Space Operations Communicator
Vol. 5, No. 4, October – December 2008

METEOSAT Second Generation: Automated Procedures Execution Algorithms

Lee Matheson[1]
EUMETSAT – European Organisation for the Exploitation of Meteorological Satellites

The Meteosat Second Generation (MSG) program consists of a series of geostationary satellites, which have a primary Optical payload that images the entire earth every 15 minutes. To achieve high image availability with optimal image quality, requires a repetitive and high frequency of commanding in a short time frame. To achieve this high availability, EUMETSAT utilises automated procedures for the commanding of the MSG Spacecraft platform and payloads. This paper goes into the generic algorithm considerations and implementation details that can be selectively applied in coding automated procedures, to ensure safety and high reliability. The examples used in this paper trace to experience gained in the use of automated procedures that were implemented for the commanding of the primary MSG Optical Payload, which is the Spinning Enhanced Visible and Infra-Red Imager (SEVIRI) Instrument. The paper covers the lessons learned and the applicability of the philosophy used in the algorithms to future Earth Observation Missions.

Nomenclature

CEV	=	Command Execution Verification
CF	=	Control Facility
ESTEC	=	European Space and Technology Centre
EUMETSAT	=	European Organisation for the Exploitation of Meteorological Satellites
FES	=	Full Earth Scanning
FMECA	=	Failure Modes Effects and Criticality Analysis
FOM	=	Flight Operations Manual
FOP	=	Flight Operations Procedures
HRV	=	High Resolution Visible
MPS	=	Mission Planning System
MOP	=	METEOSAT Operational Program
MSG	=	METEOSAT Second Generation
MTP	=	METEOSAT Transitional Program
OOL	=	Out of Limit
PE	=	Procedure Execution
RSS	=	Rapid Scan Service
TMTC	=	Telemetry and Telecommanding
PTV	=	Pre-transmission Verification
SEVIRI	=	Spinning Enhanced Visible and Infra-Red Imager

I. Introduction

Experience obtained in the use of automated procedures for the commanding of the EUMETSAT MOP/MTP geostationary satellites, was used in the design of the procedures for the MSG series of spacecraft. This commonality in concept, philosophy and implementation of automated commanding of the MOP and MTP satellite Instruments also eased the learning curve of the engineers, analysts and Satellite Controllers, when migrating from the operation of MOP/MTP to MSG[1].

[1] Spacecraft Ops Engineer, GEO, EUMETSAT, Kavalleriesand 31, 64295 Darmstadt, Germany.

The primary Imaging Instrument on MSG is the Spinning Enhanced Visible and Infra-Red Imager (SEVIRI) Instrument. The SEVIRI Instrument continuously images the entire earth 24 hours/day (every 15 minutes). During this imaging, the earth is continually kept centered in the Field of View, a High Resolution Visible (HRV) image position is adjusted, and Star Sensing (for orbit refinement) is continually commanded. In addition, to achieve the desired image performance specification, the Instrument is frequently commanded to conduct a high frequency of routine calibrations. To obtain optimal performance over 100,000 commands/year are sent to the Instrument.

The optimal operation of the SEVIRI instrument requires a high level of very frequent repetitive commanding, typically within a small time frame, with numerically small (but important) differences in command arguments. Automated procedure based commanding is used, because such automated procedures have an advantage in that they address the dangers and risks of ground Satellite Controller monotony associated with repetitive commanding, and also because such automated procedures can efficiently command the Instrument in a short period of time. The automation frees up the time of the Satellite Controllers such that they can monitor procedure execution in a "hands-off" manner.

The automated procedures have also been coded to take into account safety aspects of the Spacecraft/Instrument, such that in the worst case failure scenario, they will not further degrade the situation, and indeed may function such that they assist the Satellite Controller diagnosis and/or implement initial reactions for both satellite and selected ground failures.

Since the first MSG spacecraft going operational, the Imaging procedure has successfully executed more than 30,000 times/year, and the Calibration procedure more than 8,000 times/year, per MSG spacecraft.

II. Routine Automated Procedures

The automated EUMETSAT Flight Operational Procedures (FOPs) that are discussed in this paper are those that are executed dozens of times/day, as part of the conduct of the nominal "precision" imaging and calibration of the SEVIRI instrument.

The MSG program uses an automated scheduling system (referred to as Mission Planning System (MPS)), which will start the execution of procedures strictly according to a fixed chronological schedule, independent of any real time input from external events and independent of the spacecraft’s real time status. In the preparation of this schedule, detailed flight dynamics, seasonal, and spacecraft/instrument operational requirements are directly taken into account. Typically a new schedule is prepared once/week, although the duration can be changed due to personnel or spacecraft tasking factors. The preparation of the schedule is done by an engineer or analyst using software tools that, given specific inputs, automates the creation of the week's procedural activities. The nominal spacecraft operation, as conducted by the MPS, is then supervised by the on-shift Spacecraft Controller.

EUMETSAT's automated Flight Operational Procedures (FOP), whose execution is initiated by the MPS, are typically coded with a top level system procedure, which in turn will call, as appropriate, various child procedures, where the child procedures were coded in a "building block" approach, such that the lowest of the “building block” procedures conduct very specific functions. All "coded" procedure's trace back directly to specific contractor (and in some cases sub-contractor) written "paper" procedures, where these "paper" procedures (in a Flight Operations Manual (FOM)) were reviewed by the Instrument Contractor, the Spacecraft Prime Contractor, by ESTEC and by EUMETSAT. The existence of the paper procedures in the FOM forms an essential part of both a contractual, and of a software development process, that has contributed to the high reliability of the final FOP procedures.

Because the commanding of the SEVIRI Instrument required significant command repetition, it was well suited to the use of automated procedures, and hence it is used as the main example in this paper.

The specific MSG routine automated procedures associated with the SEVIRI imaging and calibration are:

(1) Full Earth Scanning (FES) Imaging (for images of the entire earth, executed once every repeat cycle, where a "repeat cycle" is typically 15 minutes in length)

(2) Rapid Scan Service (RSS) Imaging (for images of Europe, executed once every 3rd repeat cycle, where a “repeat cycle” is typically 5 minutes in length)

(3) Calibrations with a Black Body (where an ambient calibration is executed once per hour, and a heated calibration executed twice per day). However the calibration procedures were designed such that they could nominally be executed once per repeat cycle.

The routine imaging procedures' execution window is very timing constrained, having to match the specific state of the SEVIRI instrument (where the Instrument's details change dynamically with time). Hence it is important these automated procedures are launched at a specific, regular, predefined start time (and that they execute within the small time window).

For a typical 24 hour period, there are typically 96 imaging procedure instances executed and 26 calibrations procedure instances executed. The Instrument is complex, and many input arguments are necessary in the procedures, to have the necessary flexibility to properly command the Instrument.

Given that the input arguments to these procedure instances are minutely different, and that the launch time of each procedure requires high reliability and consistency, to expect a Satellite Controller to reliably input a large number of input argument values manually into a procedure on a constant and repetitive basis, and then constantly launch the procedures manually at very specific times, is unrealistic. Manual argument population and manual procedure launch by a user creates a risk of an incorrect launch time, and the risk of incorrectly entered procedure argument values.

