System	Subsystem	Potential Subcomponents/systems
Space Vehicle	Propulsion	Thrustors
		Control Electronics
		Fuel Storage
		Control Valves
		Pressure Sensors
		Propulsion Heaters
	ADCS / ACS	Attitude Sensors
		Actuators
		Software
	EPS	Electronics
		Power Generation (i.e., solar panels)
		Power Storage (i.e., batteries)
		Power distribution
	ODC / GN&C	Sensors
		Software
	C&DH / OBC	Electronics
		Commanding Software
	TT&C / COMM	Radios
		Antennas
		Routers
		Crypto
		Switches
		Intrusion Detection
	SMS	Structures
		Brackets
		Fasteners
		Actuators (on-board movement)
	TCS	Electrical Heaters
		Cryocoolers
		Thermoelectric Coolers (TEC)
		Fluid Loops
		Active Thermal Architecture (ATA)
	Payload - Imagery	<Spacecraft Specific/Mission Dependent>
	Payload - RF	<Spacecraft Specific/Mission Dependent>
	Payload - OCT	<Spacecraft Specific/Mission Dependent>
	Payload - Data Proc	<Spacecraft Specific/Mission Dependent>
	Payload - Hosted	<Spacecraft Specific/Mission Dependent>

Other Spreadsheet Content Links

Content of Log Records	Description of minimum content to be logged
SPARTA Mapping	Deconstruction of SPARTA for this BPG

Acronyms	
ACS	Attitude Control System
ADCS	Attitude Determination & Control Subsystem
API	Application Programming Interface
BOL	Beginning of Life
BPG	Best Practice Guide
C&DH	Command & Data Handling
CAN	Controller Area Network
CMD	Command
COMM	Communications (RF)
CPU	Central Processing Unit
DoS	Denial of Service
EDAC	Error Detection and Correction
EMI/EMC	Electromagnetic Interference/Compatibility
EOL	End of Life
EPS	Electrical Power Subsystem
FMS	Fault Management System
FPA	Focal Plane Array
GN&C/GNC	Guidance, Navigation, & Control
GPS	Global Positioning System
MECH	Mechanical
NIST	National Institute of Standards and Technology
OBC	On-Board Computer
OCT	Optical Communications Terminal
ODC	Orbit Determination & Control
OS	Operating System
OSAM	On-orbit Servicing, Assembly, & Manufacturing
Prop	Propulsion
RF	Radio Frequency
RTS	Relative Time Sequence
SDN	Software-Defined Networking
SDR	Software Defined Radio
SMS	Structures & Mechanisms Subsystem
SPARTA	Space Attack Research and Tactic Analysis
SNR	Signal-to-Noise Ratio
SSC	Stephenson Stellar Corporation
SSCR	Stellar Space & Cyber Range
SV	Space Vehicle
TCS	Thermal Control System
TEC	Thermoelectric Coolers
TT&C	Telemetry, Tracking, & Communications
WDT	Watchdog Timer

Table Column Titles	Table Column Descriptions
Subsystem	Primary Sub-System of the Space Vehicle (SV)
Subcomponent	Sub-component of the SV Subsystem
SPARTA ID Ref	Reference ID from Aerospace Corp. SPARTA framework
non-SPARTA Ref	Other Reference other than SPARTA
Possible Attack Vectors/Indicators of Compromise	Attack vector that may be utilized by adversary or malicious insider
Logging Best Practice	Description of what should be logged to alert to possible cyber activity
Minimum Logged Data	Data that should be captured to assist with validating cyber event occurrence
Impact/Prioritization	What is the impact to the mission should this attack be realized
(Low/Medium/High)	Loosely based on the typical Fault/Warning/Info messaging scheme from the FMS
FMS Redundancy	If a separate Intrusion Detection System will receive these logs and potentially take
(Likely/Possible/Unlikely)	action, will it interfere with the FMS
Response Significance	Significance to the spacecraft should the attack be realized, possible reasons for the
(User or FMS)	attack, and any role the FMS may play should the attack occur

Abstract - SV Logging Best Practices Guide

Effective logging within the subsystems of a Space Vehicle (SV) will enable operators to quickly diagnose and troubleshoot issues and enhance the space system's overall security posture. At the time of this research, there have been no guidelines instituted to provide insight into what should be logged within the individual subsystems of a SV that would highlight indicators of malicious cyber activity.

This spreadsheet is intended to be a guideline as to what should be evaluated and logged within each spacecraft subsystem. This guideline of best practices was derived from analysis of the Aerospace Corporation's SPARTA framework and through specialized research performed by Stephenson Stellar Corporation (SSC) and their Stellar Space & Cyber Range (SSCR).

Each SV will have a unique design and differing capabilities/payloads, so this guideline is intended to be a starting point of logging best practices that can be applied to enhance the SV security posture. This is not a requirements document. However, these guidelines can be applied where applicable and used to assist space organizations with defining their overall computer network defense strategy and cyber protections of operational spacecraft.

Questions/comments: SV-Logging-BPG@stephensonstellar.org

Minimum Content of Log Record (*Reference NIST SP 800-53r5 AU-3 & AU-3 (1)*)

ID	Log Content	Description	Sample Log Field/Content
1	Type of Event	Audit records must contain information that establishes **what type** of event occurred	Event title and description
2	Time	Audit records must contain information that establishes **when** the event occurred	Time stamp
3	Location/Device	Audit records must contain information that establishes **where** the event occurred	Source and destination addresses | Filenames involved
4	Source	Audit records must contain information that establishes the **source** of the event	User identifiers | Process identifiers
5	Effect	Audit records must contain information that establishes the **outcome** of the event	Success or fail indications | Event-specific results
6	Identity	Audit records must contain information that establishes the **identity** of any individuals, subjects, or objects/entities associated with the event	User identifiers | Process identifiers
7	Rule ID	Audit records, *when possible and apply* , must contain information that identify an access control or flow control **rule**(s) triggered by the event	Rule identifiers. *Only applies to access control or rule-based logs*

