CFS SC Requirements

Code 582
Flight Software Systems Branch

Dec 18, 2014

ID	Summary
4491	CFS SC Requirements Document Version 1.5

SR_Contains:

ID	ReqID	Text	Rationale	Heritage_Reference
4493		# CFS Stored Command (SC) Requirements # 1.0 Introduction ## 1.1 Document Purpose The Core Flight Software System (CFS) Stored Command (SC) Application will be developed by the Flight Software Branch (FSB) of the Software Engineering Division (SED). The purpose of this requirements specification is to define the requirements to be satisfied by the Stored Command Application. This application is developed for re-use. For this reason, several nomenclatures are used in this document to identify configurations for a mission. The CFS is specified as a multi-platform product. Mission-specific features and customization requirements which are applicable for all platforms are tagged with <MISSION_DEFINED>. Platform-specific features and customizations requirements are tagged with either "<PLATFORM_DEFINED>" or "<OPTIONAL>." Additional nomenclature is used along with the tag to specify a CFS default value for the platform-specific feature: "<PLATFORM_DEFINED, Default_Value>". Reference platforms (single processor and multi-processor architectures) are defined to supply the default CFS application configuration. These configurations define the "maximum" CFS Application deployments such that any refined deployment is a subset of a reference platform. ## 1.2 Document Scope The scope of this document is limited to the specification of requirements for the Stored Command Software. These include functional, performance, qualification, and design requirements. ## 1.3 Document Organization This document is organized into three additional sections and several appendices. Section 2 gives the Stored Command context. Section 3 documents the Stored Command system design decisions and constraints. Section 4 contains the Stored Command functional and performance requirements. Appendix A contains a list of abbreviations and acronyms used in this document.		

1.4 Relevant Documents

1.4.1 Parent Documents

None

1.4.2 Reference Documents

1. Operating System Abstraction Layer (OSAL) Library
2. cFE Application Developer's Guide 582-2007-001
3. cFE User's Guide

2.0 CFS Stored Command Application Context

The Stored Command (SC) application provides a spacecraft with the ability to be commanded 24 hours a day using sequences of commands that are loaded via tables from the ground and stored for later execution. Each stored command has a time tag associated with it, permitting the command to be released for distribution at predetermined times.

The Flight Software supports both Absolute Time tagged command Sequences (ATSs), as well as multiple Relative Time tagged command Sequences (RTSs). ATSs are command sequences timed to execute at some absolute point in time. RTSs are command sequences which execute at some point in time, relative to the previous command in the relative time command sequence. Time for both the ATSs and RTSs is resolved to one second. The Flight Software will provide operators the ability to load examine and change command sequences.

Figure 1.0 shows the context diagram for the CFS Stored Command (SC) Application. The Scheduler Application (SCH) sends periodic commands to SC as defined in the SCH Schedule Table in order to wakeup the SC application such that it can process the Absolute Time Sequence (ATS) and Relative Time Sequence (RTS) tables. In addition, SCH generates a request for SC's housekeeping message. Ground commands come from the Command Ingest task (CI). Messages are routed to SC by the cFE SB Application. SC learns of ground updates to the SC tables through the cFE Table Services application. Messages generated by SC are routed to Housekeeping (HK), TO and Data Store (DS) (as long as the applications subscribe to them). Commands sent from the SC application are sent to all applications

Time is a critical element of the SC Application. For Absolute Time Sequence commands, there is a field in the command that represents the absolute time, in seconds, that each command will execute; For Relative Time Command Sequence Commands there is a field that represents the time in seconds that the command will delay before executing. This time is relative to the time when the previous Relative Time Tagged Command was executed (or in the case of the first command of the sequence, the time when the sequence was started.).

The time used by the SC Application is either UTC or TAI. A configuration parameter specifies the desired setting.