To ensure reliable and precise launch of the automated procedures, their execution is mostly initiated by the MPS.

III. General Automated Flight Operations Procedure (FOP) Methods

The automated procedures were coded and then implemented with an effort to obtain high availability, while maintaining spacecraft and instrument health and safety.

When designing an automated procedure, consideration needs to be given to its intended use, its planned frequency of use, the criticality of the operations being conducted, the potential of failure(s), the potential seriousness of any failures, and the anticipated level of Satellite Controller, analyst, or sub-system engineering expert monitoring of the procedure execution. These considerations in turn dictate how many of the generic algorithmic considerations, detailed below, need be followed (and if possibly more considerations are required).

A key fundamental assumption underlying the execution of all automated procedures is that the ground system is setup to distinguish between valid telemetry, and invalid telemetry, and flag the telemetry accordingly. This required fundamental telemetry validity determination "feature" is used extensively by the automated procedures.

In the case of the EUMETSAT MSG routine automated Imaging and Calibration procedures, each procedure contains code and logic:

(1) such that the procedures can be safely aborted at any time during their execution (especially during a failure state), with no (to minimal) essential follow-up action necessary by the Satellite Controller,

(2) to provide resilience/robustness against brief telemetry drops;

(3) to provide automated checks against incorrect input-arguments inappropriately passed from the Satellite Controller, or the Control Facility's scheduling system, to the procedure,

(4) such that <u>before</u> any commanding, the procedure(s) conduct automated checks of the current and planned (system level) status of the Instrument relevant to the commands that are about to be sent, to ensure compliance with the contractor's Instrument constraints,

(5) such that <u>after</u> commanding, they conduct automated checks of the complete (system level) status of the Instrument based on the commands sent, to ensure compliance with the contractor's Instrument constraints

(6) such that they take automated contingency action (for specific failure scenarios), placing the SEVIRI Instrument in a safe position (relative to the sun angle and relative to the Instrument's calibration section), when the procedure detects a need to quickly place the Instrument into a safe standby mode. Such a "quick need" could result from the procedure detecting from telemetry (or other criteria) that the contractor's specified constraints are not being met.

(7) to provide automated checks against specific (pre-identified) inappropriate Satellite Controller reactions to selected procedure failures,
(8) to provide automated run-time quality checks (and automated contingency reactions) against the ground control facility's procedure execution running too slow,
(9) to make use of MSG satellite onboard Time Tagged commands, coupled with ground commands, to ensure two independent commanding methods are in place for "performance" critical and "health/safety" critical commanding;
(10) to provide Spacecraft Controller visibility into the procedure automated execution. This was conducted by implementing an assertable parameter in the Ground control facility's Telemetry/Telecommand Database that tracks the execution health of the procedure. The procedure sets this database value at various stages of execution, and there are database limits in place that will go Out-Of-Limit (raising an alarm), dependant on the database value that has been set by the procedure.
(11) to automatically log to a ground facility, an event history in an electronic ascii log file, which detailed paths the procedure followed, to support subsequent data analysis.
(12) to be directly traceable, compatible and compliant with the Spacecraft Prime Contractor's recommended and detailed commanding FOM "paper" procedures.

Note that not all of the above details, are implemented in every EUMETSAT automated procedure. Instead, the procedure’s level of automation is custom tailored to its intended use.

Some more detail on each of the above aspects follows:

A. Reaction To Take in the Event of an Automated Procedure Failure

Every automated procedure can credibly fail for a number of reasons. (The types of failures that an automated procedure can experience are described later in this section). Hence it is critical that for every step in an automated procedure, that the possibility of a procedure failure is considered. Having written that, it is not practical to have a different automated contingency reaction for every step in a procedure. Rather the approach adopted by EUMETSAT was that when the procedure failed, it would fail in such a manner that it was supportive of the analysis that need be done next by the Satellite Controllers.

During procedure design, having reviewed every proposed procedure step, it was possible to categorize the procedure's critical steps, and also possible to categorize the types of failures that are more likely to occur. The procedures could then be structured during coding, with these credible failure possibilities in mind.

This failure categorization was not done for every spacecraft procedure, but it was done for automated procedure’s that were typically launched often, and were executed in an unattended manner.

With respect to the procedures where the failure analysis was conducted, automated procedures will typically fail if:

(1) inputs required by the procedure are incorrectly provided (such as no spacecraft telemetry, or missing procedure arguments, or incorrect procedure arguments, or an inability to access a database, or an inability of a procedure to access an appropriate image file), and/or
(2) the control facility execution environment that supports the procedure fails (ie a ground software or hardware hard (or soft) failure that affects the execution of the procedure), and/or
(3) spacecraft/instrument fails the checks/criteria that are hard coded into the procedure, and/or
(4) Satellite Controller provides an incorrect reaction to a procedure interaction.

In all of the above failure cases, similar failures can also occur without the use of automated procedures. In other words, most automated procedure failures have equivalent failures in a non-automated procedure environment. However, with automated procedures the failure indication is presented to the Spacecraft Controller by the notification of a problem with Procedure Execution software, in addition to being presented by telemetry Out-Of-Limit anomalies, or by Spacecraft controller display monitoring, or by various Ground computer anomaly warnings, or by commanding failures.

Typically, the anomalies encountered specific to automated procedures (that do not occur in a manual execution environment) were either due to the failure of the CF automated procedure environment software itself (ie by a software bug in the “procedure execution environment”), or by the Operating System environment in whch the automated procedure execution system resides, or by improper Satellite Engineer automated procedure coding (such as coding an inappropriate TM check, or coding inappropriate timing between successive steps in an automated procedure, (where execution of sequential functions can occur vary rapidly)).

A Satellite Control Facility (CF) Procedure Execution (PE) environment (such as the Apex system used by EUMETSAT[2]) will typically provide various means to recover a procedure, in the event a procedure fails. These environment failure recovery reactions could include aborting a procedure, suspending a procedure, repeating the failed step, resuming at the next step, or even repeating/resuming at different phases of a failed step.

1. Identical Reaction to Procedure Failures by Users

The MSG automated imaging procedures (for the SEVIRI Instrument) were structured such that in the event of a procedure failure, the identical "initial" Satellite Controller action should be taken in all failure cases. Having the identical "initial" action simplified the Satellite Controller training, and significantly reduced the possibility of error due to the Satellite Controller not initially knowing what to do in the event of a procedure failure.

Such an identical approach (to a failure) may not always possible, nor appropriate, for control of all spacecraft subsystems, but in the case of the MSG SEVIRI Instrument Imaging procedures, it was possible to implement this approach.

For SEVIRI, the Satellite Controller action for a failure in an Imaging or Calibration Procedure, is to always abort the “parent” procedure when there is any failure of the "parent" or any failure of an associated “child” procedure.