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
Propulsion		EX-0012.07		Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes could result in mission loss or severe degradation.
Propulsion				Access to propulsion subsystem is acquired from another sub-system (ex: ADCS) to initiate actions	Log and alert all access to the propulsion subsystem. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
Propulsion				Access from propulsion subsystem to another sub-system (ex: ADCS) is initiated	Log all access from the propulsion system. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Propulsion system generally has little communication with subsystems other than flight computer.
Propulsion				Communication to propulsion from another subsystem	Log all messages directly addressed to the propulsion system (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
Propulsion				Critical propulsion subcomponents (heaters, flow valves, pressure sensors, gimbals, etc.) signal anomalies	Log and alert to any signal disruption to heaters, valves, gimbals, or sensors within the subsystem	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot/change to a fault mode. Could indicate a simple component failure or intrusion.
Propulsion				Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	High	Possible	Unauthorized temperature set limits could result in mission loss. Critical compromise.
Propulsion				Change in control logic	Log and alert any changes to gains/etc., or to relative time sequence scripts	Key-value pairs of control parameters, script changes (or hashes), and time tags	High	Possible	Burn sequence scripts/control logic constants rarely change. Could be an indicator of compromise.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/ Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
ADCS		EX-0012.08		Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible).	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
ADCS				Access to ADCS subsystem is acquired from another sub-system (ex: Payload) to initiate actions	Log and alert all access to the ADCS system. Confirm access is authenticated and authorized (if possible).	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
ADCS				Access from ADCS subsystem to another sub-system (ex: Payload) is initiated	Log all access from the ADCS system. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
ADCS		IA-0011		Unusual access from one ADCS subcomponent to another ADCS subcomponent is acquired (ex: Star Tracker to Reaction Wheels) to initiate actions	Log and alert abnormal intra-ADCS access between subcomponents. Confirm access is authenticated and authorized (if possible)	Source subcomponent, target subcomponent, request/command, and time tag	High	Unlikely	Unauthorized subcomponent communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance, lateral movement, and/or supply chain concern.
ADCS				Communication to ADCS from another subsystem	Log all messages directly addressed to the ADCS system (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
ADCS		IA-0011		Abnormal communication among ADCS subcomponents (ex: Star Tracker to Reaction Wheels)	Log all unusual messages among ADCS subcomponents	Capture source subcomponent, target subcomponent, message content, with time tags	High	Unlikely	Unauthorized ADCS subcomponent communication could indicate compromise. Abnormal intra-ADCS communication could indicate DoS, reconnaissance, lateral movement, and/or supply chain concern.
ADCS	Sun sensors, Earth horizon sensors, star trackers, magnetometers, inertial measurement unit			Critical ADCS sensors signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot/change to a fault mode. Could indicate a simple component failure or intrusion.
ADCS	Torque rods, reaction wheels, control moment gyros, thrusters, gimbals			Critical ADCS actuators signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot/change to a fault mode. Could indicate a simple component failure or intrusion.
ADCS	Processing electronics, star trackers, inertial measurement unit, magnetometers, reaction wheels, control moment gyros, thrusters			Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	Medium	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
ADCS				Change in determination logic/algorithms	Log and alert any changes to gains/etc. or to algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Attitude control logic/constants rarely change after Launch and Early Operations. Could be an indicator of compromise.
ADCS				Change in control logic/algorithms	Log and alert any changes to gains/etc. or to algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Attitude control logic/constants rarely change after Launch and Early Operations. Could be an indicator of compromise.
ADCS	Star Tracker			Change to star maps/catalogs within Star Trackers	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory blocks along with time tag. Include hashes/checksum (if possible)	High	Possible	Unauthorized star map changes could indicate compromise. Depending on the changes, could result in mission loss or severe degradation.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/ Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/ Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
EPS		EX-0012.09		Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
EPS				Access to EPS subsystem is acquired from another sub-system (ex: Payload) to initiate actions	Log and alert all access to the EPS subsystem. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
EPS				Access from EPS subsystem to another sub-system (ex: Payload) is initiated	Log all access from the EPS subsystem. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
EPS				Communication to EPS from another subsystem	Log all messages directly addressed to the EPS system (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
EPS				Critical EPS subcomponent signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot/change to a fault mode. Could indicate a simple component failure or intrusion.
EPS	Battery, Solar Arrays (if applicable)			Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	High	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent. Changing solar array setpoints could disrupt power harvesting efficiency and thus mission availability. Changing battery setpoints could drastically reduce mission life.
EPS	Power Conditioning/ Distribution, Battery Charge/ Discharge Control, Solar Array Control			Change in control logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Power control logic/constants rarely change after Launch and Early Operations. Could be an indicator of compromise. Battery charge and discharge limits should be carefully monitored. Changing these limits could drastically reduce the mission life.
EPS				Load shedding	Log and alert all load shedding events with time tags	Affected subsystems/components and command trigger with time tags; perhaps the spacecraft state/mode	Medium	Likely	Load shedding is common during eclipse and certain seasonal events, so is expected during normal operations. However, the FMS can also trigger load sheds in the event of a serious anomaly. Knowing the context of the event will help determine if the action was appropriate or a sign of compromise.
EPS				Power reset	Log any power reset commands/events with time tags	Affected subsystems/components and command trigger with time tags; perhaps the spacecraft state/mode	Low	Likely	Power resets a relatively uncommon events during normal operations. The C&DH may use this function to resolve known issues, or the FMS could use it as part of a fault response strategy. Repeated reset commands could be an indicator of DoS, or irregular commands could be used to execute malware.
EPS				Power-on commands	Log any explicit power-on commands with time tags	Affected subsystems/components and command trigger with time tags; perhaps the spacecraft state/mode	Medium	Possible	Power-on commands are generally rare outside of normal power conditioning/distribution control or ground contacts. Commanding power-hungry subsystems/components on when the spacecraft is only operating on battery power (such as eclipse) indicates compromise. Could result in a lengthy spacecraft outage.
EPS		EX-0012.08, SV-MA-8		Change in power consumption characteristics	Log the power consumption and baseline over time for BOL (beginning of life) and EOL (end of life)	Affected subsystems/components and command trigger with time tags; upper and lower limits for power usage	Medium	Possible	Threat actors may target power subsystem due to their criticality by modifying power consumption characteristics of a device. This may cause the finite power resources to be used on rogue processes that deplete power for the satellite's mission. FMS could be used as part of a fault response strategy.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
ODC & GN&C				Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
ODC & GN&C				Access to ODC/GN&C subsystem is acquired from another sub-system (ex: Payload) to initiate actions	Log and alert all access to the ODC/GN&C system. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
ODC & GN&C				Access from ODC/GN&C subsystem to another sub-system (ex: Payload) is initiated	Log all access from the ODC/GN&C system. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
ODC & GN&C				Communication to ODC/GN&C from another subsystem	Log all messages directly addressed to the ODC/GN&C system (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
ODC & GN&C	GPS Receiver			Critical ODC/GN&C component signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, message frequency, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot/change to a fault mode. Could indicate a simple component failure or intrusion.
ODC & GN&C	Processing electronics, GPS Receiver			Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	Low	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
ODC & GN&C				Change in determination logic/algorithms	Log and alert any changes to gains/etc. or to algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Attitude control logic/constants rarely change after Launch and Early Operations. Could be an indicator of compromise.
ODC & GN&C				Change in control logic/algorithms	Log and alert any changes to gains/etc. or to algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Attitude control logic/constants rarely change after Launch and Early Operations. Could be an indicator of compromise.
ODC & GN&C				Change to burn plan	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory blocks along with time tag. Include hashes/checksum (if possible)	High	Possible	Unauthorized changes to the propulsion burn plan indicates compromise. Depending on the changes, could result in mission loss or severe degradation.
ODC & GN&C				Change to ephemerides	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory blocks along with time tag. Include hashes/checksum (if possible)	High	Possible	Unauthorized changes to the GN&C ephemerides indicates compromise. Depending on the changes, could result in mission loss or severe degradation.
ODC & GN&C	GPS Receiver	EX-0014.01, EX-0014.04, EX-0016, EX-0016.03		GPS message jamming/spoofing	Log and alert any signal power levels above a nominal range. Log and alert any timing discrepancies outside of a tolerance	Signal anomaly power level, characteristics (center frequency/bandwidth/etc.), time interval discrepancy, and time tag (possibly of last known good value)	High	Unlikely	GPS jamming/spoofing attacks will likely show abnormal signal power/other attributes or changes in time deltas from one GPS message to the next. While this vector is adjacent to cyber concerns, it is advised to include this telemetry within the IDS. GPS jamming/spoofing attacks could temporarily affect mission availability or severely impact mission life.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
C&DH		EX-0012.01, EX-0012.10		Modification of hardware configuration key-value pairs (defaults/globals). Hardware may include: memory, CPUs, databus, etc.	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
C&DH		PER-0001, EX-0012.01, EX-0012.02, EX-0012.03, EX-0012.04, EX-0010.01, EX-0010.02		Memory pokes/loads or related commands (ex: validate, activate, etc.) - this includes: tables, files, images, or specific register values	Log any memory poke/load command received. Validate with mission operations (if possible)	Memory addresses, file size, user/device/application who sent the command (if possible) along with time tag	High	Unlikely	Uploading unauthorized information to the spacecraft is a strong indicator of breach. This vector could cause a wide range of issues, including hijacking or loss of mission.
C&DH				Memory peeks/dumps that reveal any C&DH configuration or operational information	Log any memory peek/dump command received. Validate with mission operations (if possible)	Memory addresses, requested information, user/device/application who made the request (if possible) along with time tag	High	Unlikely	Downlinking any information about how the ground connects to the spacecraft could be an indicator of breach. This information would be necessary to establish contact through a rogue ground station.
C&DH		EX-0012.11		Suspension or changes to watchdog services, including: poke/pet tasks, timeout settings, reset frequency	Log and alert for any changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications (ex: Health and Safety) along with time tags. Also, log any messages that request changes to watchdog services along with time tags	Medium	Possible	Watchdog timers are important mechanisms for space operations. They provide a backstop to runaway software processes. Software must continue to monitor and "pet" the watchdog to ensure the mission is not interrupted. Changes to settings of any watchdog services will be extremely rare throughout the life of the spacecraft. If watchdog services are attacked, the mission could experience an extended outage.
C&DH		EX-0009, EX-0009.01, EX-0009.02, PER-0002		Exploiting code flaws or backdoors	Log and alert	Log any off-nominal behavior (ex: special mode changes, unusual commands, changes in the types and frequencies of telemetry, power/memory/CPU utilization, etc.). May require conditional logic to trigger.	High	Possible	Software developers often write logic or create hidden modes with special commands for ease of development, but not intended for operations. Sometimes this code is not removed before uploading to the spacecraft. Additionally, software may have bugs or emergent behaviors that were not discovered during testing. These poor development practices result in poor cyber hygiene and offer attackers unique vectors which often cause extreme harm. Monitoring for strange behaviors is critical for discovering this compromise.
C&DH		EX-0004, EX-0005, EX-0010.03, EX-0010.04		Changes to or corruption of default (golden) software images, default (golden) firmware images, payload software/firmware images, and boot mechanisms (if possible)	Log and alert if mismatch occurs. Validate with mission operations (if possible)	Include actual and expected check sum/hash values along with memory addresses (if applicable)	High	Likely	FMS will likely troubleshoot/change to a fault mode (ex: Safe Mode) if software/firmware images or boot mechanisms are corrupted. Could indicate a simple component failure or introduction of malicious code. FMS may not intervene if spacecraft successfully boots/resets, even if malicious code is present.
C&DH		EX-0003, DE-0004, DE-0006		Changes to user/application authentication and authorization policies, including: roles, white lists, blacklists, etc.	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	High	Possible	Authentication and authorization policies dictate which users, devices, and applications have access to which resources, including critical spacecraft commands. Changing these policies could allow users/devices/applications access to innapropriate resources. This is a high value target for lateral movement across spacecraft subsystems.
C&DH		EX-0012.04		Changes to trust zone boundary definitions and policies, including: publish/subscribe messaging services, segmented software/data communication bus networks, event services, time services, table services, etc.	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	High	Possible	Trust zones define collections of spacecraft resources that users/devices/application may be granted access. Changing these definitions and policies could allow users/devices/applications access to innapropriate resources. This is a high value target for lateral movement across spacecraft subsystems.
C&DH		DE-0004		Changes to user, device, or application certificates/ digital signatures	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	High	Possible	Unauthorized changes to certificates/digital signatures could result in denial of service or be an indicator of enumeration and lateral movement.
C&DH				Suspension or changes to encrypted storage services	Log and alert for any changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to encrypted storage services along with time tags	Medium	Possible	If the spacecraft uses encrypted storage for critical operational data or logs, any changes to this service could be an indicator of breach. Changes to the settings of any encrypted storage services will be extremely rare throughout the life of the spacecraft.
C&DH		DE-0001, IA-0010, IMP-0001		Suspension or changes to fault management services, including: limit checking, command scripts, audit logs, event messages, mode definitions (ex: Safe Mode)	Log and alert for any changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications (ex: Limits Checker) along with time tags. Also, log any messages that request changes to fault management services along with time tags	High	Possible	Fault management services are critical to continued operations in the harsh space environment. They take corrective action to safe the spacecraft when ground operators cannot. Changes to these services will be rare throughout the life of the spacecraft. Because fault management mechanisms are granted special access to critical commands, any manipulation could result in severe consequences.
C&DH				CPU utilization is abnormally high	Log and alert	Utilization rate (above a threshold), running tasks/processes ranked by % utilization (if possible) along with time tag	Medium	Possible	Abnormal CPU utilization could be an indicator of attack in progress. The OS or FMS make take corrective active to kill any runaway processes.
C&DH		EX-0001, EX-0001.01		Mismatch in command counter between ground and spacecraft	Log any command counter increment, including: received/accepted, rejected, executed, failed. Alert if ground command counter mismatches the spacecraft command counter	Increments to any command counter, along with time tag. If mismatch, log ground command counter and spacecraft command counter along with time tag.	Medium	Possible	Normally the ground system will include a command counter in each command packet so the spacecraft knows if any packets were lost in transmission. The spacecraft has another counter on board, and these should always be in sync. A mismatch may be in indicator of a replay attack or connection with a rogue ground station. Logging all counters will also aid forensic audits.
C&DH				Any type of reset	Log any type of reset, including: power-on reset, processor reset, hard reset, application resets, device resets	Increment to any reset counter along with time tag.	Low	Possible	Resets are not uncommon during normal operations, but abnormal resets or number of resets could indicate breach. This indicator does not warrant an alert on its own, but may be useful in the presence of other indicators/signatures.

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
C&DH		LM-0005		Virtualization/ containerization escapes	Log and alert for any abnormal/unauthorized port activity or movement outside defined environment from virtual machines/container	Affected ports or resources along with time tag	Medium	Unlikely	Unauthorized activity from virtual machines/containers could be an indicator of breach and lateral movement.
C&DH				Virtualization/ containerization changes to initialization/ build files.	Log and alert for any changes to initialization/ build files. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	Unauthorized changes to virtual machines/containers could be an indicator of breach and lateral movement.
C&DH				Resource/ trust zone access denials	Log and alert any access attempts that result in denial	User/device/application making the request, resource/trust zone requested, along with time tag	Medium	Unlikely	Access denials are an indicator of privilage escalation and possible breach.
C&DH		EX-0012.02		Unauthorized access or changes to table services	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to table services along with time tags	High	Possible	Some spacecraft employ table services that manage configuration parameters for various hardware/firmware/software functions. These could include: controller gains, global/environment variables, conversion factors, algorithm settings, etc. Changing some parameters could severely impact normal operations, which could result in destruction of the spacecraft. Also note that it is rare for two applications or devices to share a table.
C&DH				Any critical command (ex: propulsion burn sequence)	Log any critical command whether it comes from a ground user or on-board device/application. Validate with mission operations (if possible)	Command sent, message contents, source of command, time tag	Medium	Likely	Some spacecraft have "critical commands" that require special permissions to execute because they affect mission essential functions. These commands are regularly executed during normal operations, so this indicator is not necessarily cause for alarm. However, this indicator may be useful in the presence of other indicators/signatures.
C&DH				Changes to flight rules	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	High	Possible	Some spacecraft employ "flight rules" that are used to enforce various operational constraints (ex: always use redundant component upon startup). Unauthorized changes to flight rules could result in a wide spectrum of issues.
C&DH		EX-0001.02, EX-0013, EX-0013.01, EX-0013.02, EX-0014.02, LM-0002		Unauthorized access or changes to software bus services or common databus services (ex: SpaceWire, CAN, etc.)	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, message protocols, network segmentations, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to databus services along with time tags	High	Possible	The software bus and databuses pass information between on-board applications and devices. Any configuration changes to how these services operate could severely impact the mission. Changes to settings of any databus services will be extremely rare throughout the life of the spacecraft.
C&DH		EX-0012.12		Unauthorized access or changes to clock services	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings (ex: biases, frequency, waveform, etc.), number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to clock services along with time tags	High	Possible	If flight software is capable of controlling distribution of derivative clock services anywhere on the spacecraft, any unauthorized changes could severely impact the mission. Changes to settings of any clock services will be extremely rare throughout the life of the spacecraft.
C&DH				Any application exit	Log and alert any time an application exits	Application along with time tag. Also, log any messages that request the exit along with time tags.	Medium	Possible	Once a spacecraft has completed its boot sequence and enters normal operations, it is extremely rare for a software application to exit. This could be an indication of a simple bit flip or a breach. The FMS may intervene and restart the application upon noticing it has been exited.
C&DH				Unauthorized access or changes to logging services	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to logging services along with time tags	High	Possible	Logging is critical for recovering from anomalies or auditing after an attack. Unauthorized changes to any logging services is a strong indicator of breach. Changes to settings of any logging services will be rare throughout the life of the spacecraft.
C&DH		EX-0012.13		Unauthorized access or changes to machine learning services	Log any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings (weights, biases, etc.), number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to machine learning services along with time tags. Input data drift from distribution of training data should also be monitored.	Low	Unlikely	Some spacecraft employ machine learning models for data processing, anomaly detection, or possibly even autonomous control. Unauthorized changes to a model, its service, or corruption of input data could have a wide spectrum of consequences. It is not uncommon for model settings to change throughout the mission life, so this indicator is not necessarily cause for alarm. However, this indicator may be useful in the presence of other indicators/signatures.
C&DH		EX-0008		Unauthorized access or changes to scheduler services	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to scheduler services along with time tags	High	Possible	The scheduler is critical for keeping activities on the spacecraft in-sync. Any disruption to this service could cause extreme harm. Changes to settings of any scheduling services will be rare throughout the life of the spacecraft.
C&DH				Unauthorized access or changes to stored command services	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to stored command services along with time tags	High	Possible	Stored command scripts are critical for normal operations and anomaly recovery. Unauthorized changes or suspensions of these services could case extreme harm. Changes to settings of any stored command services will be rare throughout the life of the spacecraft.
C&DH				Unauthorized access or changes to telemetry services	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to telemetry services along with time tags	High	Possible	The telemetry service is critical for monitoring and maintenance of the spacecraft. It regularly gathers data from applications and devices to compile for downlink. Unauthorized changes or suspensions of these services could cause extreme harm. Changes to settings of any telemetry services will be rare throughout the life of the spacecraft.
C&DH				Unauthorized access or changes to diagnostic services	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, self-tests, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to diagnostic services along with time tags	Medium	Possible	Diagnostic services are used to execute built-in self-tests on the spacecraft to help troubleshoot performance issues. Unauthorized changes or suspensions of these services could prolong any recovery efforts. Changes to settings of any diagnostic services will be rare throughout the life of the spacecraft.