Stored Command Application contains tables in support of ATSs and RTSs:

1. ATS Tables – 2 tables which define the absolute time sequence commands
2. ATS Status Tables – dump only tables used to report ATS status for both of the ATS tables
3. RTS Tables – defines the relative time sequence commands. There are separate tables for each relative time sequence
4. RTS Status Tables – dump only tables used to report the RTS status for all of the RTSs

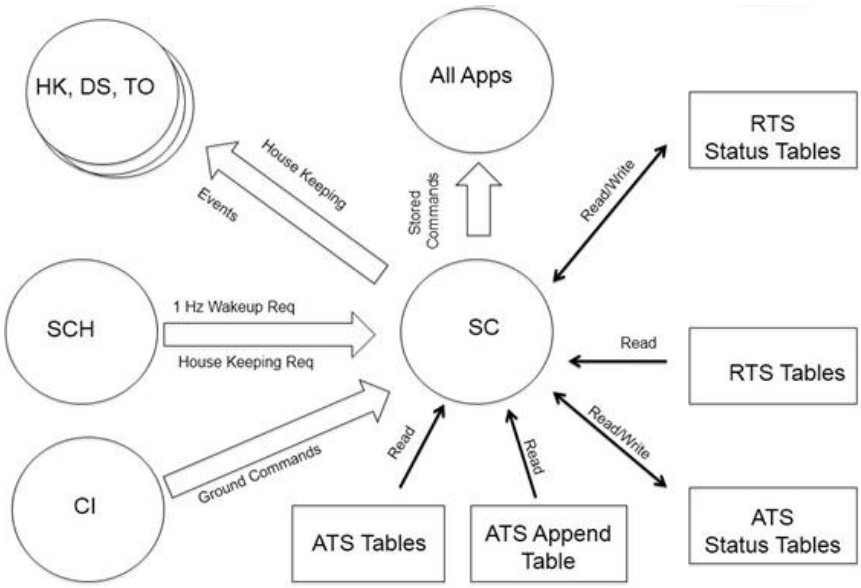

Figure 1.0 – CFS SC Context

2.1 Assumptions

The following list summarizes the assumptions made by the CFS Stored Command Application:

· cFE API and OSAL are being used

· A command is sent to SC to schedule the application to wakeup at a 1Hz rate. This is required as the resolution of the commands is one second.

3.0 Design Specifications

The Stored Command Application's requirements and design are based on the results of the CFS heritage analysis effort, however, since LRO did not deviate much from previous missions such as SDO and ST-5, no formal heritage analysis was done.

3.1 Design Constraints

The design of SC is not tied to the Consultative Committee on Space Data Systems (CCSDS) protocol. SC should, wherever possible, use the APIs that provide access to the parts of the command that are required instead of using CCSDS specific references (see cFE SB APIs).

4.0 Subsystem Requirements

4621	CFS-600	The FSW shall provide a stored command capability to receive, store, and execute sequences of commands.	Missions need the ability to provide unattended spacecraft commanding.	LRO, SDO
4623	CFS-601	The FSW shall provide 2 absolute time sequence (ATS) command tables with an accuracy of 1 second command execution relative to spacecraft time.	A time granularity of one second is sufficient for absolute time command sequences to support the management of spacecraft operations. Two tables are necessary to facilitate efficient spacecraft operation; one table may be loaded while the other is being used.	LRO, SDO
4625	CFS-602	The FSW shall provide an ATS command table capability of at least <PLATFORM_DEFINED> commands totaling <PLATFORM_DEFINED> bytes.		LRO, SDO
4627	CFS-603	The FSW shall provide the capability to execute relative time sequences (RTSs) of commands with an accuracy of 1 second command execution relative to the previous command in the sequence.	A time granularity of one second is sufficient for fault management responses and the 1 second period virtually guarantees the sequential execution of commands.	LRO, SDO
4631	CFS-604	The FSW shall provide <PLATFORM_DEFINED> RTS command tables, each with a size of at least <PLATFORM_DEFINED> bytes.		LRO, SDO
4633	CFS-605	The FSW shall verify the integrity of each stored command before distribution.	Stored commands may be resident in memory for long periods of time. Verification will prevent corrupted commands from being distributed.	LRO, SDO
4635		**5.0 Detailed Requirements**		