This “always abort” approach for an Imaging/Calibration procedure, was an obvious approach to adopt, as it means a single unified "initial" approach can be adopted for:
(1) a catastrophic ground commanding failure, and
(2) for any other procedure failure.

Given these procedures execute in excess of 30,000 times/year, having one common failure reaction was very beneficial.

In some cases, the failure of one automated procedure can affect the execution of other automated procedures, especially in cases where there are parent/child procedure relationships (ie much like sub-procedure calls in a piece of software code). Hence the MSG Imaging procedures were coded such that, in the case of a failure of a synchronous child procedure, the Satellite Controller action required (after observing and documenting the problem) is to first abort the parent of the failed synchronous child procedure. In the case of the EUMETSAT "procedure execution system"[2], aborting the parent causes both the parent and any "synchronous" child procedures to automatically abort.

This ensures that a parent (and child) procedure does not keep executing (and does not keep sending commands to the spacecraft), when a child (and parent) procedure only completed a fraction of its functions.

2. Planned Abort if Failure & Associated Procedure Coding Constraints

To enable this specified Satellite Controller re-action to work (where the Spacecraft Controller must always abort the failed procedure), all of the commanding and all of the checks (within the parent and child procedures) had to be structured in such an order, that it is safe to abort the procedure’s execution at any time.

The impact of a failure in every parent and child procedure step had to be considered. The implementation and precise timing of commands and telemetry checks (including the use of time tagged commands), and the use of an appropriate selection of "normal child" procedures (where the parent waits for the child to complete), and of "orphaned-child" procedures (where the parent does not wait for the child to complete), had to be examined to ensure that this "abort" (the parent procedure) methodology would always work.

B. Procedure Resilience to Telemetry Drops

A drop of spacecraft telemetry can occur at any time during the controlling of a spacecraft.

The question the procedure coder had to answer, was what should a procedure do when there is no telemetry? Also to be asked was when should telemetry be checked?

The criticality of a telemetry drop depends on the function of the procedure, the frequency in which the procedure is launched, the commanded state of the spacecraft at the time of the telemetry drop, and the criticality of the spacecraft subsystem the procedure was commanding.

Hence it was key that some of these procedures would handle such drops in a graceful manner, and for other less frequently run procedures, having a Satellite Controller monitor the execution was either sufficient or necessary (and thus extra procedure logic was not required).

This section goes on to examine cases where the procedure itself needed to monitor the telemetry status.

1. User Abort Procedure if Procedure Failure & Associated Procedure Coding Constraints

In the case of the MSG SEVIRI Imaging procedures, one of the very first procedure steps after the procedure commenced execution, was for the procedure to check the validity status of every telemetry parameter needed by the procedure or by the parent procedure’s child procedures (referred to as “children”). If at the parent procedure(s) start, any one parameter did not have the correct validity, the parent procedure would wait for one-minute for the telemetry to become valid, and then automatically (if telemetry did not become valid) execute a contingency thread that would immediately have the procedure gracefully exit (after this one-minute time “window”). In such a failure case, as part of the contingency thread exit, the procedure would assert an Out of Limit assertable telemetry parameter in the Spacecraft’s TMTC (telemetry and telecommanding) database (with a resultant audible alarm), and log an event that the procedure’s sampled telemetry was bad, providing the Satellite Controller warning of the anomaly. Based on the value of the assertable telemetry parameter, the Satellite Controller(s) have a manual procedure to follow, advising them of what re-actions they needed to take next.

If within the one minute before the procedure’s contingency thread activated (while the procedure was still waiting for telemetry to be restored), all the telemetry was restored and became valid, then the procedure would detect the restoration, and would not fail, but rather the procedure would instead continue executing nominally.

A side benefit of this was every time an Imaging Procedure was launched (which was every 15 minutes), the validity of the Spacecraft telemetry was independently checked by the Imaging Procedure. Experience has proven that on occasions where the ground control computers malfunctioned, many times the very first indication of bad telemetry came when the Imaging Procedures flagged a telemetry validity problem.

2. Automated Procedure Telemetry Checks During Procedure Execution

During procedure execution, telemetry can “drop” (and not be available) at any time. Even though a procedure had proper valid telemetry at its initial execution, telemetry can still drop while the procedure is in the middle of its execution.

Hence some EUMETSAT MSG procedures had even further telemetry checks interspaced through the body of the procedure. This was done only for procedures that were run with minimal supervision and that were run a very large number of times (such as the Imaging procedures).

For the Imaging procedures, for every step where a check of telemetry is required, each step has a trigger expression that waits for the validity status of the telemetry to become valid prior to the remainder of the step continuing. The time frame in which a procedure's step would wait for valid telemetry was selected based upon the function/criticality of the step, and the location of the step within the procedure. The time varied, but typically a wait of 30 seconds to 60 seconds was implemented.

In the event that the telemetry associated with a step did not become valid within the waiting time frame, the step would fail. This means the procedure will fail, the procedure execution would stop, and the procedure execution environment will raise an audible alarm and raise an interaction requiring Satellite Controller attention. As noted above, the Satellite Controller reaction to such an imaging procedure failure, in all cases, is to abort the procedure.

Typically, prior to aborting, the Satellite Controller would perform appropriate control computer screen dumps and take notes, to document the location of the failed step, to help in subsequent analysis. Sometimes a failure in an imaging procedure was indicative of a bigger failure on the spacecraft, and hence this had to be taken into account by the Satellite Controller when documenting the failure.

C. Automated Procedure Checks Against Incorrect Procedure Input Arguments

Input arguments (parameter values) to both commands in a Telecommand Database and input arguments to procedures, require checks to ensure they are within range, and that they are safe and "reasonable". The extent to which these checks are done, are dependent on the function/criticality of the spacecraft subsystem being commanded.

In the case of the Imaging procedures, every parent imaging procedure has been coded such that there are validity checks conducted against every input argument that can be provided to and used by the procedure. Such input arguments are normally inserted (when the procedure is initially executed) either by the MPS or by the Satellite Controller.

To try and ensure a high quality of input arguments were provided to procedures, EUMETSAT has implemented automation in the MPS preparation (with associated automated checks and constraints within the MPS), and also provided a high degree of training and clear manual procedures governing the use of automated procedures. The weekly MPS are also independently checked every week by an engineer prior to being brought "on line" for use. This has ensured that the possibility of either an MPS planner, or a Spacecraft Controller, will provide an incorrect argument to an automated imaging procedure is very remote and very small. However we still live in an imperfect world, and mistakes can still be made (and have been made).

Hence at the start of an automated Imaging procedure's execution (after telemetry validity checks), the automated imaging procedure will then check the range of an input argument's value to see if it is within a predefined nominal range. The automated procedure will also do cross consistency checks of the input argument values against each other, and also cross consistency checks against current spacecraft telemetry.

The type of checks that are coded in a procedure are governed by:

(1) common sense,
(2) an understanding of the Spacecraft platform and the payload, and also by
(3) pre-defined guidelines provided by the Spacecraft Prime Contractor in the Contractor's provided FOM, as to what is acceptable commanding for the Spacecraft and the payload,
(4) experience gained during months of ground "operational scenario" development tests of the procedure (run against a simulator) and during spacecraft commissioning and subsequent spacecraft operations.