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
C&DH				Unauthorized access or changes to data packaging services (ex: high-rate payload data, health telemetry, logs, self-test reports, etc.)	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to stored command services along with time tags	High	Possible	Data integrity and confidentiality is critical for any space mission. Adultured data, especially payload data, will cause a loss of confidence in the mission. Unauthorized changes or suspensions of data packaging services could cause extreme harm. Changes to settings of any data packaging services will be rare throughout the life of the spacecraft.
C&DH		EX-0008, EX-0008.01, EX-0008.02		Changes to stored command scripts (ex: absolute time sequence, relative time sequence, burn sequence, corrective actions, etc.)	Log any unauthorized changes. Validate with mission operations (if possible)	Script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	Changes to stored command scripts will be very frequent throughout the mission life. While not normally a cause for alarm, unauthorized changes to sensitive stored commands (ex: burn sequence) could result in extreme harm.
C&DH				Changes to built-in self-tests	Log any unauthorized changes. Validate with mission operations (if possible)	Script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	Built-in self-tests are often employed by mission operators as a way to gather more detailed diagnostic information after a spacecraft experiences an anomaly. Any changes to these on-board tests could disrupt recovery actions. Changes to these tests will be rare throughout the life of the spacecraft.
C&DH		DE-0010		Memory performance issues (ex: corruption, system/ application crashes, fault states, etc.)	Log and alert	Memory utilization rate, heap/stack/buffer overflows (if detectable), affected memory locations (if possible), any other memory log information available, and time tags	High	Likely	Memory safety is critical for ensuring the reliable and predictable operation of the spacecraft's subsystems. Memory safety issues incude: heap/ stack/buffer overflow, memory leaks, use after free, use of uninitialized memory, and double free. These issues can cause unexpected behaviors that could lead to system failures or open up other attack vectors. Sometimes these vulnerabilities are the result of poor coding practices or radiation-induced faults. Attackers may use these weaknesses to place the spacecraft in a fault state or as part of a broader attack chain.
C&DH				Unauthorized access or changes to memory management services	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to memory management services along with time tags	High	Possible	The memory management service in an operating system is responsible for efficiently managing the flight computer's memory resources. It plays a crucial role in allocating, deallocating, and organizing memory to ensure that processes and applications run smoothly. Changes to settings of memory management services will be rare throughout the life of the spacecraft.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/ Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
TT&C				Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
TT&C	SDR Routers Crypto Intrusion Detection			Access to TT&C subsystem is acquired from a subsystem other than the flight computer (assuming connection to common databus)	Log and alert all access to the TT&C system if not from the flight computer. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	High	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. The TT&C should primarily interact with the C&DH subsystem. Could be a leading indicator for reconnaissance/lateral movement.
TT&C	SDR Routers Crypto Intrusion Detection			Access from TT&C subsystem to a subsystem other than the flight computer is initiated (assuming connection to common databus)	Log all access from the TT&C system if not to the flight computer. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	High	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. The TT&C should primarily interact with the C&DH subsystem. Could be a leading indicator for reconnaissance/lateral movement.
TT&C	SDR Routers Crypto Intrusion Detection			Communication to TT&C from a subsystem other than flight computer (assuming connection to common databus)	Log all messages addressed to the TT&C system if not from the flight computer	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	High	Unlikely	Unauthorized subsystem communication could indicate compromise. The TT&C should primarily interact with the C&DH subsystem. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
TT&C				Memory peeks/dumps that reveal any TT&C configuration information	Log any memory peek/dump command received	Memory addresses, requested information, user who made the request (if possible) along with time tag	High	Unlikely	Downlinking any information about how the ground connects to the spacecraft could be an indicator of breach. This information would be necessary to establish contact through a rogue ground station.
TT&C	SDR Antennas Crypto	IA-0004, IA-0004.02		Communication with a redundant TT&C component (assuming it is not being used as the primary)	Log all messages addressed to the redundant TT&C component	Capture source uplink/subsystem, message contents, databus ports involved (if applicable), with time tags	High	Unlikely	Threat actors may attempt to establish connection through a secondary/backup TT&C component to evade other active detection measures. This poses an equal risk for the uplink and downlink; the attack may result in mission denial and/or data exfiltration.
TT&C	SDR	IA-0002		Changes to or corruption of stored firmware images and boot mechanisms (if possible)	Log and alert if mismatch occurs. Validate with mission operations (if possible)	Include actual and expected check sum/hash values along with memory addresses (if applicable)	High	Likely	FMS will likely troubleshoot/change to a fault mode (ex: Safe Mode) if the SDR firmware image is corrupted. Could indicate a simple component failure or introduction of malicious code that may result in hijacking of spacecraft.
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to signal protocol parameters and/or message standards	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	Changing the signal protocol for communicating with the ground could prevent the spacecraft from receiving properly formatted commands, and prevent the ground from receiving properly formatted telemetry/mission data. FMS may intervene if any configuration changes occur. Changes are extremely rare throughout the life of a spacecraft, and this situation will likely result in a prolonged outage or even loss of mission.
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to frequency hopping characteristics (if applicable)	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Possible	If the up/downlink employ a frequency hopping scheme, any configuration changes could severely impact the ability to communicate with the spacecraft. FMS may intervene if any configuration changes occur.
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002, EXF-0004		Changes to carrier frequency/waveform	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	High	Possible	Changes to the carrier frequency could result in loss of service between the ground and spacecraft. FMS may intervene if any configuration changes occur. Changes are extremely rare throughout the life of a spacecraft.
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to modulation/demodulation schemes	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	Changes to the mod/demodulation schemes could result in loss of service between the ground and spacecraft. FMS may intervene if any configuration changes occur. Changes are extremely rare throughout the life of a spacecraft.
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to ground authentication and authorization policies and/or digital signature management	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	Changes to ground user authentication/authorization could be an indicator of breach and/or privilege escalation.
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to error detection and correction algorithms/ parameters	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Low	Possible	Changes to EDAC methodologies could result in malformed packets being sent/received between the spacecraft and ground. This might result in interruptions to the mission. FMS may intervene if any configuration changes occur. Changes are extremely rare throughout the life of a spacecraft.
TT&C	SDR Routers Crypto	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to router configurations (if applicable)	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Possible	If the TT&C system employs a router/SDN for directing information on various databuses, configuration changes could seriously impact spacecraft operations.