		5.1 Basic Requirements The following requirements are basic requirements of Stored Command. Some of them are included here to avoid repeating these requirements for each applicable requirement.		
4495	SC1000	Upon receipt of a No-Op command, SC shall increment the SC Valid Command Counter and generate an event message.	Debug command to verify application is alive.	LRO
4497	SC1001	Upon receipt of a Reset command, SC shall reset the following housekeeping variables to a value of zero: a) Valid Command Counter b) Command Rejected Counter c) ATS Command Counter d) ATS Command Error Counter e) RTS Command Counter f) RTS Command Error Counter g) Number of RTS Started Counter h) Number of RTS Started Error Counter	Important for testing and on-orbit flight operations in order to start with a "clean slate."	LRO, SDO
4499	SC1002	For all SC commands, if the length contained in the message header is not equal to the expected length, SC shall reject the command and issue an event message.	Basic command verification in the event of SEU or memory corruption.	LRO, SDO
4501	SC1004	If SC accepts any command as valid, SC shall execute the command, increment the SC Valid Command Counter and issue an event message.	Operators require feedback on command execution. Note that this only applies to "ground commands" (i.e. does not include requests that come from the scheduler).	LRO, SDO
4503	SC1005	If SC rejects any command, SC shall abort the command execution, increment the SC Command Rejected Counter and issue an error event message.	Operators require feedback on command execution. Note that this only applies to "ground commands" (i.e. does not include requests that come from the scheduler).	LRO, SDO
4637		**5.2 ATS/RTS - General** The following are the requirements, mainly sizing and performance requirements related to ATSs and RTSs.		

4505	SC2000	SC shall define <PLATFORM_DEFINED> bytes of storage for each of two (2) Absolute Time-tagged command Sequence (ATS) tables.	One table will be used for uploads, while the other is executing.	LRO, SDO
4507	SC2000.1	SC shall resolve time to 1 second for Absolute Time Command Sequences (ATS).	Heritage missions have shown that this is adequate resolution.	LRO, SDO
4509	SC2000.2	SC shall accept a maximum of <PLATFORM_DEFINED> commands per ATS.	Required in order to bound the command number.	LRO, SDO
4511	SC2000.3	SC shall accept a variable number of variable length commands from each ATS. Each ATS command shall contain: a) A command number b) A time tag denoting the time at which to execute the command c) A variable length command	Note: The time format is a cFE configuration parameter which allows for either UTC time or TAI time.	LRO, SDO
4652	SC2000.4	SC shall use the <PLATFORM_DEFINED> time format (UTC or TAI).	Provides flexibility on time format. Note that on SDO, TAI was used to telemetry packets, however, UTC was used for SC.	New
4513	SC2001	Upon receipt of a table update indication for an ATS Table, SC shall validate the following for the ATS table: a) Duplicate command numbers b) Invalid command lengths c) Commands that run off of the end of the table d) Command number	SC application needs to validate the table to ensure gross errors are caught. Note that cFE Table Services handles the ground interface to tables. Note: A command that runs off the end of the table indicates a partial command.	LRO, SDO
4515	SC2002	SC shall allocate <PLATFORM_DEFINED> Relative Time-tagged Sequences (RTSs) with each capable of storing <PLATFORM_DEFINED> bytes of stored command data.	Specifies the limits for table sizing purposes.	LRO, SDO
4517	SC2002.1	SC shall resolve time to 1 second for Relative Time Command Sequences (RTS).	Heritage missions have shown that this is adequate	LRO, SDO

			resolution.	
4519	SC2002.2	SC shall accept variable length packed RTS commands within the <PLATFORM_DEFINED> byte relative time-tagged sequences.		LRO, SDO
4521	SC2002.3	Each individual command within the sequence shall consist of: a) Time tag with a one second resolution b) A variable length command, with a maximum length of <PLATFORM_DEFINED> bytes	Each command within an RTS needs to contain a time with a one second resolution.	LRO, SDO
4523	SC2003	Upon receipt of a table update indication for an RTS Table, SC shall set the RTS status to DISABLED.	Since the RTS definition table does not include a default state, safer to assume disabled.	LRO
4525	SC2004	SC shall execute commands in the ATS table in ascending order, based upon the time-tag of the commands, regardless of the order in which the commands are stored in the ATS table.	Allows flexibility in ground system tools and load generation (command location within an ATS doesn't matter; Time matters).	LRO, SDO
4527	SC2005	SC shall execute no more than <PLATFORM_DEFINED> commands per second from all currently executing RTS tables and/or ATS tables.	Provides bounds on SC processing.	LRO, SDO
4529	SC2005.1	SC shall defer execution of pending RTS commands, when the combined execution count, of ATS and RTS, exceeds the command per second limit. Note: RTS commands that are deferred may take priority over ATS commands that are scheduled to execute in the next second.	ATS that are scheduled to execute in the same second as RTSs are executed first (get higher priority). Any RTSs that are not executed in the current second are executed in the next second.	
4531	SC2005.2	SC shall allow up to the maximum number of defined RTSs to be active concurrently.	RTSs can run concurrently. The limitation is the number of commands that can be sent in one second.	LRO, SDO
4533	SC2006	SC shall execute the RTSs in priority order based on the RTS number where RTS #1 has the highest priority.	Provides a known order to the processing of RTSs so that missions can organize the RTSs	LRO, SDO