All of these factors were useful in improving the quality of these input argument checks.

In the event that such an input argument value check failed, the procedure will typically exit immediately in a graceful manner, while at the same time flagging an Out of Limit assertable telemetry parameter (with a resultant audible alarm) in the TMTC database, and log an event that sampled telemetry was bad.

Based on the value of the assertable telemetry parameter, the Satellite Controller has a manual procedure to follow advising them of what further re-actions they need to take next.

D. Automated Procedure Pre-Commanding Checks

Prior to any command being sent to the Spacecraft, or to the Instrument, automated checks are conducted of the current and planned (system level) status of the SEVIRI instrument, based upon the commands that are about to be sent, to ensure compliance with the contractor's Instrument constraints.

Every Spacecraft command is entered in a database within the CF, where automated checks are conducted by the TMTC database and prior to a command executing. This is to ensure the spacecraft and associated subsystems are in the correct state, prior to the command being sent. If the check of the Instrument state does not pass, a command would fail its Pre-Transmission Verification (PTV) check in the TMTC database, and in addition,

(1) the procedure would fail,
(2) the procedure's execution would stop,
(3) the PE environment would raise an audible alarm and
(4) the PE environment would raise a procedure interaction requiring Satellite Controller attention.

As noted in para-3.1 above, the Satellite Controller reaction to such an imaging procedure failure, in all cases, is to abort the procedure.

In addition, prior to the above CF database PTV checks, the (Imaging) Procedures are in some cases coded with additional checks (where such checks are too specific to be conducted by the CF command database) to ensure the Spacecraft subsystem is in the precisely correct state for commanding and that the command arguments are precisely appropriate per the contractor's provided FOM guidance. In the event that any such check failed, the procedure would automatically and immediately gracefully exit, while at the same time providing the Satellite Controller both an Out of Limit assertable telemetry parameter (with a resultant audible alarm), and log an event that the planned command in the procedure failed its checks.

Based on the value of the assertable telemetry parameter, the Satellite Controller had a manual procedure to follow, advising them of what further re-actions they needed to take next.

E. Automated Procedure Post-Commanding Checks

Nominally, as part of regular spacecraft commanding, after every nominal command being sent to the Spacecraft platform, or to the Instrument, (and after every time tagged command's execution), automated checks would be done of the current and planned (system level) status of the command, to ensure proper execution.

Again, dependent upon the criticality and complexity of the operation being completed, after commanding it was necessary (during the design/coding phase) by the procedure coder to decide if further checks were needed by the procedure being coded. The more complex the procedure, the more complex the validation, and this is discussed further in Section-VII (Automated Procedure Validation) and also Section-IX (Lessons Learned).

Every Spacecraft command is entered in a database within the CF, where automated checks are conducted by the database after a command has executed, to ensure the spacecraft and associated subsystem are in the correct state, after the command has executed. If the state is not met, a command will fail its Command-Execution-Verification (CEV) check, the procedure will fail, procedure execution will stop, and the PE environment will raise an audible alarm and raise an interaction requiring Satellite Controller attention. As noted in para-3.1 above, the Satellite Controller reaction to such an imaging procedure failure, in all cases, is to abort the procedure.

In addition, after the above CF database CEV checks were completed, in some cases the Platform/Imaging Procedures were coded with additional checks (which are too specific to be conducted by the CF command database) to ensure the Platform/Imaging Payload were in the precisely correct synchronized state for commanding and that the command arguments were precisely appropriate per the Spacecraft Prime Contractor's provided FOM.

In the event that any such procedure level check failed, the procedures were coded to react based on the seriousness of the procedure's command check's failure.

The details, as to the type of contingency reactions that were coded to be taken, are described in the next section.

Based on the value of the assertable telemetry parameter, the Satellite Controller(s) have a manual procedure to follow advising them of what further re-actions they need to take next.

F. Procedure Automated Contingency Reactions

This is perhaps one of the more controversial areas to be considered in automated procedure execution. How much can one rely on a procedure to detect, and then take the appropriate reaction in the event of a failure?

As already noted in paragraph E above, the automated procedures have been coded, for specific well defined circumstances/failure scenarios, to take limited and selected automated contingency reactions.

In the case of the MSG Imager (SEVIRI), typically in a case where a safe contingency re-action was required, the contingency reaction would place the SEVIRI Instrument into a safe position (relative to the sun angle, and relative to critical equipment on board, such as the Instrument's calibration section). Such a need to take such contingency reactions is typically driven by the Spacecraft Prime Contractor's pre-defined cautions and constraints, especially where there may be a time criticality aspect associated with the contingency reaction.

While ideally, in Satellite Control, there would be no time critical aspects for the ground to handle, in practice cost and schedule constraints when building a spacecraft, and when building a spacecraft payload, can limit the functionality that can be placed on the spacecraft and on the payload. In the case of MSG Imaging payload "SEVIRI", there are time critical activities that were needed to be handled in a timely manner, for not only health and safety, but also for Image availability and quality. The tradeoff in terms of the amount functionality that resides in the ground, as opposed to residing in the satellite/payload, is invariably programmatically and technically driven, and going into such specific programmatic and technical tradeoffs are outside the scope of this paper.

1 Types of Contingency Reactions

The automated Imaging and Calibration procedures have been coded to take automatic contingency reactions under certain failure cases. The level of contingency reactions to take when the procedure detects a need for a contingency reaction, are as described below:

(1) (contingency-reaction-1) procedure will automatically exit immediately, flagging an OOL in the TMTC database so as to advise the Satellite Controller that there was a minor problem, and to provide guidance where the problem lay,

(2) (contingency-reaction-2) procedure will automatically stop the execution of the nominal commanding path, and instead the procedure will launch an asynchronous orphan procedure to place the Instrument in a safe state. The procedure will also require the on-shift Satellite Controller acknowledge this contingency is being taken, and the procedure will provide a high level indication to the Satellite Controller as to why the contingency reaction is being taken. In the case of the SEVIRI Imaging procedures, the Satellite Controller acknowledgement was at a point after the automated procedure's initial (urgent) Contingency Reaction initiation had either already commenced, or had already completed. Failure cases where a Satellite Controller decision might be needed to interact with an automated procedure, and initiate a pre-defined contingency reaction were not coded into the EUM automated Imaging procedures (In fact, there were no identified SEVIRI/payload specific failure cases requiring an initial Satellite Controller interactive approach with an automated procedure).