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/ Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to bit encoding/ decoding schemes	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	Changes to the bit en/decoding schemes could result in loss of service between the ground and spacecraft. Changes are extremely rare throughout the life of a spacecraft.
TT&C	SDR Antennas Routers Crypto Intrusion Detection	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to off-nominal mode configurations (Sleep, Safe, Dwell, Standby, etc.)	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	Upon changing spacecraft modes (ex: Safe Mode), the TT&C is heavily relied upon for troubleshooting and safing the spacecraft. Any changes to the special configuration or expected behavior during these emergencies could result in loss of mission. FMS may intervene if any configuration changes occur.
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes in transmission power levels	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Medium	Possible	Changing transmission power levels could be an indication of attack execution. Power is a precious resource on a spacecraft, and RF transmission is expensive. Increasing power levels could affect the spacecraft's power budget and may be part of a larger attack. The FMS is unlikely to flag a change in power levels, but may intervene if the overall power budget drops below a certain threshold.
TT&C	SDR	EXF-0006, EXF-0006.01, EXF-0006.02, DE-0002, DE-0002.03, IMP-0002		Changes to automatic gain control settings	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Low	Possible	Changing gain control settings could prevent the spacecraft from distinguishing the uplink signal from the noise floor and cause a disruption in service. FMS may intervene if any configuration changes occur.
TT&C	SDR	EX-0016.01, IMP-0002		Abnormal uplink signal characteristics (ex: low SNR, high power levels, etc.)	Log and alert	Spacecraft position and uplink signal characteristics (power levels, SNR, center frequency, etc.) if possible	High	Possible	Abnormal signal characteristics could indicate the spacecraft is being jammed, either from a source on the ground or in space. Logging any information about the anomalous signal along with any geolocation information available will help determine if the spacecraft is under attack.
TT&C	SDR Antennas Routers Crypto Intrusion Detection			Abnormal logging behaviors	Log and alert when any irregular logging behaviors are detected (if possible)	Log expected behavior and observed behavior, along with time tags	Medium	Unlikely	Because the SDR is reprogrammable, its logging behaviors can also be changed. Modifying or deleting logs is a common practice for attackers that want to obfuscate actions taken on their target. If there are any changes to the frequency at which the TT&C system reports log messages, or the content of those messages, these events should be logged and alerted.
TT&C	Encryptor	PER-0004		Changes to cryptographic key management and/or storage	Log and alert for any changes. Validate with mission operations (if possible).	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	If it is possible to upload/change new cryptographic keys and/or how the keys are managed/rotated, this could pose a critical attack vector. It could cause a loss of mission or possibly even spacecraft hijacking. FMS may intervene if any configuration changes occur.
TT&C	Encryptor	EX-0006		Any received bypass commands	Log and alert under all circumstances. Validate with mission operations (if possible)	Command sent and time tag at a minimum. Spacecraft position and uplink signal characteristics (power levels, SNR, center frequency, etc.) if possible	High	Likely	Encryptor bypass commands should be extremely infrequent throughout the life a spacecraft. They are provided as a backup in case the encryptor fails. Any time these commands are sent they should be carefully monitored.
TT&C	Encryptor	PER-0004		Any received key change commands	Log and alert under all circumstances. Validate with mission operations (if possible)	Command sent and time tag at a minimum. Spacecraft position and uplink signal characteristics (power levels, SNR, center frequency, etc.) if possible	High	Possible	Changing keys is common practice during normal operations. However, because matching keys are critical for symmetrical encryption algorithms, extreme care should be taken when executing these commands. Key mismatch will result in loss of communication between the ground and spacecraft.
TT&C	Encryptor	EX-0006		Disable encryptor (if possible)	Log and alert under all circumstances. Validate with mission operations (if possible)	Command sent and time tag at a minimum. Spacecraft position and uplink signal characteristics (power levels, SNR, center frequency, etc.) if possible	High	Possible	Under extreme circumstances (ex: Safe Mode), it may be possible to disable or turn off the encryptor. This poses a critical attack vector, and could cause a loss of mission or possibly even spacecraft hijacking. FMS may or may not intervene depending on the spacecraft's state.
TT&C	Antenna			Changes to gimbal control constants	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Low	Unlikely	Changing control constants for directional antenna gimbals could prevent communication between the ground and spacecraft. Most spacecraft include omni-directional antennas as a backup, so this vector is low threat in those instances. However, this is an indicator of breach.
TT&C	Antenna			Changes to signal tracking algorithms (if not handled in SDR)	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Low	Unlikely	Changing signal tracking algorithms for directional antennas could prevent communication between the ground and spacecraft. Most spacecraft include omni-directional antennas as a backup, so this vector is low threat in those instances. However, this is an indicator of breach.
TT&C	Antenna			Off-nominal activation/ deactivation of RF switches (if not handled in SDR)	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory blocks along with time tag. Include hashes/checksum (if possible)	Medium	Possible	Unauthorized activation/ deactivation could indicate breach. Deactivation could prevent communication with the ground, and activation could expend unnecessary amounts of power. FMS may intervene if any configuration changes occur.
TT&C	Power amplifiers			Changes to configuration parameters (if software controlled)	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Medium	Possible	Similar to changing transmission power levels, changing power amplifier configuration (if possible in software) could result in unnecessary power expenditures. It could also make incoming signals too loud to decipher.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
SMS				Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
SMS				Access to S&M subsystem is acquired from another sub-system (ex: Payload) to initiate actions	Log and alert all access to the S&M subsystem. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
SMS				Access from S&M subsystem to another sub-system (ex: Payload) is initiated	Log all access from the S&M subsystem. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
SMS				Communication to S&M from another subsystem	Log all messages directly addressed to the S&M system (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
SMS				Critical S&M subcomponent signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot/change to a fault mode. Could indicate a simple component failure or intrusion.
SMS	Gimbals, Deployment mechanisms, Docking mechanisms (if applicable)			Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	High	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
SMS	Gimbals, Deployment mechanisms, Docking mechanisms (if applicable)			Change in control logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Thermal control logic/constants rarely change after Launch and Early Operations. Could be an indicator of compromise. Changes in how heaters, coolers, louvers/shutters, or radiators are controlled could have severe consequences to the mission.
SMS	Docking mechanisms	IA-0005.01, IA-0005.02, IA-0005.03, IA-0011, LM-0004		Unplanned docking	Log and alert any unplanned docking	Telemetry such as motor movements, databus/port chatter, abrupt attitude changes, along with time tags	High	Possible	Unplanned docking could be an indicator of a physical attack. While an adjacent concern to cybersecurity, this vector could be used to physically inject malware into the spacecraft.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
TCS				Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
TCS				Access to TCS subsystem is acquired from another sub-system (ex: Payload) to initiate actions	Log and alert all access to the TCS subsystem. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
TCS				Access from TCS subsystem to another sub-system (ex: Payload) is initiated	Log all access from the TCS subsystem. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
TCS				Communication to TCS from another subsystem	Log all messages directly addressed to the TCS system (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
TCS				Critical TCS subcomponent signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot/change to a fault mode. Could indicate a simple component failure or intrusion.
TCS	Processing electronics, Heaters, Coolers, Louver/ Shutter/ Radiator mechanisms (if applicable)			Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	High	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
TCS	Temperature control, Louver/Shutter control, Radiator control			Change in control logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Thermal control logic/constants rarely change after Launch and Early Operations. Could be an indicator of compromise. Changes in how heaters, coolers, louvers/shutters, or radiators are controlled could have severe consequences to the mission.
TCS	Thermistors, Thermocouples			Change calibration tables	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Unlikely	If temperature sensor data are converted to engineering units on-board the spacecraft there may be calibration tables to convert raw bits. Unauthorized changes could be catastrophic for temperature control.
TCS	Thermoelectric Coolers (TEC)			Change in polarity	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters and time tags	Medium	Unlikely	Thermoelectric Coolers are often used to directly cool sensitive electronic components. If it is possible to change the polarity in software, this could add heat rather than remove heat and result in mission degradation or loss.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
Payload - Imagery		EX-0012.06		Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
Payload - Imagery		EXF-0010		Access to payload is acquired from another sub-system (ex: ADCS) to initiate actions	Log and alert all access to the payload. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
Payload - Imagery				Access from payload to another sub-system (ex: ADCS) is initiated	Log all access from the payload. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
Payload - Imagery				Communication to payload from another subsystem	Log all messages directly addressed to the payload (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
Payload - Imagery				Critical payload subcomponent signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot or disable the payload. Could indicate a simple component failure or intrusion.
Payload - Imagery				Changes to collection requests or stored command scripts (ex: absolute time sequence, relative time sequence, etc.)	Log any unauthorized changes. Validate with mission operations (if possible)	Script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Low	Unlikely	Changes to collection requests will be very frequent throughout the mission life. While not normally a cause for alarm, unauthorized changes (perhaps while not in contact with the ground) could be an indication of breach.
Payload - Imagery	Focal Plane Array (FPA)			Change calibration tables/sequences	Log and alert when values or command sequences are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Unlikely	Some FPAs occasionally need to be calibrated, and this can be done automatically via command script or by manually updating table values from the ground. Unauthorized changes could severely impact image quality/collection.
Payload - Imagery	FPA, Control electronics, Heaters, Coolers, Pointing gimbals, Mechanisms (ex: iris, shutter, louver, radiator, lens focus, filters, etc.) (if applicable)			Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	High	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
Payload - Imagery	Image capture control, Power conditioning/ distribution, Pointing control, Mechanism control (ex: iris, shutter, louver, radiator, lens focus, filters, etc.)			Change in control logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Camera control logic/constants rarely change which could be an indicator of compromise. Changes in how power, heaters, coolers, iris/shutters, filters, focus mechanisms, or radiators are controlled could have severe consequences to the mission.
Payload - Imagery	Thermoelectric Coolers (TEC)			Change in polarity	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters and time tags	Medium	Unlikely	Thermoelectric Coolers are often used to directly cool sensitive electronic components like the FPA. If it is possible to change the polarity in software, this could add heat rather than remove heat and result in mission degradation or loss.
Payload - Imagery	Iris/Shutter			Change in light/photodiode set limits	Log and alert to any changes in light limits	Any key-value pairs associated with set limits, along with a time tag	High	Possible	Camera iris/shutters are important mechanisms for protecting the FPA from damaging levels of photonic energy (light). Unauthorized light set limits could result in mission degradation/loss.
Payload - Imagery	FPA			Change in correction logic/algorithms	Log and alert any changes to image correction constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	FPAs often have correction algorithms that can remove background noise, static objects, etc. Changes to these algorithms could severely impact image processing on-board and/or on the ground.
Payload - Imagery	FPA			Abnormal noise floor/saturation	Log and alert	Spacecraft position and attitude, along with image characteristics (average energy levels, number and location of saturated pixels, etc.) and time tag	High	Unlikely	Abnormal image characteristics could indicate the spacecraft is being dazzled, either from a source on the ground or in space. Logging any information about the anomalous image along with any geolocation information available will help determine if the spacecraft is under attack.
Payload - Imagery	FPA			Persistent hot/dead pixels	Log any new pixels	Number of persistent hot/dead pixels, along with time tag	Low	Unlikely	Pixels that consistently read at the max value of their dynamic range are called "hot pixels." Pixels that consistently read at the minimum value of their dynamic range are called "dead pixels." Either case can occur if the FPA experiences a damaging amount of exposure to photonic energy, or perhaps from extreme space weather events (among other reasons). Some payloads will count these pixels and disable them, typically after calibrating against a dark background (with the iris closed). While not an alarming event on its own, if there is an unusual increase in dysfunctional pixels it could indicate some kind of attack.
Payload - Imagery	FPA			Pixels marked/unmarked as hot/dead	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Medium	Unlikely	There is sometimes a way to ignore hot/dead pixels in software/firmware so they do not disrupt processing algorithms. Any pixels added or removed from this list should be logged.
Payload - Imagery	FPA			Changes in exposure settings	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Medium	Unlikely	Exposure settings dictate how an FPA collects and reads photonic energy. Any changes could severely disrupt mission data integrity.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/ Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
Payload - RF		EX-0012.06		Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
Payload - RF		EXF-0010		Access to payload is acquired from another sub-system (ex: ADCS) to initiate actions	Log and alert all access to the payload. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
Payload - RF				Access from payload to another sub-system (ex: ADCS) is initiated	Log all access from the payload. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
Payload - RF				Communication to payload from another subsystem	Log all messages directly addressed to the payload (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
Payload - RF				Communication with a redundant payload component (assuming it is not being used as the primary)	Log all messages addressed to the redundant payload component	Capture source uplink/subsystem, message contents, databus ports involved (if applicable), with time tags	High	Unlikely	If the RF payload is acting as a relay, threat actors may attempt to establish connection through a secondary/backup payload component to evade other active detection measures. This poses an equal risk for the uplink and downlink; the attack may result in mission denial and/or data exfiltration.
Payload - RF				Critical payload subcomponent signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot or disable the payload. Could indicate a simple component failure or intrusion.
Payload - RF				Changes to collection/allocation requests or stored command scripts (ex: absolute time sequence, relative time sequence, etc.)	Log any unauthorized changes. Validate with mission operations (if possible).	Script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Low	Unlikely	Changes to collection/allocation requests will be very frequent throughout the mission life. While not normally a cause for alarm, unauthorized changes (perhaps while not in contact with the ground) could be an indication of breach.
Payload - RF	SDR			Changes to or corruption of stored firmware images and boot mechanisms (if possible)	Log and alert if mismatch occurs. Validate with mission operations (if possible)	Include actual and expected check sum/ hash values along with memory addresses (if applicable)	High	Likely	FMS will likely troubleshoot/change to a fault mode (ex: Safe Mode) if the payload firmware image is corrupted. Could indicate a simple component failure or introduction of malicious code that may result in hijacking of spacecraft.
Payload - RF	SDR			Changes to signal protocol parameters and/or message standards	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	If the RF payload is acting as a relay, changing the signal protocol could prevent user communication. Changes are extremely rare throughout the life of a spacecraft, and this situation will likely result in a prolonged outage.
Payload - RF	SDR			Changes to frequency hopping characteristics (if applicable)	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	If the up/downlink employ a frequency hopping scheme, any configuration changes could severely impact the ability of the payload to act as a relay.
Payload - RF	SDR			Changes to carrier frequency/waveform	Log and alert for any changes. Validate with mission operations (if possible).	New values, memory addresses/blocks (if applicable), along with time tag	Medium	Unlikely	If the RF payload is acting as a relay, changes to the carrier frequency could result in loss of service for users.
Payload - RF	SDR			Changes to modulation/demodulation schemes	Log and alert for any changes. Validate with mission operations (if possible).	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	If the RF payload is acting as a relay, changes to the mod/demodulation schemes could result in loss of service for users.
Payload - RF	SDR			Changes to user authentication and authorization policies and/or digital signature management	Log and alert for any changes. Validate with mission operations (if possible).	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	If the RF payload is acting as a relay, changes to user authentication/authorization could be an indicator of breach and/or privilege escalation.
Payload - RF	SDR			Changes to error detection and correction algorithms/ parameters	Log and alert for any changes. Validate with mission operations (if possible).	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Low	Unlikely	If the RF payload is acting as a relay, changes to EDAC methodologies could result in malformed packets being sent/received.
Payload - RF	SDR			Changes to router configurations (if applicable)	Log and alert for any changes. Validate with mission operations (if possible).	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	If the RF payload is acting as a relay and employs a router/SDN for channelizing signals, configuration changes could seriously impact user connectivity.
Payload - RF	SDR			Changes to bit encoding/ decoding schemes	Log and alert for any changes. Validate with mission operations (if possible).	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	If the RF payload is acting as a relay, changes to the bit en/decoding schemes could result in loss of service for users.
Payload - RF	SDR			Changes to off-nominal mode configurations (Sleep, Safe, Dwell, Standby, etc.)	Log and alert for any changes. Validate with mission operations (if possible).	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	Upon changing spacecraft modes (ex: Safe Mode), payload communication channels may be used for troubleshooting and safing the spacecraft. Any changes to the special configuration or expected behavior during these emergencies could result in loss of mission. FMS may intervene if any configuration changes occur.
Payload - RF	SDR			Changes in transmission power levels	Log and alert for any changes. Validate with mission operations (if possible).	New values, memory addresses/blocks (if applicable), along with time tag	Medium	Possible	Changing transmission power levels could be an indication of attack execution. Power is a precious resource on a spacecraft, and RF transmission is expensive. Increasing power levels could affect the spacecraft's power budget and may be part of a larger attack. The FMS is unlikely to flag a change in power levels, but may intervene if the overall power budget drops below a certain threshold.
Payload - RF	SDR			Changes to automatic gain control settings	Log and alert for any changes. Validate with mission operations (if possible).	New values, memory addresses/blocks (if applicable), along with time tag	Low	Unlikely	Changing gain control settings could prevent the payload from distinguishing the uplink signal from the noise floor and cause a disruption in service/data collection. FMS may intervene if any configuration changes occur.
Payload - RF	SDR			Abnormal uplink signal characteristics (ex: low SNR, high power levels, etc.)	Log and alert.	Spacecraft position and uplink signal characteristics (power levels, SNR, center frequency, etc.) if possible.	High	Possible	Abnormal signal characteristics could indicate the spacecraft is being jammed, either from a source on the ground or in space. Logging any information about the anomalous signal along with any geolocation information available will help determine if the spacecraft is under attack.

