security controls appropriate to the value of their system and the information processed in it. It is intended to tailor the generic security framework and controls of the ISO 27000 standards to the specific needs of spacecraft and space mission support facilities.

This is a novel effort for two reasons. First, only in recent years has the body of knowledge known to information security practitioners been codified into a well-known systematic and widely-accepted framework such

[1] Senior System Engineering Staff, Facilities Development Operations Contract,
2101 NASA Parkway, Mail Code DD12, Houston, TX 77058
[2] Technical Director, Sparta Defense Sector, 7110 Samuel Morse Drive, Columbia, MD 21046

as the ISO 27000 series. Second, the prior lack of accepted (and/or bureaucratically imposed) frameworks led many space missions in the past to address problematic security requirements through broad waivers and ad hoc assertions of inapplicability. This effort updates and extends prior work done within NASA to develop security requirements for the Constellation program and associated projects.

As the relevant branch of the International Standards Organization (ISO), the CCSDS develops voluntary standards for space systems in the areas of communications protocols and computing system applications. The CCSDS carries out its work as ISO Technical Committee 20 (Aircraft and Space Vehicles), Subcommittee 13 (Space Data and Information Transfer Systems).

II. Information Security Management Systems

The information security field has evolved over the last decade-and-a-half from an approach focused primarily on compliance with the letter of regulations and statutes into a risk-based approach that seeks to enumerate the security objectives of a system, which can then be used to evaluate the likely risks and apply countermeasures against them in proportion to their perceived level of risk. This overall methodology is referred to as an information security management system (ISMS). The stated security objectives of a system are called *controls*.

A. Security Controls and Frameworks

Controls are analogous to system-level requirements, but not directly equivalent; controls specify an organizational objective (what behavior should occur). The actual decomposition of a control objective into mechanisms or methods by which the objective is reached may be allocated among various components of the system. They may also be satisfied by the shared use of common infrastructure and/or services, including the use of third-party service agreements. Certain controls can also compensate for other control objectives that are not met by themselves; for example, implementation of logical (data) access controls in a system may compensate for an absence of physical access controls, or vice versa.

When control objectives are collected into a hierarchical grouping of related security concerns, this is known as a controls framework. The purpose of a security controls framework is to guide the system owner in setting policy and aid in decomposing policy into more specific procedural and technical design requirements for implementation. It makes it possible to assess whether and how the system meets its security objectives. Most frameworks will recommend either more or less stringent controls based upon the organization's pre-determined assessment of the criticality and sensitivity (with respect to confidentiality, availability, and integrity) of the data types processed within the system. For example, if a system has low availability requirements, controls pertaining to availability may be reduced. Likewise, if a system has high integrity requirements for a specific type of data, the components of the system where that data resides will have increased integrity controls.

B. The ISO/IEC 27000 Series

The ISO 27000 series of documents cover all aspects of managing information security for an enterprise, from basic security concerns through best practices to audit and risk assessment methods. An overview discussion of information security management systems may be found in ISO/IEC 27000[2].

The best known of this series of standards, ISO/IEC 27001[3], identifies a security controls framework encompassing management, operational, and technical capabilities. The framework addresses the most common aspects of protecting the confidentiality, integrity, and availability of information and information systems. There are dozens of individual controls available in the ISO framework, which are organized according to the high-level categories listed in Table 1.

The companion ISO/IEC documents numbered 27002 through 27005[4,5,6,7] provide accompanying implementation guidance. Collectively, these documents comprise the '27000 Series' which has been adopted as an international standard for the practice of information security management.

III. The Problems of Mismatch between Space Systems and Generic IT Systems

Although the ISO 27000 series is useful to most systems as an organizing principle for information security management, its generic nature causes problems of scope and applicability that can severely limit usefulness if its requirements are applied as-is to specialized environments.