2 Generic Failure Cases

Automated contingency reactions have been predefined as being required when the procedure identifies that the Spacecraft Prime Contractor's specified Instrument operating constraints are not being met during a routine operation. The credible failures likely to be encountered (that could lead to such operation outside of pre-defined constraints) have been pre-analyzed, and were grouped according to severity. The types of severity identified were:

(1) (failure-case-1) prior to any commanding, the procedure detects it is being requested to command the Instrument with inappropriate values - the procedure automatically initiates contingency reaction-1,

(2) (failure-case-2) prior to any commanding, the procedure detects it is being requested to command the Instrument at an inappropriate time, relative to on-going Instrument and Spacecraft operations - the procedure automatically initiates contingency reaction-1,

(3) (failure-case-3) after commanding, the procedure detects inappropriate Instrument telemetry values related to the failure of a command's execution, where such a failure has no health and safety, nor any major performance implications, nor any minor performance implications that could escalate to major problems - the procedure automatically initiates contingency reaction-1,

(4) (failure-case-4) after commanding, the procedure detects the commanding needed by the Instrument was completed too late, which if not acted upon immediately, could directly cause an Instrument anomaly (possibly resulting in the Spacecraft powering off the Instrument within 10 to 25 minutes, or worse, Instrument damage) - the procedure automatically initiates contingency reaction-2,

(5) (failure-case-5) after commanding, the procedure detects Instrument telemetry values, indicating a failure, where such a failure could result in a major imaging outage, or could cause an Instrument anomaly (resulting in the Spacecraft powering off the instrument within 10 to 25 minutes, or worse, Instrument damage) - the procedure automatically initiates contingency reaction-2.

The contingency action to take for "contingency-case-2", where commands are sent to the satellite to place the Instrument in a Safe configuration, was carefully examined, and reviewed by EUMETSAT engineers, reviewed by the Satellite Prime contractor, and validated by EUMETSAT for all credible failure scenarios, to ensure that it was a minimally prudent reaction, and that the reaction was 100% safe.

For all of the above cases, there are a set of predefined Satellite Controller reactions, written in a users manual, for use by the Satellite Controllers, analysts, and engineers, providing guidance as to what reactions need to be taken in the case of known and predicted problems, and what to examine and what to investigate where the cause of the problem is not immediately obvious.

Note that in the most part, automated contingency actions are not taken by the procedure in the case of failures of the CF PE environment in which the procedure executes, as that is not practical.

G. Automated Procedure Checks Against Human Error

During the pre-launch Operations Scenario Testing of procedures, there were a number of cases where despite training to the contrary, Satellite Controllers re-acted inappropriately when a procedure failed.

For example, on some occasions, a Satellite Controller conducted a “repeat step” (telling the procedure to repeat the failed step) or a Satellite Controller conducted an “acknowledge – go to next step” (telling the procedure to ignore the failure and go to the next step), when an abort was the required reaction. A possible reason for the “repeat step” Satellite Controller failure, is because a “repeat step” (or “acknowledge – go to next step”) is a common recovery action for non-time critical Satellite automated procedures (with less automation) where a failure is due to a TM drop, or due to a timing issue between procedure steps. A “repeat step” will often address such a simple non-time critical scenario. In this and other cases, Satellite Controllers were used to being instructed to “repeat a step” or “acknowledge – go to next step” by a Satellite Engineer, or by a Satellite Analyst for non-time critical procedures (being executed slowly under close supervision of an Satellite Engineer). Hence the Satellite Controllers had observed different reactions for non-time critical automated procedures that run slowly (under close supervision) than what they were required to use for automated Imaging procedures that ran quickly, automatically and unattended. The required reaction for the two types of automated procedures was different, and this initially led to some Satellite Controller confusion (despite ongoing training to clarify).

Because the SEVIRI Imaging procedure’s have a relatively short pre-defined time within to execute, a “repeat step” selected minutes after a failure, could result in an automated procedure step executing too late, or making an inappropriate temporal calculation. An “acknowledge – go to next step” could result in a procedure executing further steps that were inappropriate given the failure.

Another example of human error was the policy in the event of a procedure failure, where both parent procedure (ie the main program) and child procedures (ie a procedure that corresponds to a subroutine in a program) were executing in parallel. The required action is to abort the parent procedure first, and not abort the child procedure first. The danger here is if the Satellite Controller aborts the child procedure first, the parent procedure may continue to execute, even though the child procedure did not complete its functions. Dependant on the child procedure's functions that were not completed, this could have severe consequences on the parent procedure's activities. On rare occasions, despite training to the contrary, Satellite Controllers would make mistakes, and mistakenly abort the child procedure first (causing the parent procedure to inappropriately execute with the actions of the child procedure not completed). Subsequently, based upon observing this common mistaken Satellite Controller behaviour, the parent procedures were modified with revised code to check to see if the child procedure had been aborted, and if the child procedures were aborted, the parent procedures would then fail (ie a second failure after the first failure), with an interaction. This modified coding gave the Satellite Controllers the opportunity to then reconsider their action, and correctly abort the parent procedure with no adverse impact (and hence in essence rectify their mistake).

Hence based upon the experience gained in the pre-launch testing, it was possible to categorize the typical location, and the typical type of operator failures, and then hard code in the procedure specific checks at selected key (health, safety and availability related) locations internal to the procedure, to handle the possibility that a previous step may have incomplete execution, or that the procedure may be executing late, or that a child procedure was inappropriately aborted first, because of the Satellite Controller mishandling a previous procedure failure.

Dependant on the type of automated procedure check, the procedure will either simply fail a second time or, the procedure will automatically and immediately gracefully exit, while at the same time providing the Satellite Controller both an Out of Limit assertable telemetry parameter (with a resultant audible alarm), and log an event that the planned check in the procedure failed.

Based on the value of the assertable telemetry parameter, the Satellite Controller has a manual procedure to follow, advising them of what further re-actions they needed to take next. If it was a type of failure that was typically associated with a Satellite Controller mistake, the Satellite Controller would read this in the associated manual procedure.

Note that extensive pre-launch Operational Scenario testing of the procedure against a high fidelity Spacecraft/Instrument simulator was key in keeping the scope of these checks down to the bare minimal level. These checks in essence cover a double failure, and coding for double failures is incredibly complex. Hence it was essential to code these sorts of checks based upon known experience in only the most important health and safety related areas.

An alternative approach (in addition to automated checks against human error) is to simply add more training to a Satellite Controller's possibly already busy training schedule. However simply adding "training upon training" to a Satellite Controller is not always the best approach, when an identified re-occurring problem can also be cured by adding more robustness to an automated procedure. Invariably when deciding the approach to take, there is a trade off being the predicted success (and time and effort) associated with further Satellite Controller training, as opposed to assigning effort associated with changing the automated procedure (with the associated validations, configuration control, and possible new training associated with the change). Where appropriate, in addition to increased training, EUMETSAT modified selected procedures to detect inappropriate Satellite Controller failure reactions.

H. Automated Procedure Runtime Quality Checks

At certain key locations in the procedure, there were hard coded run-time quality checks (and automated contingency reactions) against the procedure running too slow within the ground control facility's PE environment.

Even though a procedure was launched in time, it was possible that intermittent telemetry could result in the procedure running slower than intended, as the automated procedure paused at various locations waiting for telemetry to be restored. Alternatively, the CF computers themselves could be suffering from an anomaly, causing the environment in which the procedure ran to slow down, and hence cause the procedure to run excessively slow.