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/ Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
Payload - RF	SDR			Abnormal logging behaviors	Log and alert when any irregular logging behaviors are detected (if possible)	Log expected behavior and observed behavior, along with time tags	Medium	Unlikely	Because the SDR is reprogrammable, its logging behaviors can also be changed. Modifying or deleting logs is a common practice for attackers that want to obfuscate actions taken on their target. If there are any changes to the frequency at which the payload reports log messages, or the content of those messages, these events should be logged and alerted.
Payload - RF	Encryptor			Changes to cryptographic key management and/or storage	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	If it is possible to upload/change new cryptographic keys and/or how the keys are managed/rotated, this could pose a critical attack vector. FMS may intervene if any configuration changes occur.
Payload - RF	Encryptor			Any received bypass commands	Log and alert under all circumstances. Validate with mission operations (if possible)	Command sent and time tag at a minimum. Spacecraft position and uplink signal characteristics (power levels, SNR, center frequency, etc.) if possible	High	Likely	Encryptor bypass commands should be extremely infrequent throughout the life a spacecraft. They are provided as a backup in case the encryptor fails. Any time these commands are sent they should be carefully monitored.
Payload - RF	Encryptor			Any received key change commands	Log and alert under all circumstances. Validate with mission operations (if possible)	Command sent and time tag at a minimum. Spacecraft position and uplink signal characteristics (power levels, SNR, center frequency, etc.) if possible	High	Possible	Changing keys is common practice during normal operations. However, because matching keys are critical for symmetrical encryption algorithms, extreme care should be taken when executing these commands. Key mismatch will result in loss of communication between the ground and spacecraft.
Payload - RF	Encryptor			Disable encryptor (if possible)	Log and alert under all circumstances. Validate with mission operations (if possible)	Command sent and time tag at a minimum. Spacecraft position and uplink signal characteristics (power levels, SNR, center frequency, etc.) if possible	High	Possible	Under extreme circumstances (ex: Safe Mode), it may be possible to disable or turn off the encryptor. This poses a critical attack vector, and could cause a loss of mission or possibly even spacecraft hijacking. FMS may or may not intervene depending on the spacecraft's state.
Payload - RF	Antenna			Changes to gimbal control constants	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Low	Unlikely	Changing control constants for directional antenna gimbals could prevent communication/collection.
Payload - RF	Antenna			Changes to signal tracking algorithms (if not handled in SDR)	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Low	Unlikely	Changing signal tracking algorithms for directional antennas could prevent communication/collection.
Payload - RF	Antenna			Off-nominal activation/ deactivation of RF switches (if not handled in SDR)	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory blocks along with time tag. Include hashes/checksum (if possible)	Medium	Possible	Unauthorized activation/deactivation could indicate breach. Deactivation could prevent communication/collection, and activation could expend unnecessary amounts of power. FMS may intervene if any configuration changes occur.
Payload - RF	Power amplifiers			Changes to configuration parameters (if software controlled)	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Medium	Possible	Similar to changing transmission power levels, changing power amplifier configuration (if possible in software) could result in unnecessary power expenditures. It could also make incoming signals too loud to decipher.
Payload - RF	Control electronics, Heaters, Coolers, Mechanisms (ex: radiator) (if applicable)			Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	High	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
Payload - RF	Power conditioning/ distribution, Heaters, Coolers, Mechanism control (ex: radiator)			Change in control logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Control logic/constants rarely change which could be an indicator of compromise. Changes in how power, heaters, coolers, or radiators are controlled could have severe consequences to the mission.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
Payload - OCT		IA-0003, IA-0008, IA-0008.02, LM-0003		Unauthorized crosslink connections	Log all connections with other spacecraft	Log any authorization/ authentication information (if available), signal characteristics, time tag	High	Unlikely	Establishing a crosslink with a compromised or malicious spacecraft could result in severe consequences.
Payload - OCT		EX-0012.06		Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
Payload - OCT		EXF-0010		Access to payload is acquired from another sub-system (ex: ADCS) to initiate actions	Log and alert all access to the payload. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
Payload - OCT				Access from payload to another sub-system (ex: ADCS) is initiated	Log all access from the payload. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
Payload - OCT				Communication to payload from another subsystem	Log all messages directly addressed to the payload (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
Payload - OCT				Communication with a redundant payload component (assuming it is not being used as the primary)	Log all messages addressed to the redundant payload component	Capture source uplink/subsystem, message contents, databus ports involved (if applicable), with time tags	High	Unlikely	Threat actors may attempt to establish connection through a secondary/backup payload component to evade other active detection measures. This poses an equal risk for the uplink and downlink; the attack may result in mission denial and/or data exfiltration.
Payload - OCT				Critical payload subcomponent signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot or disable the payload. Could indicate a simple component failure or intrusion.
Payload - OCT				Changes to signal protocol parameters and/or message standards	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	Changing the signal protocol could prevent user communication. Changes are extremely rare throughout the life of a spacecraft, and this situation will likely result in a prolonged outage.
Payload - OCT				Changes to carrier frequency/waveform/polarization	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Medium	Unlikely	Changes to the carrier frequency could result in loss of service for users.
Payload - OCT				Changes to modulation/demodulation schemes	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	Changes to the mod/demodulation schemes could result in loss of service for users.
Payload - OCT				Changes to error detection and correction algorithms/ parameters	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Low	Unlikely	Changes to EDAC methodologies could result in malformed packets being sent/received.
Payload - OCT				Changes to bit encoding/ decoding schemes	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Medium	Unlikely	Changes to the bit en/decoding schemes could result in loss of service for users.
Payload - OCT				Changes to automatic gain control settings	Log and alert for any changes. Validate with mission operations (if possible)	New values, memory addresses/blocks (if applicable), along with time tag	Low	Unlikely	Changing gain control settings could prevent the payload from distinguishing a signal from the noise floor and cause a disruption in service.
Payload - OCT				Changes to off-nominal mode configurations (Sleep, Safe, Dwell, Standby, etc.)	Log and alert for any changes. Validate with mission operations (if possible)	Values of new default parameters, script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	High	Possible	Upon changing spacecraft modes (ex: Safe Mode), payload communication channels may be used for troubleshooting and safing the spacecraft. Any changes to the special configuration or expected behavior during these emergencies could result in loss of mission. FMS may intervene if any configuration changes occur.
Payload - OCT				Abnormal uplink signal characteristics (ex: low SNR, high power levels, etc.)	Log and alert	Spacecraft position and attitude, along with image characteristics (average energy levels, number and location of saturated pixels, etc.) and time tag	High	Unlikely	Abnormal image characteristics could indicate the spacecraft is being dazzled, either from a source on the ground or in space. Logging any information about the anomalous signals along with any geolocation information available will help determine if the spacecraft is under attack.
Payload - OCT	Control electronics, Heaters, Coolers, Pointing gimbals, Mechanisms (ex: steering mirrors) (if applicable)			Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	High	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
Payload - OCT	Signal tracking, Power conditioning/ distribution, Heaters, Amplifiers, Modulators, Collimators, Filters, Mechanism control (ex: steering mirrors)			Change in control logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	High	Possible	Control logic/constants rarely change which could be an indicator of compromise.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
Payload - Data Processing		EX-0012.06		Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
Payload - Data Processing		EXF-0010		Access to payload is acquired from another sub-system (ex: ADCS) to initiate actions	Log and alert all access to the payload. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
Payload - Data Processing				Access from payload to another sub-system (ex: ADCS) is initiated	Log all access from the payload. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
Payload - Data Processing				Communication to payload from another subsystem	Log all messages directly addressed to the payload (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
Payload - Data Processing				Communication with a redundant payload component (assuming it is not being used as the primary)	Log all messages addressed to the redundant payload component	Capture source uplink/subsystem, message contents, databus ports involved (if applicable), with time tags	High	Unlikely	Threat actors may attempt to establish connection through a secondary/backup payload component to evade other active detection measures. The attack may result in mission denial and/or data exfiltration.
Payload - Data Processing				Critical payload subcomponent signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot or disable the payload. Could indicate a simple component failure or intrusion.
Payload - Data Processing				Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	Medium	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
Payload - Data Processing				Change in control logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	Medium	Possible	Control logic/constants rarely change which could be an indicator of compromise.
Payload - Data Processing				Change in signal detection, classification, or processing logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	Medium	Possible	Changes to data processing logic/constants could be an indicator of compromise.
Payload - Data Processing		EX-0014.03		Unauthorized access or changes to data packaging services (ex: high-rate payload data, health telemetry, logs, self-test reports, etc.)	Log and alert for any unauthorized access or changes. Validate with mission operations (if possible)	Changes to settings, number of resets, or APIs for all responsible applications along with time tags. Also, log any messages that request changes to stored command services along with time tags	Medium	Possible	Data integrity and confidentiality is critical for any space mission. Adulterated data, especially payload data, will cause a loss of confidence in the mission. Unauthorized changes or suspensions of data packaging services could cause extreme harm. Changes to settings of any data packaging services will be rare throughout the life of the spacecraft.

Index & Acronyms (link)

Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/Prioritization (Low/Medium/High)	FMS Redundancy (Likely/Possible/ Unlikely)	Response Significance (User or FMS)
Payload - Hosted		EX-0012.06		Modification of hardware configuration key-value pairs	Log and alert when values are modified. Validate with mission operations (if possible)	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation.
Payload - Hosted		EXF-0010		Access to payload is acquired from another sub-system (ex: ADCS) to initiate actions	Log and alert all access to the payload. Confirm access is authenticated and authorized (if possible)	Source subsystem, request/command, and time tag	Medium	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise. Could be a leading indicator for reconnaissance/lateral movement.
Payload - Hosted		IA-0006, LM-0001		Access from payload to another sub-system (ex: ADCS) is initiated	Log all access from the payload. Confirm access is authenticated and authorized (if possible)	Target subsystem, request/command, and time tag	Low	Unlikely	Unauthorized subsystem communication/commanding could indicate compromise.
Payload - Hosted				Communication to payload from another subsystem	Log all messages directly addressed to the payload (not broadcast/subscribed messages)	Capture source subsystem, message contents, databus ports involved (if applicable), with time tags	Low	Unlikely	Unauthorized subsystem communication could indicate compromise. Abnormal intra-spacecraft communication could indicate DoS, reconnaissance, lateral movement, or attack in progress.
Payload - Hosted				Communication with a redundant payload component (assuming it is not being used as the primary)	Log all messages addressed to the redundant payload component	Capture source uplink/subsystem, message contents, databus ports involved (if applicable), with time tags	High	Unlikely	Threat actors may attempt to establish connection through a secondary/backup payload component to evade other active detection measures. This poses an equal risk for the uplink and downlink; the attack may result in mission denial and/or data exfiltration.
Payload - Hosted				Critical payload subcomponent signal anomalies	Log and alert any signal disruptions or anomalies	Abnormal events like loss of power/comm, abrupt signal changes, or states not typically entered in context of the spacecraft state/mode	High	Likely	FMS may troubleshoot or disable the payload. Could indicate a simple component failure or intrusion.
Payload - Hosted				Changes to collection/allocation requests or stored command scripts (ex: absolute time sequence, relative time sequence, etc.)	Log any unauthorized changes. Validate with mission operations (if possible)	Script/routine changes (or hashes), memory addresses/blocks (if applicable), and time tags	Low	Unlikely	Changes to collection/allocation requests will be very frequent throughout the mission life. While not normally a cause for alarm, unauthorized changes (perhaps while not in contact with the ground) could be an indication of breach.
Payload - Hosted				Change in temperature set limits (high/low)	Log and alert to any changes in temperature limits	Any key-value pairs associated with set limits, along with a time tag	Medium	Possible	Unauthorized temperature set limits could result in mission degradation/loss depending on the affected subcomponent.
Payload - Hosted				Change in control logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	Medium	Possible	Control logic/constants rarely change which could be an indicator of compromise.
Payload - Hosted				Change in signal detection, classification, or processing logic/algorithms	Log and alert any changes to control constants or algorithms	Key-value pairs of control parameters, script/routine changes (or hashes), and time tags	Medium	Possible	Changes to data processing logic/constants could be an indicator of compromise.