			appropriately. Note that RTS numbers start at 1.	
11890	SC2007	SC shall define <PLATFORM_DEFINED> bytes of storage for an ATS Append Table.		
11892	SC2007.1	The ATS Append Table format is the same as the ATS tables		
11894	SC2008	Upon receipt of an Apply ATS Append Table command SC shall append the ATS Append Table contents to the command-specified ATS table.		
11896	SC2008.1	The Append command may be performed on either ATS table.		
11898	SC2008.2	If the number of entries in the ATS and ATS Append Table exceeds the size of the ATS table SC shall reject the Apply ATS Append Table command.		
11900	SC2008.3	The Apply ATS Append Table command shall add all ATS Append Table data to the end of the command-specified ATS table.		
11902	Sc2008.4	The Apply ATS Append Table command shall provide the ability to add new commands to the ATS buffer		
11904	Sc2008.5	The Apply ATS Append Table command shall provide the ability to modify existing commands in the ATS buffer		
11906	SC2008.6	Upon completion of the Apply ATS Append Table Command, SC shall issue an info event message indicating the number of commands that were appended to the ATS.		
11908	Sc2008.7	Upon completion of the Apply ATS Append Table Command, SC shall recompute the command execution sequence.		
11910	SC2009	Upon receipt of a table update indication for an ATS Append Table, SC shall validate the following for the ATS table: a) Duplicate command numbers b) Invalid command lengths c) Commands that run off the end of the table d) Command number		
4639		## 5.3 ATS Processing The following requirements relate to the Absolute Time Sequence processing. There are 2 ATS tables provided so that one can be executing while the other is being loaded. Commands are provided in order to start, stop, switch between the ATSs and jump to another location within a currently executing ATS.		
4535	SC3000	Upon receipt of a Start ATS command, SC shall start the command-specified ATS provided all of the following conditions are satisfied: a) The command-specified ATS table identification is valid b) The ATS table contains at least one command c) Neither of the two ATS tables is currently executing		
4537	SC3000.1	SC shall mark all ATS commands with time less-than the current time as SKIPPED and an event message shall be generated.	Don't want to process commands that are tagged with times from the past since there are absolute timed commands. Provides the ground knowledge of which commands were not processed (skipped).	LRO, SDO

4543	SC3000.3	Prior to the dispatch of each individual ATS command, SC shall verify the Data Integrity Check Value of the stored command.	Provides verification that the ATS is not corrupted or the commands are not malformed. The Data Integrity Check algorithm is specified in the cFE.	LRO, SDO
4545	SC3000.3.1	For any ATS command which fails the Data Integrity Check Value, the following shall be performed: a) Discard the command b) Mark the command with DATA INTEGRITY CHECK VALUE VERIFICATION FAILED c) Issue an event message	Ground needs to know if any commands weren't executed.	LRO
4547	SC3000.3.2	If the Continuation Execution of ATS On Error Flag is Disabled, SC shall terminate the execution of the ATS.	Provides ground the ability to abort the ATS execution in the event of a data integrity failure.	LROS
4549	SC3001	Upon receipt of a Stop ATS Command, SC shall a) Stop processing the currently executing ATS b) Set the state of that ATS to IDLE	Note that the Stop ATS can be contained in the ATS.	LRO, SDO
4551	SC3001.1	If no ATS is executing, SC shall increment the Valid Command Counter.		LRO, SDO
4553	SC3002	Upon receipt of a Switch ATS Command, SC shall a) Terminate the processing of the current ATS table after processing all of the commands within the current second b) Start processing of the alternate ATS table	Allows the ground to chain ATS tables.	LRO, SDO
4555	SC3002.1	SC shall begin processing the first ATS command after the next 1 second occurs containing a time which is greater-than-or-equal-to the current time.	Allows ATS tables to overlap each other so that the ground can switch at anytime. Need to wait until the next second occurs to ensure that the overlapping in ATSs doesn't cause the same commands to be executed twice.	LRO, SDO
4557	SC3002.2	SC shall mark all ATS commands with time less-than the current time as SKIPPED and an event message shall be generated.	Provides the ground knowledge of which commands were not processed (skipped).	
4559	SC3002.3	If the alternate ATS table has not been loaded, SC shall reject the command.	Shouldn't	LRO, SDO