In particular, the need for such checks were confirmed after launch, where it was only after launch that the CF computers were run for month after month without a restart, and minor CF incremental problems were observed to build up. Hence automated procedure checks (that were not in place for the pre-launch Operations Scenario Testing) were subsequently added to the automated procedures as part of on-orbit procedure maintenance.

The Imaging activities on the SEVIRI instrument are conducted with a pre-planned timeline in place. The commanding needs to be synchronized to the Instrument's operation. If the procedure is executing significantly late at any particular time, there is the risk that health and safety checks or even Instrument commanding could be completed at a point in time that are inappropriate to the imaging mission.

Hence a small number of key locations were identified in the procedure, where it was noted as being most important that the procedure was still executing in a timely manner, prior to the procedure proceeding. At those locations, the procedure would check telemetry as to how much time was left (in a repeat cycle) to determine if it was prudent for the procedure to continue executing. If the time check failed its criteria (i.e. insufficient time was remaining), the procedure would automatically and immediately gracefully exit, while at the same time providing the Satellite Controller both an Out of Limit assertable telemetry parameter (with a resultant audible alarm), and log an event that the procedure was experiencing run time difficulties.

Based on the value of the assertable telemetry parameter, the Satellite Controller had a manual procedure to follow advising them of what further re-actions they needed to take next.

I. Automated Procedure Duplicate and Time Tagged Commanding

As noted, a key requirement was that the automated Imaging procedure could be safely aborted at any time and location during its execution, with no health and safety impact. In order to implement such a methodology, it was necessary to make use of MSG satellite onboard Time Tagged commands, coupled with ground commands, to ensure two independent commanding methods are in place for "performance" critical and "health/safety" critical commanding.

For example, in some cases, the “OFF commands” for a key function were uploaded automatically by the procedure to the satellite's On-Board-Schedule as Time Tagged commands (tagged for execution at a specific time in the future). These Time Tagged commands were typically uploaded prior to the “ON” commands such that, after the procedure switched a function ON, if the procedure then immediately failed (and hence not able to switch OFF a key Instrument function) the Time Tagged commands would still execute and switch “OFF” the associated Instrument function.

Dependant on the functional aspects (health, safety, and also telemetry timing) of the command in the on-board satellite schedule, if for some reason a minor anomaly on the Spacecraft disabled the satellite's On-Board-Schedule (and hence prevented the Time Tagged Command from executing), the procedure, if it was still running, would either:

(1) Monitor telemetry, and send the appropriate Command from the ground if it was not observed to execute from the on-board schedule, or

(2) Based on time send the appropriate Command from the ground in parallel to the Time Tagged command(s) execution from the on-board satellite schedule.

Each and every case in which this time-tagged commanding was implemented, all aspects of the commanding had to be carefully analyzed in terms of the failures that could credibly arise. This was to ensure that in all cases the reactions automatically taken by the procedure in parallel with the time tagged commanding were appropriate or, that in the event of a procedure failure, the time-tagged commands were sufficient to restore the Instrument to a safe state with no further procedure commanding required.

J. User Real Time Visibility into an Automated Procedures Execution

Automated procedures can have complex logic, and they can typically execute in a very rapid manner, such that it can be difficult to understand what the procedure is doing at any specific timeframe. While slowing down the execution of a procedure is one approach (to better monitor a procedure's execution), it is not always feasible, nor always desirable, to artificially slow down a procedure's execution.

EUMETSAT CF PE[2], can display procedures to Satellite Controllers, during the procedure's execution, in a graphical, flow chart, presentation (see section-V below). This presentation, if each step is properly labeled, can provide an excellent insight and index into a procedure's logical structure, making it easy to follow a procedure's execution, and also assist in the analysis of a procedure failure.

However given other tasks that need to be conducted in a Control Facility (including the monitoring of health and safety of other spacecraft), and given the potential speed of a procedure's execution, it is often not possible for a Satellite Controller to monitor the automated and rapid flow chart execution of every step within a procedure. Accordingly, EUMETSAT decided it should be possible for a Satellite Controller to quickly glance at a alpha-numeric display, and have a high level indication as to what the Imaging procedure is functionally doing (at a very top level) at any specific time frame.

EUMETSAT achieved this top level visibility into the Imaging procedure's execution, by implementing an assertable parameter in the Ground control facility's Telemetry and Telecommand Database, where the assertable parameter is setup to track the execution health of the procedure. This assertable parameter was defined in the mentioned database, with a text set of values corresponding to various key top level (and simplistic) functional states of the procedure, indicating what state the procedure was currently in during its execution.

During execution, the procedure asserts this database parameter to different values, with it displayed via an Alpha Numeric Display (AND) indicating the procedure's progress. Hence the Satellite Controller only needs to examine this value to know if the procedure is relatively "OK", or if it is in the process of conducting some key operation, or if the procedure has "run into trouble" and is executing a contingency path. In the event of a contingency path being executed there are database limits in place that will go Out-Of-Limit (raising an audible alarm), dependant on the database value that has been set by the procedure.

This "feature" to monitor procedure execution was added as a post launch "feature", after operationally controlling the satellite for an extended period of time. The "feature" was found to be very useful in providing Satellite Controllers a means of making a rapid top level assessment of an automated procedure's status.

Based on the value of the assertable telemetry parameter, the Satellite Controllers have a manual procedure to follow advising them of what re-actions they need to take next.

K. Procedure Automatic Log of its Own Execution Details

To assist in analysis of a procedure anomaly, and also to assist in verification of a procedure (before operational use), the Imaging procedures were coded with steps that automatically logged to a ground facility the results of various procedure and Instrument events in an electronic ASCII text log file (called the event history). This electronic ASCII log thus details selected critical paths (and the associated times) and activities the procedure followed, to support subsequent data analysis.

When conducting formal validations of a procedure, this electronic ASCII log was also invaluable in the verification test analysis, in confirming the correct function of an automated procedure.

L. Procedure Direct Traceability to Spacecraft Prime Contractor's Requirements

As already noted, the coding of the procedures were done such that they were directly traceable, compatible, and compliant with the Spacecraft Prime Contractor's recommended and detailed commanding guidance provided in FOM "paper" procedures.

In some cases, where specific complex checks were done that were critical to the health and safety of the Instrument, reference was made within the procedure's comment section to the appropriate FOM section. This simplified the verification and maintenance of the procedures, as the relevant sections could be traced in case there were concerns about the step implementation, from a maintenance, or verification perspective. Both the "paper"

FOM’s and automated electronic FOP’s were placed under configuration control, and any changes to the FOM resulted in the Change Control Review Board, or in the Anomaly Review Board, placing actions on engineers to ensure automated FOP procedures and paper FOM procedures were updated in parallel. As the program matured, the FOM updates (from the satellite prime contractor) occurred very infrequently.

IV. Mission Planning System (MPS) Schedule Implementation

The MSG CF Mission Planning Schedule (MPS) will launch procedures according to a fixed chronological time, without regard to external events. Hence if one procedure were to fail (and be aborted) there could still be another procedure scheduled to be launched for execution very soon in time. This schedule execution is supervised, and run by the on-shift Satellite Controller.