SPARTA_Mapping Tab

Mini-Abstract - SPARTA Matrix Deconstruction

The following **SPARTA_Mapping** tab is a deconstruction of the SPARTA matrix with applied analytics within the Stellar Space Cyber Range (SSCR) to identify which subsystems these attack vectors could be applied to. The table outlines all the attacks, found within Aerospace's SPARTA matrix, that are directed specifically at the spacecraft's subsystems.

Each attack has an included ID# (with SPARTA website link), Name, and Description pulled directly from the SPARTA Matrix. Each attack is further broken down into the affected Subsystem, Sub-component, Data type, and the associated Attack Vector.

Questions/comments: SV-Logging-BPG@stephensonstellar.org

SPARTA Mapping Abstract (link)

ID	Name	Description	Subsystem	Sub-Component	Data Type	Attack Vector
IA-0002	Compromise Software Defined Radio	Threat actors may target software defined radios due to their software nature to establish C2 channels. Since SDRs are programmable, when combined with supply chain or development environment attacks, SDRs provide a pathway to setup covert C2 channels for a threat actor	Comm	SDR	Logged Commands, Authentication Logs	Weak Authentication
IA-0003	Crosslink via Compromised Neighbor	Threat actors may compromise a victim spacecraft via the crosslink communications of a neighboring spacecraft that has been compromised. spacecraft in close proximity are able to send commands back and forth. Threat actors may be able to leverage this access to compromise other spacecraft once they have access to another that is nearby	Comm	SDR & OCT	Comm & Command Data	Compromised Sat
IA-0004	Secondary/Backup Communication Channel	Threat actors may compromise alternative communication pathways which may not be as protected as the primary pathway. Depending on implementation the contingency communication pathways/solutions may lack the same level of security (i.e., physical security, encryption, authentication, etc.) which if forced to use could provide a threat actor an opportunity to launch attacks. Typically these would have to be coupled with other denial of service techniques on the primary pathway to force usage of secondary pathways	Comm	Mission data link, CMD/TLM data Link	Command Data & Authentication Logs	Weak Encryption, DOS
IA-0004.02	Receiver	Threat actors may target the backup/secondary receiver on the space vehicle as a method to inject malicious communications into the mission. The secondary receivers may come from different supply chains than the primary which could have different level of security and weaknesses. Similar to the ground station, the communication through the secondary receiver could be forced or happening naturally	Comm	Redundant Transponder	Command Data & RF	Weak encryption/Authentication, FMS Bypass, Malware injections
IA-0005	Rendezvous & Proximity Operations	Threat actors may perform a space rendezvous which is a set of orbital maneuvers during which a spacecraft arrives at the same orbit and approach to a very close distance (e.g., within visual contact or close proximity) to a target spacecraft	Comm	Transponder	Crosslink Comm	Proximity, Physical, MITM
IA-0005.01	Compromise Emanations	Threat actors in close proximity may intercept and analyze electromagnetic radiation emanating from crypto equipment and/or the target spacecraft(i.e., main bus) to determine whether the emanations are information bearing. The data could be used to establish initial access	EPS, Data Bus, Comm	Non-hardened EMI/EMC components	Crosslink Comm, EME Leakage	MITM, Proximity, Side Channel
IA-0005.02	Docked Vehicle/OSAM	Threat actors may leverage docking vehicles to laterally move into a target spacecraft. If information is known on docking plans, a threat actor may target vehicles on the ground or in space to deploy malware to laterally move or execute malware on the target spacecraft via the docking interface	ADCS, Structures and Mechs	Docking Mechanism, Connection Port, Attitude, and actuators	Port Chatter, physical interface connections, log data, Docking mechanism log, Attitude anomalies	Physical Interface
IA-0005.03	Proximity Grappling	Threat actors may posses the capability to grapple target spacecraft once it has established the appropriate space rendezvous. If from a proximity/rendezvous perspective a threat actor has the ability to connect via docking interface or expose testing (i.e., JTAG port) once it has grappled the target spacecraft, they could perform various attacks depending on the access enabled via the physical connection	ADCS, Structures and Mechs	Docking Mechanism, Connection Port, Attitude, and actuators	Port Chatter, physical interface connections, log data, Docking mechanism log, Attitude anomalies	Physical Interface
IA-0006	Compromise Hosted Payload	Threat actors may compromise the target spacecraft hosted payload to initially access and/or persist within the system. Hosted payloads can usually be accessed from the ground via a specific command set. The command pathways can leverage the same ground infrastructure or some host payloads have their own ground infrastructure which can provide an access vector as well. Threat actors may be able to leverage the ability to command hosted payloads to upload files or modify memory addresses in order to compromise the system. Depending on the implementation, hosted payloads may provide some sort of lateral movement potential	Payload, Adjunct Payload	Data Bus, EPS	Command data, payload data, permissions requests, data volume, mission data	Hosted Payload Compromise
IA-0008	Rogue External Entity	Threat actors may gain access to a victim spacecraft through the use of a rogue external entity. With this technique, the threat actor does not need access to a legitimate ground station or communication site	Comm	Transponder, Modem, Encryptor, SDR	Command Data, RF, Crosslink	Side Channel, Weak Authentication
IA-0008.02	Rogue Spacecraft	Threat actors may gain access to a target spacecraft using their own spacecraft that has the capability to maneuver within close proximity to a target spacecraft to carry out a variety of TTPs (i.e., eavesdropping, side-channel, etc.). Since many of the commercial and military assets in space are tracked, and that information is publicly available, attackers can identify the location of space assets to infer the best positioning for intersecting orbits. Proximity operations support avoidance of the larger attenuation that would otherwise affect the signal when propagating long distances, or environmental circumstances that may present interference	Comm, Payload	Transponder, Modem, Encryptor, SDR	Command Data, Crosslink	Eavesdropping, side-channel, MITM
IA-0010	Exploit Reduced Protections During Safe-Mode	Threat actors may take advantage of the victim spacecraft being in safe mode and send malicious commands that may not otherwise be processed. Safe-mode is when all non-essential systems are shut down and only essential functions within the spacecraft are active. During this mode, several commands are available to be processed that are not normally processed. Further, many protections may be disabled at this time	Flight Computer, ADCS, TCS, EPS, Comm	FMS	Command data, Command counts, Bus Data, memory registers, configuration changes, SW uploads, telemetry data	malicious script upload, logic bomb

ID	Name	Description	Subsystem	Sub-Component	Data Type	Attack Vector
IA-0011	Auxiliary Device Compromise	Threat actors may exploit the auxiliary/peripheral devices that get plugged into space vehicles. It is no longer atypical to see space vehicles, especially CubeSats, with Universal Serial Bus (USB) ports or other ports where auxiliary/peripheral devices can be plugged in. Threat actors can execute malicious code on the space vehicles by copying the malicious code to auxiliary/peripheral devices and taking advantage of logic on the space vehicle to execute code on these devices. This may occur through manual manipulation of the auxiliary/peripheral devices, modification of standard IT systems used to initially format/create the auxiliary/peripheral device, or modification to the auxiliary/peripheral devices' firmware itself	ADCS, Structures and Mechs	Docking Mechanism, Connection Port, Attitude and actuators	Port Chatter, physical interface connections, log data, Docking mechanism log, Attitude anomalies	Physical Interface, Supply chain
EX-0001	Replay	Replay attacks involve threat actors recording previously recorded data streams and then resending them at a later time. This attack can be used to fingerprint systems, gain elevated privileges, or even cause a denial of service	Flight Computer, Comm	Transponder Receiver, Encryptor	Command/Telemetry Data, Command Count	Replay, DOS
EX-0001.01	Command Packets	Threat actors may interact with the victim spacecraft by replaying captured commands to the spacecraft. While not necessarily malicious in nature, replayed commands can be used to overload the target spacecraft and cause its onboard systems to crash, perform a DoS attack, or monitor various responses by the spacecraft. If critical commands are captured and replayed, thruster fires, then the impact could impact the spacecraft's attitude control/orbit	Flight computer	Data Bus	Command data, Command count, Data Bus Control Messages	Replay, DOS
EX-0001.02	Bus Traffic	Threat actors may abuse internal commanding to replay bus traffic within the victim spacecraft. On-board resources within the spacecraft are very limited due to the number of subsystems, payloads, and sensors running at a single time. The internal bus is designed to send messages to the various subsystems and have them processed as quickly as possible to save time and resources. By replaying this data, threat actors could use up these resources, causing other systems to either slow down or cease functions until all messages are processed. Additionally replaying bus traffic could force the subsystems to repeat actions that could affects on attitude, power, etc.	Flight computer	Data Bus	Data Buss Messages	Replay, DOS
EX-0002	Position, Navigation, and Timing (PNT) Geofencing	Threat actors may leverage the fact that spacecraft orbit through space unlike typical enterprise systems which are stationary. Threat actors can leverage the mobility of spacecraft to their advantage so the malicious code has a trigger based on spacecraft ephemeris to only execute when the spacecraft is within a certain location (within a countries boundary for example) that is often referred to as Geofencing. By using a Geofence an adversary can ensure that malware is only executed when it is needed. The relative or absolute position of the spacecraft could be combined with some form of timing to serve as the trigger for malware execution	Guidance nav and control ODC, Flight Computer	GPS Receiver	GPS Messages, RTS	Geofencing Attack
EX-0003	Modify Authentication Process	Threat actors may modify the internal authentication process of the victim spacecraft to facilitate initial access, recurring execution, or prevent authorized entities from accessing the spacecraft. This can be done through the modification of the software binaries or memory manipulation techniques	Flight Computer	Encryptor	Authentication Logs	Weak Authentication, Key Exchange
EX-0004	Compromise Boot Memory	Threat actors may manipulate boot memory in order to execute malicious code, bypass internal processes, or DoS the system. This technique can be used to perform other tactics such as Defense Evasion	Flight Computer	Boot Memory	Boot Memory	DoS, Malicious code injection, Boot loader, writable memory
EX-0005	Exploit Hardware/Firmware Corruption	Threat actors can target the underlying hardware and/or firmware using various TTPs that will be dependent on the specific hardware/firmware. Typically, software tools (e.g., antivirus, antimalware, intrusion detection) can protect a system from threat actors attempting to take advantage of those vulnerabilities to inject malicious code. However, there exist security gaps that cannot be closed by the above-mentioned software tools since they are not stationed on software applications, drivers or the operating system but rather on the hardware itself. Hardware components, like memory modules and caches, can be exploited under specific circumstances thus enabling backdoor access to potential threat actors. In addition to hardware, the firmware itself which often is thought to be software in its own right also provides an attack surface for threat actors. Firmware is programming that's written to a hardware device's non-volatile memory where the content is saved when a hardware device is turned off or loses its external power source. Firmware is written directly onto a piece of hardware during manufacturing and it is used to run on the device and can be thought of as the software that enables hardware to run. In the space vehicle context, firmware and Field Programmable Gate Array (FPGA)/Application-Specific Integrated Circuit (ASIC) logic/code is considered equivalent to firmware	Flight Computer, Redundant Flight Computer Memory Storage	Memory Storage	Logs, Software Logs, Memory Registers	supply chain, malicious code injection, writable memory
EX-0006	Disable/Bypass Encryption	Threat actors may perform specific techniques in order to bypass or disable the encryption mechanism onboard the victim spacecraft. By bypassing or disabling this particular mechanism, further tactics can be performed, such as Exfiltration, that may have not been possible with the internal encryption process in place	Comm	Encryptor	Command Data, Encryptor Messages	weak encryption, safe mode exploits, backup channel
EX-0008	Time Synchronized Execution	Threat actors may develop payloads or insert malicious logic to be executed at a specific time	C&DH	Data Bus	Logs	Malicious Code injection, Time Bomb
EX-0008.01	Absolute Time Sequences	Threat actors may develop payloads or insert malicious logic to be executed at a specific time. In the case of Absolute Time Sequences (ATS), the event is triggered at specific date/time - regardless of the state or location of the target	C&DH	Scheduler App	Scheduler Messages and Logs	Time Bomb

