A Cyber Secure Architecture and Design for a Spacecraft/Ground Station System

Joseph Beaubien, Doreen Joseph, George Shaffer, Patrick Donahue, Seth Glover
Customer: Dr. Michael Papay, **Subject Matter Expert:** Chris Mellroth

INTRODUCTION

- Spacecraft and ground station systems are increasingly under threat
- Such systems are typically not built with security in mind
- Security must be implemented into the design of systems from inception
- Designing, reviewing, and analyzing the systems to prevent cyber attacks is important to ensure the safety of equipment

Purpose

To create a secure model of a spacecraft and ground station system, containing the ground station, the spacecraft, and their communications (Fig. 1), using Systems Modeling Language (SysML) in Cameo Systems Modeler, a modeling software.

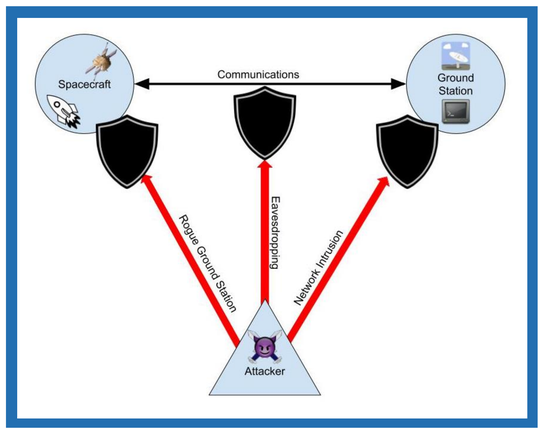

Fig. 1. Concept of operations. The red arrows represent the methods by which an adversary can compromise the spacecraft, ground station, and their communications, while the black shields represent the protections put in place to stop the adversary.

APPROACH

Phase One: Creating Requirements

- Derived from the National Institute of Standards and Technology's (NIST) Cyber Security Framework. (See Fig. 2)
- Apply to the specific concerns of a spacecraft and ground station
- Categorized based on
  - Function
  - Type
- Approximately eighty requirements were created in the decomposition process

#	Name	Text	Owner	Derived From
1	4 Ground Station Requirements		System Element Requirements	
2	4.1 Ground Station Inventory	The ground station shall be inventoried as a system of communication/network devices and computers.	4 Ground Station Requirements	NIST-CSF-ID1.1
3	4.2 Ground Station Baseline	A baseline for ground station network activity will be established and categorized by user/system.	4 Ground Station Requirements	NIST-CSF-DE1.1
4	4.3 Suspicious Events	Abnormal events shall be cataloged by the ground station and analyzed.	4 Ground Station Requirements	NIST-CSF-DE1.1
5	4.4 Physical Connection Alerts	Critical devices shall be configured to alert the system if a USB or other physical connections are attached.	4 Ground Station Requirements	NIST-CSF-DE1.2
6	4.5 Access Control Systems	Critical devices shall be secured with logged access control systems alongside visual monitoring.	4 Ground Station Requirements	NIST-CSF-DE1.2
7	4.6 Physical Ground Station Protection	Physical access to the ground station shall be protected with the use of physical barriers, multi-factor authentication, and monitoring devices.	4 Ground Station Requirements	NIST-CSF-PR1.1
8	4.7 Role-based Access Control	Role-based access control shall be utilized on systems and assets of the ground station.	4 Ground Station Requirements	NIST-CSF-PR1.6
9	5 Software Requirements		System Element Requirements	
10	5.1 Software Management	Software in use on the ground stations and spacecraft shall be identified and cataloged.	5 Software Requirements	NIST-CSF-ID1.1
11	5.2 Anti-Virus	An anti-virus/anti-malware program shall be deployed on the ground station and control centers.	5 Software Requirements	NIST-CSF-DE1.1
12	6 Network Requirements		System Element Requirements	
13	6.1 Communication Map	All communication to and from the spacecraft and ground station shall be mapped.	6 Network Requirements	NIST-CSF-ID1.1
14	6.2 Communication Baseline	A baseline for spacecraft communications shall be established to compare against mission objective.	6 Network Requirements	NIST-CSF-DE1.1
15	6.3 Authentication and Authorization	Only authenticated and authorized users shall interface with spacecraft.	6 Network Requirements	NIST-CSF-ID1.3
16	6.4 Air gapped System	Any machines/networks that either directly or indirectly interact with the spacecraft will be air gapped.	6 Network Requirements	NIST-CSF-ID1.3
17	6.5 IDS and IPS	Intrusion detection and prevention systems shall be implemented in the ground station (especially on the connection to the spacecraft).	6 Network Requirements	NIST-CSF-DE1.2

Fig. 2. Requirements Table. This table displays our functional requirements, their owner and what NIST requirement they were derived from.