			switch to an invalid ATS.	
4561	SC3002.4	If the Switch command is located within an ATS, SC shall immediately execute the switch command.	A switch command located within an ATS is handled differently than from the ground. If from the ground, must wait until next second to prevent overlapping of 2 ATS from duplicating commands.	LRO
4563	SC3003	Upon receipt of a Jump Command, SC shall transfer execution to the command within the currently executing ATS table whose time-tag is equal to a command-specified time value.	Does it finish executing the current commands in the time slot before jumping?	
4565	SC3003.1	If no command exists that is equal to the command-specified jump time, SC shall wait for the first command after the jump time.	The jump command may contain a time which does not correspond to a command so SC should just wait until the time elapses.	
4567	SC3003.2	If the command-specified time value is less-than or equal-to the current time, SC shall skip all of the commands in the past.		LRO, SDO
4569	SC3003.2.1	The status of all ATS commands skipped over as a result of the Jump command shall be marked as SKIPPED and an event message shall be generated.		LRO, SDO
4571	SC3003.2.2	If all of the commands in the ATS have been skipped, SC shall stop the ATS and issue an event message.	This may be an indication of an invalid Jump command.	LRO, SDO
4573	SC3003.3	If neither of the two ATS tables are currently executing, SC shall reject the Jump command.		LRO, SDO
4575	SC3003.4	If multiple commands exist that satisfy the JUMP condition, the commands shall be executed in ascending command number order (as they exist in the ATS table).	If multiple commands exist with the same time as specified in the JUMP command, execute the first command in the table at that time.	LRO, SDO
4577	SC3004	Upon receipt of an Enable Continuation Execution of ATS On Error Command, SC shall set the Continuation Execution of ATS On Error Flag to ENABLED.	Provides control on how serious a data integrity check failure is – in this	LRO

			case, continue to execute the ATS.	
4579	SC3005	Upon receipt of a Disable Continuation Execution of ATS On Error Command, SC shall set the Continuation Execution of ATS On Error Flag to DISABLED.	Provides control on how serious a data integrity check failure is – in this case, terminate the current ATS.	LRO
4641		**5.4 RTS Processing** The following requirements relate to the Relative Time Sequence processing. Commands are provided to start, stop each RTS. In addition, commands are provided in order to disable and enable individual RTSs.		
4581	SC4000	Upon receipt of a Start RTS Command, SC shall execute the command-specified RTS, or range of RTS, provided all of the following conditions are met: a)The command-specified RTS, or range of RTS, is not currently executing b) The RTS, or range of RTS, table(s) is Enabled c) The RTS, or range of RTS, table(s) has been Loaded	Method for starting an RTS.	LRO, SDO
4583	SC4000.1	If the conditions are met, SC shall issue an event message indicating the RTS started if the RTS number is less than <PLATFORM_DEFINED> RTS number.	Provides the ground an indication that an RTS started Having a config parameter allows a range of RTSs to be specified such that no event message is sent.	LRO, SDO
4585	SC4000.2	If the conditions are not met, SC shall reject the command and send an event message.	Ground needs to know if an RTS was not executed.	LRO, SDO
4587	SC4001	SC shall dispatch commands within the RTS table, in position order, as the relative time-tag specified in the RTS command expires.	RTS contain relative times between commands.	LRO, SDO
4589	SC4001.1	The time-tag shall be interpreted as the number of seconds to delay relative to the previous RTS command dispatched from that RTS table.		LRO, SDO
4591	SC4001.2	For the first command in an RTS table, the delay time shall be relative to the receipt of the RTS Start Command.	Provides the ability to delay the executing of the first command.	LRO, SDO
4593	SC4001.3	Prior to the dispatch of each individual RTS command, SC shall verify the validity of the following command parameters: a) RTS command length b) Embedded command Data Integrity Check Value	Basic verification that the RTS is not corrupt.	LRO, SDO
4595	SC4001.3.1	In the event an RTS command fails the validation checks, SC shall: a) Discard the invalid RTS command b) Generate an event message		