ID	Name	Description	Subsystem	Sub-Component	Data Type	Attack Vector
EX-0008.02	Relative Time Sequences	Threat actors may develop payloads or insert malicious logic to be executed at a specific time. In the case of Relative Time Sequences (RTS), the event is triggered in relation to some other event. For example, a specific amount of time after boot	C&DH	Scheduler App	Scheduler Messages and Logs	Time Bomb
EX-0009	Exploit Code Flaws	Threats actors may identify and exploit flaws or weaknesses within the software running on-board the target spacecraft. These attacks may be extremely targeted and tailored to specific coding errors introduced as a result of poor coding practices or they may target known issues in the commercial software components	Flight computer, ADCS, EPS, TCS, Payload, various	Micro Controllers	Code Reviews	non-redundant verification, weak authentication, injection attack
EX-0009.01	Flight Software	Threat actors may abuse known or unknown flight software code flaws in order to further the attack campaign. Some FSW suites contain API functionality for operator interaction. Threat actors may seek to exploit these or abuse a vulnerability/misconfiguration to maliciously execute code or commands. In some cases, these code flaws can perpetuate throughout the victim spacecraft, allowing access to otherwise segmented subsystems	Flight Computer, Payload	N/A	Telemetry Data, Logs	Code Injection
EX-0009.02	Operating System	Threat actors may exploit flaws in the operating system code, which controls the storage, memory management, provides resources to the FSW, and controls the bus. There has been a trend where some modern spacecraft are running Unix-based operating systems and establishing SSH connections for communications between the ground and spacecraft. Threat actors may seek to gain access to command line interfaces and shell environments in these instances. Additionally, most operating systems, including real-time operating systems, include API functionality for operator interaction. Threat actors may seek to exploit these or abuse a vulnerability/misconfiguration to maliciously execute code or commands	Flight Computer	RTOS	unauthenticated connections, command logs	Rouge Ground station, Tampering, supply chain
EX-0010.01	Ransomware	Threat actors may encrypt spacecraft data to interrupt availability and usability. Threat actors can attempt to render stored data inaccessible by encrypting files or data and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key or to render data permanently inaccessible in cases where the key is not saved or transmitted	Flight Computer, Comm	Memory Storage	N/A	Ransomware
EX-0010.02	Wiper Malware	Threat actors may deploy wiper malware, which is a type of malicious software designed to destroy data or render it unusable. Wiper malware can spread through various means, software vulnerabilities (CWE/CVE), or by exploiting weak or stolen credentials.	Flight Computer	Memory Storage	N/A	Weak Authentication, Code injection, Wiper Malware
EX-0010.03	Rootkit	Rootkits are programs that hide the existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. Rootkits or rootkit enabling functionality may reside at the flight software or kernel level in the operating system or lower, to include a hypervisor, Master Boot Record, or System Firmware	Flight Computer RTOS	Root of Trust Software/Hardware, Boot loader	N/A	Rootkit
EX-0010.04	Bootkit	Adversaries may use bootkits to persist on systems and evade detection. Bootkits reside at a layer below the operating system and may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly	Flight Computer RTOS	Root of Trust Software/Hardware, Boot loader	N/A	Bootkit
EX-0012	Modify On-Board Values	Threat actors may perform specific commands in order to modify onboard values that the victim spacecraft relies on. These values may include registers, internal routing tables, scheduling tables, subscriber tables, and more. Depending on how the values have been modified, the victim spacecraft may no longer be able to function	Flight Computer, Various	Various	N/A	Spoofing
EX-0012.01	Registers	Threat actors may target the internal registers of the victim spacecraft in order to modify specific values as the FSW is functioning or prevent certain subsystems from working. Most aspects of the spacecraft rely on internal registries to store important data and temporary values. By modifying these registries at certain points in time, threat actors can disrupt the workflow of the subsystems or onboard payload, causing them to malfunction or behave in an undesired manner	Flight Computer	Flight Software	Check sums or hash values, Data Tables	DOS
EX-0012.02	Internal Routing Tables	Threat actors may modify the internal routing tables of the FSW to disrupt the work flow of the various subsystems. Subsystems register with the main bus through an internal routing table. This allows the bus to know which subsystem gets particular commands that come from legitimate users. By targeting this table, threat actors could potentially cause commands to not be processed by the desired subsystem	Flight Computer	Flight Software	check sums or hash values, Data Tables	DOS
EX-0012.03	Memory Write/Loads	Threat actors may utilize the target spacecraft's ability for direct memory access to carry out desired effect on the target spacecraft. Spacecraft often have the ability to take direct loads or singular commands to read/write to/from memory directly. Spacecraft that contain the ability to input data directly into memory provides a multitude of potential attack scenarios for a threat actor. Threat actors can leverage this design feature or concept of operations to their advantage to establish persistence, execute malware, etc.	Flight Computer	Flight Software	check sums or hash values, Data Tables	DOS
EX-0012.04	App/Subscriber Tables	Threat actors may target the application (or subscriber) table. Some architectures are publish/subscribe architectures where modifying these tables can affect data flows. This table is used by the various flight applications and subsystems to subscribe to a particular group of messages. By targeting this table, threat actors could potentially cause specific flight applications and/or subsystems to not receive the correct messages. In legacy MIL-STD-1553 implementations modifying the remote terminal configurations would fall under this sub-technique as well	Flight Computer	Flight Software	Check sums or hash values, Data Tables	DOS

ID	Name	Description	Subsystem	Sub-Component	Data Type	Attack Vector
EX-0012.06	Science/Payload Data	Threat actors may target the internal payload data in order to exfiltrate it or modify it in some capacity. Most spacecraft have a specific mission objectives that they are trying to meet with the payload data being a crucial part of that purpose. When a threat actor targets this data, the victim spacecraft's mission objectives could be put into jeopardy	Payload	Processing Algorithms, storage memory	data stream	DOS, Data Poisoning
EX-0012.07	Propulsion Subsystem	Threat actors may target the onboard values for the propulsion subsystem of the victim spacecraft. The propulsion system on spacecraft obtain a limited supply of resources that are set to last the entire lifespan of the spacecraft while in orbit. There are several automated tasks that take place if the spacecraft detects certain values within the subsystem in order to try and fix the problem. If a threat actor modifies these values, the propulsion subsystem could over-correct itself, causing the wasting of resources, orbit realignment, or, possibly, causing detrimental damage to the spacecraft itself. This could cause damage to the purpose of the spacecraft and shorten its lifespan	Propulsion System	Carious	Hash check for Configurations	DOS, Degradations
EX-0012.08	Attitude Determination and Control Subsystem	Threat actors may target the onboard values for the Attitude Determination and Control subsystem of the victim spacecraft. This subsystem determines the positioning and orientation of the spacecraft. Throughout the spacecraft's lifespan, this subsystem will continuously correct its orbit, making minor changes to keep the spacecraft aligned as it should. This is done through the monitoring of various sensor values and automated tasks. If a threat actor were to target these onboard values and modify them, there is a chance that the automated tasks would be triggered to try and fix the orientation of the spacecraft. This can cause the wasting of resources and, possibly, the loss of the spacecraft, depending on the values changed	ADCS	Various	Hash check for Configurations	DOS
EX-0012.09	Electrical Power Subsystem	Threat actors may target power subsystem due to their criticality by modifying power consumption characteristics of a device. Power is not infinite on-board the spacecraft, and if a threat actor were to manipulate values that cause rapid power depletion it could affect the spacecraft's ability to maintain the required power to perform mission objectives	EPS	Various	Hash check for Configurations	DOS
EX-0012.10	Command and Data Handling Subsystem	Threat actors may target the onboard values for the Command and Data Handling Subsystem of the victim spacecraft. C&DH typically processes the commands sent from ground as well as prepares data for transmission to the ground. Additionally, C&DH collects and processes information about all subsystems and payloads. Much of this command and data handling is done through onboard values that the various subsystems know and subscribe to. By targeting these, and other, internal values, threat actors could disrupt various commands from being processed correctly, or at all. Further, messages between subsystems would also be affected, meaning that there would either be a delay or lack of communications required for the spacecraft to function correctly	C&DH	Various, Payload	Hash Check	DOS
EX-0012.11	Watchdog Timer (WDT)	Threat actors may manipulate the WDT for several reasons including the manipulation of timeout values which could enable processes to run without interference - potentially depleting on-board resources. For spacecraft, WDTs can be either software or hardware. While software is easier to manipulate there are instances where hardware-based WDTs can also be attacked/modified by a threat actor	Flight Computer	WDT	Hash check for Configurations, WDT reset task suspended	DOS
EX-0012.12	System Clock	An adversary conducting a cyber attack may be interested in altering the system clock for a variety of reasons, such as forcing execution of stored commands in an incorrect order	Flight Computer	System Clock	Changes to system clock configuration, time intervals	DOS
EX-0012.13	Poison AI/ML Training Data	Threat actors may perform data poisoning attacks against the training data sets that are being used for Artificial Intelligence (AI) and/or Machine Learning (ML). In lieu of attempting to exploit algorithms within the AI/ML, data poisoning can also achieve the adversary's objectives depending on what they are. Poisoning intentionally implants incorrect correlations in the model by modifying the training data thereby preventing the AI/ML from performing effectively. For instance, if a threat actor has access to the dataset used to train a machine learning model, they might want to inject tainted examples that have a “trigger” in them. With the datasets typically used for AI/ML (i.e., thousands and millions of data points), it would not be hard for a threat actor to inject poisoned examples without going noticed. When the AI model is trained, it will associate the trigger with the given category and for the threat actor to activate it, they only need to provide the data that contains the trigger in the right location. In effect, this means that the threat actor has gained backdoor access to the machine learning model	Flight Computer	Various	Audit log for AI/ML, Training data drift	data poisoning
EX-0013	Flooding	Threat actors use flooding attacks to disrupt communications by injecting unexpected noise or messages into a transmission channel. There are several types of attacks that are consistent with this method of exploitation, and they can produce various outcomes. Although, the most prominent of the impacts are denial of service or data corruption. Several elements of the space vehicle may be targeted by jamming and flooding attacks, and depending on the time of the attack, it can have devastating results to the availability of the system	Comm, Flight Computer	Data Bus, RF link	Message frequency, packet loss, signal parameters, SNR	DOS
EX-0013.01	Valid Commands	Threat actors may utilize valid commanding as a mechanism for flooding as the processing of these valid commands could expend valuable resources like processing power and battery usage. Flooding the spacecraft bus, sub-systems or link layer with valid commands can create temporary denial of service conditions for the space vehicle while the spacecraft is consumed with processing these valid commands	Comm, Flight Computer	Data Bus, RF link	Message frequency, packet loss, signal parameters, SNR, high priority commands	DOS