The automated full-earth-imaging automated procedures, launched by the schedule, were structured such that the cancellation (or aborting) of one procedure (at the start, or anywhere internal to the procedure) does not nominally affect the functional execution of the next subsequent procedure (assuming the satellite and instrument are in a nominal state, and where the failure was due to a known, non-satellite related event). As already noted, the imaging procedures were coded such that they could be cancelled from the automatic scheduling system without having to reschedule any subsequent instances of the same (or other) imaging procedures. The same was true for the calibration procedures.

The exception to the above would be if the procedure launches a contingency reaction to place the Instrument into a safe state. In such a case, manual Satellite Controller intervention would be required, to resume imaging of the Instrument, and to also suspend the automatic schedule execution, until which time it is prudent to resume the schedule.

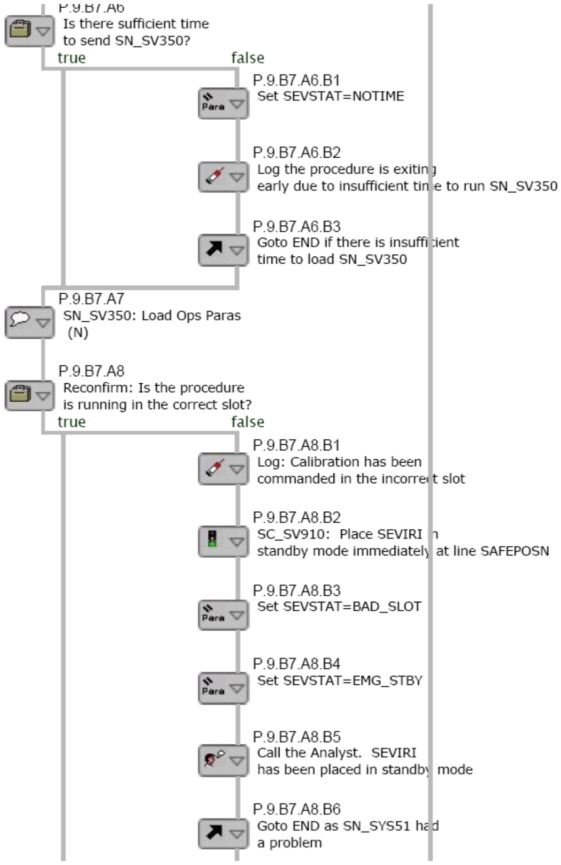
V. Automated Procedure Graphical Flow Chart Implementation

The operational procedure language at use on the MSG program at EUMETSAT has the automated procedures coded using an offline "flow chart" type display environment. When the procedures are in use on the CF PE environment, commanding the satellite, they also visually execute in a similar "flow chart" type display environment. The Satellite Controller can display this flow chart presentation, to monitor the procedure’s execution, if they wish.

The readability of such flow chart presentations is extremely important for automated procedures. Satellites are already very complex, and adding an additional layer of procedure complexity to the control of a satellite is counter productive to Satellite Controller, analyst and engineer understanding as to what is taking place on a modern spacecraft. Hence it is important that the display and execution of procedures be such that it simplifies the satellite control, and not increases the complexity.

Figure-1 provides an example of the flow chart presentation that is available to a Satellite Controller in both the offline and the online execution environment. This figure is typical of a flow chart presentation created with the APEX Automated Procedure EXecution system procured by EUMETSAT from SciSys[2].

If there is a procedure failure/stoppage, with a "flow chart" presentation, it is relatively easy to precisely identify (functionally related to controlling the satellite) where the procedure failed. It is important each step in an automated procedure be appropriately labeled such that it provides an easily understandable overview and index (with links to more detailed labels) as to the function of that step in the procedure. This flow chart presentation, is significant and important, in supporting Satellite Controllers, analysts, and engineers, in their understanding as to what has been automatically done in a operation on the satellite, and important in understanding precisely what criteria is causing an automated procedure "difficulty" (such that it stopped executing).



P.9.B7.A6
Is there sufficient time
to send SN_SV350?
true false

P.9.B7.A6.B1
Set SEVSTAT=NOTIME

P.9.B7.A6.B2
Log the procedure is exiting
early due to insufficient time to run SN_SV350

P.9.B7.A6.B3
Goto END if there is insufficient
time to load SN_SV350

P.9.B7.A7
SN_SV350: Load Ops Paras
(N)

P.9.B7.A8
Reconfirm: Is the procedure
is running in the correct slot?
true false

P.9.B7.A8.B1
Log: Calibration has been
commanded in the incorrect slot

P.9.B7.A8.B2
SC_SV910: Place SEVIRI in
standby mode immediately at line SAFEPOSN

P.9.B7.A8.B3
Set SEVSTAT=BAD_SLOT

P.9.B7.A8.B4
Set SEVSTAT=EMG_STBY

P.9.B7.A8.B5
Call the Analyst. SEVIRI
has been placed in standby mode

P.9.B7.A8.B6
Goto END as SN_SYS51 had
a problem

Figure 1- Typical Flow Chart

VI. Consistency with FMECA

Prior to MSG launch, the satellite contractor's FMECA (failure modes effects and criticality analysis) was examined by EUMETSAT, to ensure the automated procedures were consistent with any specific operations recommendations contained within the FMECA. In particular, the possibility of an "end-of-mission" single point failure had been identified in both the contractor's Flight Operations Manuals (FOM) and in the FMECA. Hence both the calibration and full earth image procedures were designed to minimize the probability of such a failure (per the contractor's recommendations). All credible scenarios that could lead to the possible single point failure were identified, and the automated procedures coded and verified that they adequately dealt with each of these failure cases.

VII. Automated Procedure Validation

The need to conduct extensive validations was a primary consideration during procedure coding, prior to validation, in scoping how much automation should be coded into an automated procedure. As noted in section IX (Lessons learned), a balance was essential between coding a procedure for full automation (with robustness to potential failures, and a capability to handle various contingencies) vs. the time and effort required to validate (and maintain) an automated procedure.

Because the Imaging and Calibration procedures were designed to execute automatically with minimal supervision, thousands of instances/year, significant attention and effort was paid to their validation.

The validation of the procedures included testing of every single path in all of the routine and contingency procedures, together with testing of procedure reaction to a series of credible failures. To facilitate this validation, EUMETSAT procured a MSG simulator, where the simulator has a high fidelity model of the SEVIRI Instrument's functional behavior. While the engineers, who wrote the code, were heavily involved in designing the tests to validate the procedures, the 3rd party validations (by engineers who did not write the code) were performed in all cases. Typically the primary and backup subsystem engineers alternated for the implementation of the coding and validations.

The Satellite Simulator used by EUMETSAT for the MSG ran the flight software, and also contained a copy of the TMTC database for appropriate calibration curves. The simulator provided the Trainer the capability to force selectable telemetry to specific values, and also provided a capability to dynamically reconfigure the satellite model via commands input directly to the simulator. Telemetry recorded during pre-launch ground based end-to-end testing, were compared to the simulator values, and subsequently used to improve the simulator fidelity. While the simulator was never connected to flight hardware, all procedures run on the satellite were first run against the simulator, and hence the simulator fidelity was incrementally improved over time.