Phase Two: Applying the Requirements

- Applying the derived requirements alongside established spacecraft/ground station architecture to design models
  - SysML Block Definition Diagram
  - SysML Internal Block Diagram
  - Whitebox Interface Control Document (ICD) Table
  - Requirements Diagram
  - Use Case Diagram

DESIGN

The architecture is for a generic spacecraft and ground station system. The design takes into account the functionality of the spacecraft and ground station in relation to elements of cyber security. User functionality was identified in the use case diagram shown in Fig. 3. In addition, the security measures and practices that would need to be modified to improve the security and resiliency of the system are identified.

- Implement an IDS and IPS on both the ground station and spacecraft
- Encrypt communications between the spacecraft and ground station
- Air gap the control room of the ground station
- Network Segmentation
- Defense in Depth
- Authorization and Authentication on both the spacecraft and ground station

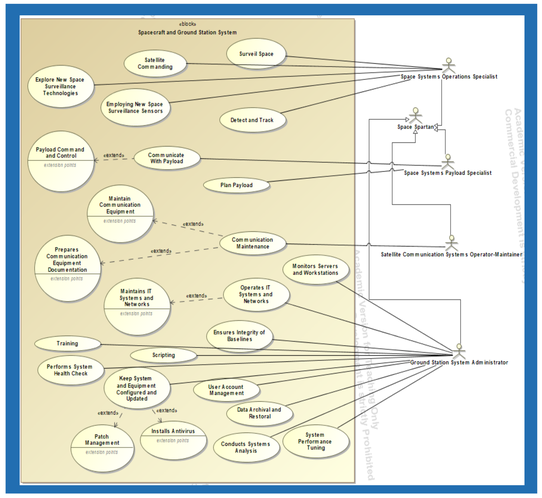

Fig. 3. SysML Use Case Diagram. The user roles (stick figures) are on the right with the use cases (circles) of the system on the left.

RESULTS AND CONCLUSION

- By comparing the functionality of the system with our derived functional requirements we were able to develop a sample architecture (Fig. 4) that is cyber secure while remaining generic
- Security polices should be implemented alongside our architecture for maximum effectiveness
- Security from conception is required to ensure that the spacecraft and ground station system are fully secure

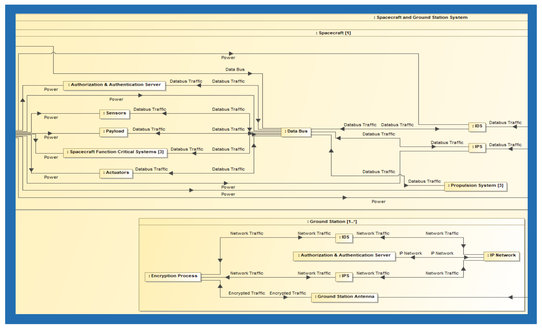

Fig. 4. SysML Internal Block Diagram. The boxes in the diagram represent components of the architecture, while the arrows indicate the connectivity between them.

ACKNOWLEDGEMENTS

- **Customer:** Northrop Grumman
  - Dr. Michael Papay, Vice President and Chief Information Security Officer
- **SME:** Chris Mellroth, Cyber Systems Engineer
- **Mentor:** Prof. Gino Manzo
  - Prof. Rock Sabetto

REFERENCES

[1] M. Fischer and A. Scholtz, "Design of a Multi-mission Satellite Ground Station for Education and Research", *Second International Conference on Advances in Satellite and Space Communications*, 2010. Available: 10.1109/SPACOMM.2010.13 [Accessed 27 March 2019].
[2] G. Phillip, "Satellite Ground Station Architecture", El Paso, TX, 2006.
[3] *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology, 2018, pp. 23-44.