ID	Name	Description	Subsystem	Sub-Component	Data Type	Attack Vector
EX-0013.02	Erroneous Input	Threat actors inject noise/data/signals into the target channel so that legitimate messages cannot be correctly processed due to impacts to integrity or availability. Additionally, while this technique does not utilize system-relevant signals/commands/information, the target spacecraft may still consume valuable computing resources to process and discard the signal	Comm, Flight Computer	Data Bus, RF link	Message frequency, packet loss, signal parameters, SNR	DOS
EX-0014.01	Time Spoof	Threat actors may attempt to target the internal timers onboard the victim spacecraft and spoof their data. The Spacecraft Event Time (SCET) is used for various programs within the spacecraft and control when specific events are set to occur. Ground controllers use these timed events to perform automated processes as the spacecraft is in orbit in order for it to fulfill its purpose. Threat actors that target this particular system and attempt to spoof its data could cause these processes to trigger early or late	GNC	GPS Radio	GPS Time intervals	Spoofing
EX-0014.02	Bus Traffic	Threat actors may attempt to target the main or secondary bus onboard the victim spacecraft and spoof their data. The spacecraft bus often directly processes and sends messages from the ground controllers to the various subsystems within the spacecraft and between the subsystems themselves. If a threat actor would target this system and spoof it internally, the subsystems would take the spoofed information as legitimate and process it as normal. This could lead to undesired effects taking place that could damage the spacecraft's subsystems, hosted payload, and critical data	Flight Computer	Data Bus	Various	Spoofing
EX-0014.03	Sensor Data	Threat actors may target sensor data on the space vehicle to achieve their attack objectives. Sensor data is typically inherently trusted by the space vehicle therefore an attractive target for a threat actor. Spoofing the sensor data could affect the calculations and disrupt portions of a control loop as well as create uncertainty within the mission thereby creating temporary denial of service conditions for the mission. Affecting the integrity of the sensor data can have varying impacts on the space vehicle depending on decisions being made by the space vehicle using the sensor data. For example, spoofing data related to attitude control could adversely impact the space vehicle's ability to maintain orbit	Payload	Various	Various	Spoofing, DOS
EX-0014.04	Position, Navigation, and Timing (PNT)	Threat actors may attempt to spoof Global Navigation Satellite Systems (GNSS) signals (i.e., GPS, Galileo, etc.) to disrupt or produce some desired effect with regard to a spacecraft's position, navigation, and/or timing (PNT) functions	GNC	GPS Radio	Attitude Control readings, time intervals	Spoofing, DOS
EX-0016	Jamming	Threat actors may attempt to jam Global Navigation Satellite Systems (GNSS) signals (i.e., GPS, Galileo, etc.) to inhibit a spacecraft's position, navigation, and/or timing functions	OBC, GNC	GPS Radio	Signal Power levels	Jamming, DOS
EX-0016.01	Uplink Jamming	An uplink jammer is used to interfere with signals going up to a satellite by creating enough noise that the satellite cannot distinguish between the real signal and the noise. Uplink jamming of the control link, for example, can prevent satellite operators from sending commands to a satellite. However, because the uplink jammer must be within the field of view of the antenna on the satellite receiving the command link, the jammer must be physically located within the vicinity of the command station on the ground https://aerospace.csis.org/aerospace101/counterspace-weapons-101	Comm	SDR	SNR	Jamming, DOS
EX-0016.03	Position, Navigation, and Timing (PNT)	Threat actors may attempt to jam Global Navigation Satellite Systems (GNSS) signals (i.e., GPS, Galileo, etc.) to inhibit a spacecraft's position, navigation, and/or timing functions	OBC, GNC	GPS Radio	Signal Power levels	Jamming, DOS
PER-0001	Memory Compromise	Threat actors may manipulate memory (boot, RAM, etc.) in order for their malicious code and/or commands to remain on the victim spacecraft. The spacecraft may have mechanisms that allow for the automatic running of programs on system reboot, entering or returning to/from safe mode, or during specific events. Threat actors may target these specific memory locations in order to store their malicious code or file, ensuring that the attack remains on the system even after a reset	Flight Computer, Payload	Memory Storage	Audit logs, hash check, checksums	Boot loader, Memory compromise
PER-0002	Backdoor	Threat actors may find and target various backdoors, or inject their own, within the victim spacecraft in the hopes of maintaining their attack	Flight Computer, Payload	Memory Storage	Authentication attempts, login audits, command data	Backdoor, RAT
PER-0004	Replace Cryptographic Keys	Threat actors may attempt to fully replace the cryptographic keys on the space vehicle which could lockout the mission operators and enable the threat actor's communication channel. Once the encryption key is changed on the space vehicle, the spacecraft is rendered inoperable from the operators perspective as they have lost commanding access. Threat actors may exploit weaknesses in the key management strategy. For example, the threat actor may exploit the over-the-air rekeying procedures to inject their own cryptographic keys	Comm	Encryptor	Checksum, Hash Check, Command data	Crypto key spoof/theft
DE-0001	Disable Fault Management	Threat actors may disable fault management within the victim spacecraft during the attack campaign. During the development process, many fault management mechanisms are added to the various parts of the spacecraft in order to protect it from a variety of bad/corrupted commands, invalid sensor data, and more. By disabling these mechanisms, threat actors may be able to have commands processed that would not normally be allowed	Flight Computer	FMS	Command Data	Malicious Commanding
DE-0002	Prevent Downlink	Threat actors may target the downlink connections to prevent the victim spacecraft from sending telemetry to the ground controllers. Telemetry is the only method in which ground controllers can monitor the health and stability of the spacecraft while in orbit. By disabling this downlink, threat actors may be able to stop mitigations from taking place	Comm	N/A	Command Data	DOS

ID	Name	Description	Subsystem	Sub-Component	Data Type	Attack Vector
DE-0002.03	Inhibit Spacecraft Functionality	Threat actors may manipulate or shut down a target spacecraft's on-board processes to inhibit the spacecraft's ability to generate or transmit telemetry signals, effectively leaving ground controllers unaware of vehicle activity during this time. Telemetry is the only method in which ground controllers can monitor the health and stability of the spacecraft while in orbit. By disabling this downlink, threat actors may be able to stop mitigations from taking place	Comm	N/A	Command Data	DOS
DE-0004	Masquerading	Threat actors may gain access to a victim spacecraft by masquerading as an authorized entity. This can be done several ways, including through the manipulation of command headers, spoofing locations, or even leveraging Insider's access (i.e., Insider Threat)	Flight Computer, Comm	N/A	Authentication and authorization logs	Masquerading, insider threat
DE-0006	Modify Whitelist	Threat actors may target whitelists on the space vehicles as a means to execute and/or hide malicious processes/programs. Whitelisting is a common technique used on traditional IT systems but has also been used on space vehicles. Whitelisting is used to prevent execution of unknown or potentially malicious software. However, this technique can be bypassed if not implemented correctly but threat actors may also simply attempt to modify the whitelist outright to ensure their malicious software will operate on the space vehicle that utilizes whitelisting	Flight Computer, Comm	N/A	Authentication and authorization logs	Whitelist manipulation
DE-0010	Overflow Audit Log	Threat actors may seek to exploit the inherent nature of flight software and its limited capacity for event logging/storage between downlink windows as a means to conceal malicious activity	Flight Computer	Persistent memory	Audit log buffer, log retention	buffer overflow
LM-0001	Hosted Payload	Threat actors may use the hosted payload within the victim spacecraft in order to gain access to other subsystems. The hosted payload often has a need to gather and send data to the internal subsystems, depending on its purpose. Threat actors may be able to take advantage of this communication in order to laterally move to the other subsystems and have commands be processed	Payload	N/A	Authentication and authorization logs, access requests	Malicious code injection
LM-0002	Exploit Lack of Bus Segregation	Threat actors may exploit victim spacecraft on-board flat architecture for lateral movement purposes. Depending on implementation decisions, spacecraft can have a completely flat architecture where remote terminals, sub-systems, payloads, etc., can all communicate on the same main bus without any segmentation, authentication, etc. Threat actors can leverage this poor design to send specially crafted data from one compromised devices or sub-system. This could enable the threat actor to laterally move to another area of the spacecraft or escalate privileges (i.e., bus master, bus controller)	Flight Computer, C&DH	Data Bus	sender and receiver headers, abnormal communication onboard Spacecraft	Priv esc, DOS
LM-0003	Constellation Hopping via Crosslink	Threat actors may attempt to command another neighboring spacecraft via crosslink. spacecraft in close proximity are often able to send commands back and forth. Threat actors may be able to leverage this access to compromise another spacecraft	Comm	Crosslink	Crosslink logs, Authentication and authorization logs	Lateral movement, Priv Esc
LM-0004	Visiting Vehicle Interface(s)	Threat actors may move from one spacecraft to another through visiting vehicle interfaces. When a vehicle docks with a spacecraft, many programs are automatically triggered in order to ensure docking mechanisms are locked. This entails several data points and commands being sent to and from the spacecraft and the visiting vehicle. If a threat actor were to compromise a visiting vehicle, they could target these specific programs in order to send malicious commands to the victim spacecraft once docked	Structs and mechs, Flight Computer	Docking Mechanism	Request logs, Authentication and authorization logs	physical
LM-0005	Virtualization Escape	In virtualized environments, threat actors can use the open ports between the partitions to overcome the hypervisor's protection and damage another partition. Further, if the threat actor has compromised the payload, access to a critical partition can be gained through ports allowed by hypervisor	Flight Computer	Virtual Payload	Virtual Payload Audit logging, port monitoring, request logs	VM Hopping
EXF-0004	Out-of-Band Communications Link	Threat actors may attempt to exfiltrate data via the out-of-band communication channels. While performing eavesdropping on the primary/second uplinks and downlinks is a method for exfiltration, some space vehicles leverage out-of-band communication links to perform actions on the space vehicle (i.e., re-keying). These out-of-band links would occur on completely different channels/frequencies and often operate on separate hardware on the space vehicle. Typically these out-of-band links have limited built-for-purpose functionality and likely do not present an initial access vector but they do provide ample exfiltration opportunity	Comm	N/A	Out of band activation, alarms	Eavesdropping
EXF-0006	Modify Communications Configuration	Threat actors can manipulate communications equipment, modifying the existing software, hardware, or the transponder configuration to exfiltrate data via unintentional channels the mission has no control over	Comm, Flight Computer	SDR, Transceiver	Command data	Malicious file manipulation
EXF-0006.01	Software Defined Radio	Threat actors may target software defined radios due to their software nature to setup exfiltration channels. Since SDRs are programmable, when combined with supply chain or development environment attacks, SDRs provide a pathway to setup covert exfiltration channels for a threat actor	Comm	SDR	Command data, configuration changes, registers, checksum	malicious configuration changes
EXF-0006.02	Transponder	Threat actors may change the transponder configuration to exfiltrate data via radio access to an attacker-controlled asset	Comm	Transponder	Command data, configuration changes, registers	malicious configuration changes
EXF-0010	Payload Communication Channel	Threat actors can deploy malicious software on the payload(s) which can send data through the payload channel. Payloads often have their own communication channels outside of the main TT&C pathway which presents an opportunity for exfiltration of payload data or other spacecraft data depending on the interface and data exchange	Payload	Payload Comm System	Authentication requests	Malicious code injection

ID	Name	Description	Subsystem	Sub-Component	Data Type	Attack Vector
IMP-0001	Deception (or Misdirection)	Measures designed to mislead an adversary by manipulation, distortion, or falsification of evidence or information into a system to induce the adversary to react in a manner prejudicial to their interests. Threat actors may seek to deceive mission stakeholders (or even military decision makers) for a multitude of reasons. Telemetry values could be modified, attacks could be designed to intentionally mimic another threat actor's TTPs, and even allied ground infrastructure could be compromised and used as the source of communications to the spacecraft	Flight Computer	FMS	Special modes, audit logs, FMS logging	Spoofing
IMP-0002	Disruption	Measures designed to temporarily impair the use or access to a system for a period of time. Threat actors may seek to disrupt communications from the victim spacecraft to the ground controllers or other interested parties. By disrupting communications during critical times, there is the potential impact of data being lost or critical actions not being performed. This could cause the spacecraft's purpose to be put into jeopardy depending on what communications were lost during the disruption. This behavior is different than Denial as this attack can also attempt to modify the data and messages as they are passed as a way to disrupt communications	Comm	N/A	Audit logs	DOS
IMP-0003	Denial	Measures designed to temporarily eliminate the use, access, or operation of a system for a period of time, usually without physical damage to the affected system. Threat actors may seek to deny ground controllers and other interested parties access to the victim spacecraft. This would be done exhausting system resource, degrading subsystems, or blocking communications entirely. This behavior is different from Disruption as this seeks to deny communications entirely, rather than stop them for a length of time	Comm, Flight Computer, FMS	N/A	Audit logs	DOS

Title	Comment	Link
SPARTA	Space Attack Research & Tactic Analysis (SPARTA)	https://sparta.aerospace.org/
SPARTA Resources	Papers/Articles/Blogs/Podcasts/Presentations	https://sparta.aerospace.org/resources/
Thermal Control	Listing of Passive and Active Systems	https://www.nasa.gov/smallsat-institute/sst-soa/thermal-control/
Application of Zero Trust Architecture to Spacecraft	Proprietary White Paper	Stephenson Stellar.pdf. (n.d.).
NIST Security and Privacy Controls for Information Systems and Organizations	NIST-800-53r5	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Version	Short Title	Description	Tab/Cell Reference
Distro_A-v1	Original Matrix	Original Public Release version of Space Vehicle Logging Best Practice Guideline (BPG) Matrix and associated White Paper	< All >