Operational Scenario Testing - After successful validation of individual procedures, using the high fidelity SEVIRI model in this MSG simulator, the MSG SEVIRI imaging and calibration procedures were run for weeks (24 hours/day) in a series of "unofficial" Operations Scenario Tests (referred to as "dry runs"). Anomaly reports were raised when the procedures (and simulator) had failures during this testing, and the procedures and the simulator were updated as required. In addition, Satellite Controllers were familiarized and trained with the operation of the procedures.

This "unofficial" series of tests were followed by a more formally configured "Operational Scenario Testing", again conducted for many weeks. During the formal testing further experience was gained in the operation of the procedures, and also in the training of the Satellite Controllers and engineers in the use of the procedures. Again, all control facility, database, procedure, simulator, and operator-mistake/failures were formally examined by the standard Anomaly Reporting process, and actions taken with respect to all failures. Where necessary, automated procedures were updated to minimize the possibility of repeating previously encountered failures.

VIII. Automated Procedure - User Training

Satellite Controllers, analysts, and engineers are continually trained on automated procedure operations, and are briefed with presentations on any changes and updates to specific procedures. Training sessions, including scenarios where failures are injected into the procedures, are conducted to ensure that Satellite Controllers and engineers understand the correct action that is to be taken in various failure cases.

IX. Lessons Learned

Various lessons were learned in procedure coding methods over the time frame of the MSG Operations Preparation, Ground End-to-End Testing, Operational Scenario Testing, Spacecraft Commissioning, and Subsequent Operations after the spacecraft was declared operational.

The main lessons learned were the need for robustness, while at the same time balancing the need and effort associated with validation.

The operational scenario tests injected many simulated failures, which resulted in a user (Satellite Controller, Analyst, and Engineer) demand for more automated complex procedure robustness against:

(1) TM drops,
(2) Control Facility failures (such as failed assertions, incorrect calculations, run time quality checks for slow execution),
(3) Common Satellite Controller failure reactions,
(4) Clear labeling of flow chart steps as an index into procedure code (to assist in rapid diagnosis),
(5) Top level system Alpha Numeric Display tracking of complex procedure execution.

More complex procedures result in more complex validations, and in more difficult maintenance and training. Hence a key lesson was finding a good balance, and an ongoing evaluation of the balance, between:

(1) The extent and benefit of procedure automation for hands off operation, such as high availability and reduced onsite shift monitoring (where hands off operation typically requires increased procedure complexity),
(2) The extent and benefit of automated procedure contingency capabilities for hands off operation (where contingency capabilities typically requires increased procedure complexity),

(3) The ease of maintaining a procedure (where ease of maintenance comes with procedure simplicity, and maintenance is more difficult with a more complex procedure), and
(4) The ease of training operation of a procedure (where ease of training comes with procedure simplicity, and training is more difficult with a more complex procedure).

Typically, the more “hands off” the procedure, the more complex the procedure, where complexity is often necessary in order to obtain high availability against routine ground/Control Facility “hiccups”.

For an automated procedure (that runs in a “hands off” manner) it was determined very useful to implement in the procedure:
(1) A high resilience to random and brief telemetry drops,
(2) Code with (limited) resilience to common control facility failures (such as failed parameter assertions, incorrect calculations, and run time quality checks,
(3) Code to send critical commands twice (via two independent methods),
(4) Code with (limited) reliance to common user (Satellite Controller/analyst/engineer) mistakes in handling procedure errors,
(5) Code succinct, clear, and accurate text in labeling icons/steps in flow charts. This provides a clear index into the logic and function of each step, making procedure maintenance and relatively real time analysis of failures easier,
(6) Provide more insight into the execution of “hands off” automated procedures by use of an assertable parameter in the TMTC database that displays the functional progress of various stages of a routine procedure.

For an automated procedure where an engineer or analyst will directly supervise the real time procedure execution, it was typically not necessary to code such complexity in the procedure, and the procedure could be kept very simple (limited to simple commands and simple telemetry checks).

X. Applicability to Other Missions

Experience gained from controlling the earlier First generation of Meteosat Spacecraft was used in the design of many of the procedures used in the Meteosat Second Generation (MSG) spacecraft. For example an engineer, familiar with the operation of the first generation Meteosat Spacecraft procedures, contributed to the design and coding of the MSG procedures. The principles used in these automated procedures are generic enough to be selectively applied to other missions.

In both cases (First and Second Generation of spacecraft) a similar philosophy was followed for the degree of on-shift Satellite Controller monitoring of the Control Room activities (including the automated procedure execution).

While the Imaging procedures (which executed +30,000 times/year in a “hands off” manner) had the most automation, selected techniques used within these procedures were also applied to procedures which were run with a higher degree of supervision.

Automated procedures were used for such functions as spacecraft Maneuvers, Eclipse Operation, Battery Reconditioning, Reconfiguring the spacecraft Monitoring and Reconfiguration Function, Spacecraft contingency procedures, and various levels of automated payload operation procedures. Selected aspects of the methods described within this paper were used within those procedures.

While this paper has used the Geostationary Meteosat program as the basis of its examples, similar methodology can be applied to Low Earth Orbit Spacecraft, when there is a requirement to “custom command” during a brief in time-constrained in contact period with the ground Control Facilities.

XI. Conclusions

EUMETSAT has successfully implemented a series of automated procedures for the routine commanding of the SEVIRI Instrument. Despite a very high frequency of execution (+30,000 instances/year/satellite of the imaging procedure execution, and +7,000/instances/year/satellite for the calibration procedure) there have been relatively few anomalies encountered in the use of the procedures. The extent of the automation (robustness against failure and failure contingency capabilities) was noted as being a trade off against the effort required to conduct validation, maintenance and training, Procedures requiring a high repetitive frequency of commanding were noted to benefit significantly from automation, and the methodology followed in the implementation of the repetitive SEVIRI Imaging procedures has ensured a high availability of Instrument Operation, in support of providing a resulting high availability of weather images and products to the end user.

References

Proceedings

[1]L.Schwarz, M.Williams, and J.Kugelberg, Advanced Operations Concepts of the MTP and MSG Ground Segments - SpaceOps '96, Proceedings of the Fourth International Symposium held 16-20 September 1996 in Munich, Germany. Edited by T.-D. Guyenne. ESA SP-394. Paris: European Space Agency, 1996., p.84. Retrieved 24-Sep-08 Harvard University website: http://adsabs.harvard.edu/abs/1996smog.conf...84S

[2]I.Dankiewicz., SciSys Apex (Automated Procedure EXecution) Technical Summary, SSSL/S7726/TEN/014, from SciSys Apex publicity material, 08/06/2004/. Retrieved 24-Sep-08 from SciSys Apex website: http://www.scisys.co.uk/casestudies/space/cs_apex.asp