With respect to space systems, numerous problems arise from the absence of consideration given during the development of the ISO framework to the specific environmental constraints and performance requirements of spacecraft. For example, the computers and communications systems in most spacecraft are optimized around an

unyielding power consumption budget: a spacecraft is unlikely to have the power, CPU, or communications bandwidth to carry out many typical terrestrial computer security functions to the satisfaction of corporate IT departments. In addition, the typical operating paradigm of spacecraft is inverted from that of a general-purpose computing system; the task of coordinating and arbitrating between multiple activities and commands given to the spacecraft avionics is typically carried out by a mission operations center prior to command uplink, and not left to software in the spacecraft itself.

A. The Rise of the General-Purpose OS and Network Stack: Everything is a Computer

The operating paradigm of spacecraft today remains largely as described in the previous paragraph. However, it is increasingly true that even specialized operating systems expressly designed to support the high reliability and real-time performance requirements of avionics systems are sometimes augmented with variants of the general-purpose application programming interfaces (APIs) and network stacks used in general-purpose operating systems (in particular, the system calls and networking APIs common to the Unix and Linux operating systems). Internet Protocol (IP)-based networking is now an automatic and expected capability of ground systems, development systems, and test beds, and its ubiquity in terrestrial computing systems makes it an attractive option for mission designers seeking to leverage a rich feature set of existing capabilities for inclusion even onboard the spacecraft itself for various applications.

With that rich feature set comes a rich attack surface of vulnerabilities for a potential adversary to exploit. This paper is not concerned with the use of IP networking in space systems except to note that, as a spacecraft's capabilities are extended to include networking and it appears visible on a network seemingly like any other computer, it becomes increasingly untenable for organizations to waive or ignore the range of typical network security concerns – network traffic monitoring, access control, patch management, log management, and so forth – that are applied to other nodes on the network. If it acts to other nodes on the network like a typical computer, how can it be treated as immune from the operational security concerns of the rest?

B. When Everything is a Computer, IT Policy Applies to Everything

The management of IT has also lagged behind developments in computing technology in that IT management policies and regulations are still largely aimed at typical computing systems and applications even as the marketplace has blurred the distinction between what is and what is not a computer. There are now many formerly special-purpose appliances (e.g., voice telephone keysets) whose dedicated interface hides hiding a largely ordinary computer that is performing the function. All of these, like the spacecraft described earlier which appears as a network node, have brought broadly-scoped IT regulatory compliance burdens into unexpected situations.

NASA's Constellation program experienced this tension when developing security requirements for space vehicles and for associated systems supporting Constellation development and operation. NASA IT systems, like those of other United States Government agencies, are statutorily bound to follow the Federal Information Security Management Act (FISMA), which (through Commerce Department regulation) has resulted in NASA's attempting to apply the National Institute of Standards and Technology (NIST) SP800-53[9] security controls framework (a US-developed cousin[3] of ISO 27001) to all projects and missions. NASA spacecraft have *not* been exempted from these regulations.

Yet many of the information security requirements that are straightforward to implement in ground systems are difficult or impossible to implement in space systems due to the specific performance constraints of the space environment. A better treatment of network security concerns is needed, that accounts for these differences in environments, constraints, and capabilities.

IV. Adaptation to Space Flight Constraints

Fortunately, there is precedent for altering controls to suit a constrained environment. The security of industrial control systems[4] (ICS) is one area in which existing controls frameworks have already been tailored and alternative guidance given to work around the limited capabilities of ICS equipment (e.g., programmable-logic controllers). The latest revision of NIST Special Publication 800-53 includes an appendix specifically developed for ICS

[3] NIST SP800-53 contains a cross-reference appendix mapping its own controls to those of ISO 27001.

[4] From SP800-53[9]: "An ICS is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC)."

controls. The paradigm of treating space mission operations as an industrial control system appears attractive at first glance, but there are enough significant differences to rule out a wholesale adoption of this framework.