		c) ABORT the execution of that specific RTS		
4597	SC4001.4	Upon completion of the execution of the RTS, SC shall send an event message indicating that the RTS completed.	Gives the ground indication that all of the commands in an RTS executed.	LRO, SDO
4599	SC4002	SC shall terminate the execution of an RTS table upon detection of: a) A Stop RTS Command within the RTS command table b) Null data c) The physical end of the RTS table	Note that there is a separate requirement for stopping an RTS via a command.	LRO, SDO
4601	SC4003	Upon receipt of a Stop RTS Command, SC shall terminate the execution of the command-specified RTS table, or range of RTS table.		
4603	SC4004	Upon receipt of an Enable RTS Command, SC shall set the status of the command-specified RTS to Enabled.		LRO, SDO
4605	SC4005	Upon receipt of an Disable RTS Command, SC shall set the status of the command-specified RTS to Disabled.		LRO, SDO
4607	SC4005.1	If the RTS is currently executing when the Disable RTS Command is received, the current execution of this RTS table shall: a) Be executed until completion b) Set to RTS state to Disabled, preventing it from future execution	Executes the current RTS to completion and then allows an RTS to be disabled thus preventing a Start RTS to execute the RTS (must be enabled first).	LRO, SDO
4643		## 5.5 Status Reporting		
4609	SC8000	SC shall generate a housekeeping message containing the following: a) Valid Command Counter b) Command Rejected Counter c) Total count of commands dispatched from ATSs d) Total count of commands dispatched from RTSs e) Total count of commands which failed dispatch from ATSs f) Total count of commands which failed dispatch from RTSs g) ATS Table #1 free byte count h) ATS Table #2 free byte count i) Absolute Time Command Processing State j) Identifier of the active ATS table k) Number of the next ATS command pending execution l) ATS switch pending flag m) Time the next ATS command is due to be dispatched n) The identifier of the ATS table for which the most recent ATS command failed to dispatch o) The identifier of most recent ATS command which failed to dispatch from the ATS tables p) RTS table activation count q) RTS table activation error count r) Number of active RTSs s) Identifier of the next RTS table to dispatch a command t) Time the next RTS command is due to be dispatched u) Execution status for each RTS table v) Enable status for each RTS table w) Identifier of the RTS table for which the most recent RTS command dispatch error occurred x) The word offset within the RTS for the most recent RTS command which failed to dispatch y) ATS Continue-On-Failure status	Housekeeping telemetry to indicate basic SC status.	LRO, SDO (loosely)

		z) The last append ApId aa) The last ATS Append Table command count bb) The last appended count		
4645		**5.6 Initialization Requirements** The following are the requirements associated with Stored Command on an Application reset, cFE Processor Reset or a cFE Power-on Reset		
4611	SC9000	Upon a power-on or processor reset SC shall initialize the following Housekeeping data to Zero (or value specified): a) Valid Command Counter b) Command Rejected Counter c) Total count of commands dispatched from ATSs d) Total count of commands dispatched from RTSs e) Total count of commands which failed dispatch from ATSs f) Total count of commands which failed dispatch from RTSs g) ATS Table #1 free byte count h) ATS Table #2 free byte count i) Absolute Time Command Processing State - DISABLED j) Identifier of the active ATS table - None k) Number of the next ATS command pending execution l) ATS switch pending flag m) Time of the next ATS command dispatch n) The identifier of the ATS table for which the most recent ATS command failed to dispatch o) The identifier of most recent ATS command which failed to dispatch from the ATS tables p) RTS table activation count q) RTS table activation error count r) Number of active RTSs s) Identifier of the next RTS table to dispatch a command t) Time the next RTS command is due to be dispatched u) Execution status for each RTS table - IDLE v) Status for each RTS table - DISABLED w) Identifier of the RTS table for which the most recent RTS command dispatch error occurred x) The word offset within the RTS for the most recent RTS command which failed to dispatch y) ATS Continue-On-Failure status <PLATFORM_DEFINED> z) The last append ApId aa) The last ATS Append Table command count bb) The last appended count	Need to initialize values to a default state on cFE Power-on reset.	Derived
4619	SC9004	Upon a power-on reset, SC shall start RTS #1.	Want to reserve an RTS such that commands or a series of commands can be executed on startup. RTS #1 is reserved for initialization commands that can be easily changed, rather than inline, hard-coding of the startup procedures.	LRO, SDO
15438	SC9005	Upon a processor reset, SC shall start RTS #2.		
4647		**Appendix A Terminology**		

		This appendix contains the list of terminology for the CFS Stored Command Application used in this document • Absolute Time Sequence (ATS) – sequence of commands that are to be executed at the time specified with each command • Relative Time Sequence (RTS) – sequence of commands that are to be executed at the time specified with each command relative to the previous command (or to the Start RTS command if the command is the first one in the RTS list)		