There is also precedent for extending and/or adapting the ISO 27000 series controls to a unique environment. ISO 27011[8] is one example of how an industry has extended and/or adapted the ISO 27000 series controls to its particular needs and environment. In this case, the telecommunications industry has clarified the scope of certain existing ISO 27001 controls and added other new, industry-specific controls to account for the specific characteristics of telecommunications service delivery and infrastructure.

A. The Security Guide for Mission Planners

The Security Working Group of the Consultative Committee for Space Data Systems (CCSDS) was tasked with creating an informational reference that space mission designers could utilize in the early stages of operations concept and mission architecture development, planning, and budgeting. The intent of this work was to assist the mission designer in understanding which security concerns are likely to affect the technical and operational requirements throughout the life of the mission. It is a perennial (and elusive) goal of security engineers that security be built into a system from the outset, instead of being seriously considered by an organization only after all major design decisions have been taken and the available funding allocated for other purposes.

Most members of the Security Working Group are familiar with the regulatory frameworks common to generic IT systems such as ISO 27000, the NIST 800 series of publications, as well as related frameworks commonly used in other IT-intensive industries such as the Payment Card Industry. None of these are appropriate to a space environment without modification.

The Mission Planners' Guide approaches the overall context of a space mission by treating each of its supporting assets as belonging to one of three main types of operating environment: space systems, ground operations systems, and development/test/checkout systems. All ISO 27001 security control objectives are accounted for and allocated to at least one of the three environments. New control objectives developed for the Mission Planners' Guide identify both security concerns unique to spacecraft and mission operations, and also security concerns for which these systems need to compensate for an inability to satisfy certain other ISO 27001 objectives due to the constraints intrinsic to space missions. These new control objectives are organized and numbered according to the existing ISO 27001 hierarchy as shown in Table 1, and each is numbered with a unique '.MPx' suffix (e.g., 'A.9.2.MP4').

Table 1. ISO 27001 Categories. *The hierarchy and numbering scheme used in ISO 27001 for security controls has been preserved in the Mission Planners' Guide for additional controls specific to space systems.*

Section number	Subject area
A.5	Security policy
A.6	Organization of information security
A.7	Asset management
A.8	Human resources security
A.9	Physical and environmental security
A.10	Communications and operations management
A.11	Access control
A.12	Information systems acquisition, development, and maintenance
A.13	Information security incident management
A.14	Business continuity management
A.15	Compliance

B. Special Concerns for Ground Operations Systems

Ground support systems share the most capabilities with generic IT systems, and so it is to be expected that ground support systems will be expected to provide ordinary IT controls for most functions. The Guide does allocate most existing ISO 27001 control objectives to these systems.

The Mission Planners' Guide also adds several objectives which, if not met, would impair the integrity and/or availability of a spacecraft, but which must be implemented in ground systems due to their nature.

For example, a small inaccuracy in a spacecraft internal time source can cause an increasing drift away from the corresponding value of ground-based time clocks. If operations personnel are unaware of the error, they may direct the spacecraft to execute particular commands at a particular time, only to have the operation occur at an incorrect time. This problem is not easily remedied within the spacecraft, but ground operations can (and should) monitor the deviation and account for it in ongoing operations planning.

Another example of a compensating control allocated to ground operations systems is the objective of projecting conjunctions between the spacecraft and other orbiting space objects in order to predict (and avoid) potential collisions.

C. Special Concerns for Development, Integration, and Pre-Flight Checkout Systems

Systems used for development, integration, and verification of flight software and hardware also share many capabilities with generic IT systems. The Guide also allocates most existing ISO 27001 control objectives to these systems.

These systems are addressed separately from ground operations systems partly because certain controls are addressed at systems having telecommand capability, and party because of the time-shift of when a realized risk will affect the spacecraft: ground operations security failures are more likely to impair a mission in real-time, while security failures in development may impair a mission long after the actual failure occurs, if it is even detected.

The security control objectives listed in the Guide as unique to development and test systems are directed toward the integrity risks to a spacecraft during the periods when hardware and software are most vulnerable to tampering. Spacecraft and spacecraft components should be protected by physical security controls against unauthorized modification during all periods of pre-flight handling and storage.

D. Special Concerns for Space Vehicles

The new security control objectives added in the Mission Planners' Guide as applicable to space systems are directed at the vulnerability of the space environment and the limited capabilities of space flight hardware and software.

Generic IT security controls deemed not applicable to space systems include those common to multi-user computing systems: login and account access controls, privilege separation, segregation of duties, logging and audit processing controls, and so forth. Physical access and facility security controls are not generally applicable to assets already in space!

Some controls – those pertaining to networking and user authorization – are deemed potentially applicable for certain complex spacecraft in the future. Here the experience of operating the International Space Station may serve as a case study. ISS crew functions are not typically attributable to a single individual except by other means (e.g. voice communications and video downlinks) which are not integrated into an audit log processing system. Yet the ISS continues to diversify its operations. It is conceivable that future spacecraft may be able to host untrained, paying passengers among the crew; if that is ever the case, the ability to monitor and audit individual user actions may become more important. If networked communications between spacecraft and ground continues to progress, it may become equally important to have the ability to isolate critical operations network functions from passengers' personal network access, similar to the capabilities installed on some airlines today.

The majority of space system controls, however, relate to already-understood functions of operating spacecraft: validation of uplinked telecommands, 'safe mode' operation during critical or failure recovery periods, and/or altering/limiting the command functions that may be carried out while security mechanisms are degraded or disabled. The Guide also adds security controls to the ISO 27001 complement to address the space mission planner's need to plan against the eventuality of deorbit; most IT systems do not need to plan for assets landing on an unexpected location on the earth.

Table 2. Mission Planners' Guide Controls. *There are 71 controls in the Guide, of which 24 are new (i.e. not found in ISO 27001). Each is listed by applicability to management, operational, or technical concerns.*

Control		Control Type	Control		Control Type
A.5.1.MP1		Management	A.11.1.MP1		Management
A.5.1.MP2	(new)	Management, Operations	A.11.2.MP1		Operations
A.5.1.MP3	(new)	Management, Operations, Technical	A.11.3.MP1		Operations
A.5.1.MP4	(new)	Management	A.11.4.MP1		Technical
A.5.1.MP5	(new)	Management, Technical	A.11.4.MP2	(new)	Technical
A.6.1.MP1		Management	A.11.5.MP1		Technical
A.6.1.MP2		Management	A.11.6.MP1		Technical
A.6.2.MP1		Management	A.11.6.MP2	(new)	Technical
A.7.1.MP1		Operations	A.11.7.MP1		Management, Operations, Technical
A.7.2.MP1		Operations	A.12.1.MP1		Technical
A.8.1.MP1		Management, Operations	A.12.2.MP1		Technical
A.8.2.MP1		Management	A.12.2.MP2	(new)	Technical
A.8.3.MP1		Management	A.12.2.MP3	(new)	Technical
A.9.1.MP1		Operations	A.12.2.MP4	(new)	Technical
A.9.2.MP1		Operations, Technical	A.12.3.MP1		Management, Operations, Technical
A.9.2.MP2		Operations	A.12.3.MP2	(new)	Technical
A.9.2.MP3		Operations	A.12.3.MP3	(new)	Technical
A.9.2.MP4	(new)	Operations, Technical	A.12.3.MP4	(new)	Technical
A.10.1.MP1		Operations	A.12.3.MP5	(new)	Technical
A.10.1.MP2		Operations	A.12.4.MP1		Operations, Technical
A.10.1.MP3		Operations	A.12.5.MP1		Operations
A.10.2.MP1		Management, Operations	A.12.5.MP2		Operations
A.10.3.MP1		Operations	A.12.5.MP3	(new)	Operations, Technical
A.10.3.MP2		Operations	A.12.6.MP1		Technical
A.10.4.MP1		Technical	A.13.1.MP1		Operations
A.10.5.MP1		Operations, Technical	A.13.2.MP1		Operations
A.10.6.MP1		Technical	A.13.2.MP2	(new)	Operations
A.10.7.MP1		Operations	A.14.1.MP1		Management, Operations
A.10.8.MP1		Operations	A.14.1.MP2	(new)	Technical
A.10.8.MP2	(new)	Operations, Technical	A.14.1.MP3	(new)	Technical
A.10.9.MP1		Management	A.14.1.MP4	(new)	Technical
A.10.10.MP1		Technical	A.15.1.MP1		Management, Operations
A.10.10.MP2		Technical	A.15.1.MP2	(new)	Management
A.10.10.MP3	(new)	Technical	A.15.2.MP1		Management, Technical
A.10.10.MP4	(new)	Technical	A.15.3.MP1		Operations, Technical
A.10.10.MP5	(new)	Technical			

E. Breakdown of New Security Controls by Type

There are 71 controls overall in the Mission Planners' Guide. Only 24 of them are completely new to this document; the remainder are statements of applicability tailoring existing ISO 27001 controls.

These controls may be grouped according to their intended audience. Management objectives relate to an organization's policies and practices, and should be resolved well in advance of a mission. Operational objectives involve the daily processes of operations staff. Technical objectives should be used as input to the requirements used to build a system. Table 2 provides a listing of controls in the Mission Planners' Guide and the intended audience of each.

V. Conclusion

When the Mission Planners' Guide was being developed, it was envisioned that the practical value of this effort would be for CCSDS member agencies and other space industry organizations to apply it during mission concept and architecture development, to avoid every successive mission's rehashing the same work and decision-making regarding the proper scope and feasible application of regulatory requirements. It remains to be seen how successful the Mission Planners' Guide will be in achieving this, but initial informal feedback has been positive.

The Guide has been published by the CCSDS as an informational reference and not as a recommended standard. If the space systems community comes to view this work positively and finds organizational benefit in it, it may be possible in the future to codify the work of the Mission Planners' Guide into more concrete recommendations that can be applied to space systems security management as an established discipline not needing of reinvention with every mission.

Appendix A
Acronym List

API	Application Programming Interface
CCSDS	Consultative Committee for Space Data Systems
ICS	Industrial Control System
IP	Internet Protocol
ISO	International Standards Organization
ISS	International Space Station
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology

Acknowledgments

The authors wish to thank the participating members of the CCSDS Security Working Group, who contributed considerable insight and the experience of several agencies which shaped the content of the eventual Mission Planners' Guide.

References

[1]*Security Guide for Mission Planners*, CCSDS 350.7-G-1, CCSDS, Washington DC, 2011.

[2]ISO/IEC 27000:2009, *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, ISO/IEC, Geneva, 2009.

[3]ISO/IEC 27001:2005, *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, ISO/IEC, Geneva, 2005.

[4]ISO/IEC 27002:2005, *Information Technology—Security Techniques—Information Security Management Systems—Code of Practice for Information Security Management*, ISO/IEC, Geneva, 2005.

[5]ISO/IEC 27003:2010, *Information Technology—Security Techniques—Information Security Management System Implementation Guidance*, ISO/IEC, Geneva, 2010.

[6]ISO/IEC 27004:2009, *Information Technology—Security Techniques—Information Security Management—Measurement*, ISO/IEC, Geneva, 2009.

[7]ISO/IEC 27005:2008, *Information Technology—Security Techniques—Information Security Risk Management*, ISO/IEC, Geneva, 2008.

[8]ISO/IEC 27011:2008, *Information technology—Security Techniques—Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002*, ISO/IEC, Geneva, 2008.

[9]*Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, 2009.