E. Instrument Operations

With the resumption of science operations it became clear that the number of TCs required to operate each instrument would be the driver for returning to a full science mission. In collaboration with the Science Ground Segment in ESAC, it was determined which command sequences for payload operations could be combined or replaced one-for-one with OBCP equivalents. The first phase was to replace the "command intensive" switch on and switch off command sequences with single-chain OBCPs. The initial development in the high-level procedure development environment lead to inefficient coding of some commands. "Chains" of several OBCPs calling each other in sequence were therefore required to meet the 4 kilobytes size limitation for a single OBCP. These are being replaced by recoding the OBCPs in the more efficient, low-level native environment.

With all the switch on and off OBCPs in place (January 2012) full restoration of the operations of all science instruments was achieved. Phase two of this process has been to replace each instrument command sequence with more than 4 TCs (and no parsed parameters) with an equivalent 'macro' OBCP. With this in place, the total restriction on short-MTL size no longer has any significant impact on the number of instruments that can be operated in a single science pointing: simultaneous operation of 5 instruments is now possible.

For occasions where the SSMM checksum error resulted in the SSMM being set to 'not used' all OBCPs executed via load from SSMM would not execute until the SSMM was reconnected by the flight control team. This initially resulted in some instruments being left on after the failure event. The solution was to ensure that all instrument switch off OBCPs were directly executed from DMS processor RAM. Instrument switch off OBCPs have now been recoded using the more efficient low-level development environment reducing their size by a factor of 5-10 and allowing all of them to reside directly in DMS-RAM.

For ASPERA, which is generally operated for a full day (between routine wheel off-loading 'maintenance' slots) the process has been more comprehensive. The operations concept for the instrument has been redesigned from scratch and simplified into 'switch on' high-voltage enabling, operation of the various sub-instruments, disabling of the high voltages and instrument switch off. This has resulted in the development of 8 completely new OBCPs based on combination and reduction of several command sequences, with contents of up to 60 commands per OBCP. Since the High Voltage (HV) operations are safety critical for the instrument, and shall only be used if ASPERA is completely switched on, the OBCPs for HV on and HV off have been assigned separate sub-schedules on the short MTL, which are enabled and disabled from within the ASPERA switch on and off OBCPs. This protects the execution of the HV OBCPs such that switch on is only possible when ASPERA is on and HV off, and that HV switch off OBCP only executes if HV is on.

Wherever possible, to reduce the total number of 'activities' that must be produced, checked and uplinked each week, the instrument operations have been included within the Flight Dynamics activity pointings. This is only feasible where the entire instrument operations (pre-heating, configuration etc.) takes place within the 'pointing' and associated 'slews'. For some instruments such as OMEGA the duration of a full near-infrared observation (some 2.5 hours of cryogenic cooling) prevents this, but for all other 'pointed' instruments (including OMEGA visible-range observations) this has or will soon be achieved. To make this possible certain constraints on operations had to be extended, such as increasing the minimum slew duration to or from a science pointing from 10 minutes to 20, to ensure all instrument conditioning heater operations were contained within the pointing activity.

F. Ground / Mission Control System

With one command file per activity, the number of command files to uplink to the spacecraft grew considerably, from about 25 to 125 for a week. Design limitations on the SSMM also put constraints on the ordering of the files, to avoid "ghost files" where space feed by executed files is not properly released (Figure 4). This limitation means that files are to be uplinked in reverse chronological order, with the first-to-execute the last to uplink.

The manning overhead and potential for error incurred by this was great, and identified extremely quickly. An emergency patch to the ground control system was provided to load a "manifest" of which DTCFs to load, in what order, and to what file name.

An unforeseen impact on the control system was of incorrect command verification, due to the incomplete modeling of DTCFs and their interaction with the MTL model. The MCS had difficulty in dealing with the embedded Disable / Enable SSID commands at the start and end of each activity file. This lead to commands

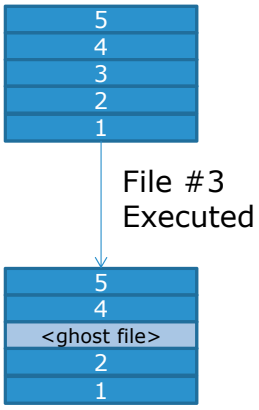

Figure 4. SSMM Ghost Files

Executing a DTCF causes it's deletion, but the space cannot be recovered until the files "above" it (4 & 5) have also been deleted.

being incorrectly marked as deleted, or disabled or any number of other states other than correctly verified. Mars Express exclusively uses report-based acknowledgement for commanding, and failure reports are still flagged and raise alarms correctly, giving an alternative to the command verification model for failure identification. Moreover the slicing of activities in self-contained files shifts the focus from commands to files. A correction to the predictive and historical model of the on-board command status is under validation.

G. Ground / Mission Planning

As well as creating the activity files themselves, a tool was needed to schedule the execution of the activities and generate the trigger commands to execute the right DTCF at the right time. Associated to this is the creation of the Manifest file, so that the activity files can be loaded into the SSMM with a predefined file name, for the trigger command to then call.

The timing of the trigger commands was critical. Too early, and valuable MTL space is blocked for longer than necessary. Too late, and the commands would be rejected as past their execution time. Furthermore, an activity can only be loaded once the previous one of the same type has been fully executed from the MTL, to avoid interference from the Disable SSID command required for file-completeness protection.

An easy-to-check rule of 10 minutes before the first command of an activity was adopted for the scheduling of the triggers. The DMS is only capable of executing one command file at a time, so the triggers also needed to be scheduled so as not to overlap each other.

An FCT-developed generic Finite State Machine already existed, which formed the basis of the new trigger scheduling tool, named "DANIELS" (Figure 5), which ingests the command files generated by the MPS and calculates the optimal time for the trigger command to execute each one, based on some simple rules, ensuring that each one is scheduled about ten minutes before the first command of the activity. The DMS is only capable of executing one DTCF at a time, so DANIELS also ensures that no trigger or the resultant execution overlap. In addition to the trigger scheduling, a collection of checklists and reports are generated to help with product checking and uplink tracking. It is also responsible for the creation of the Manifest file which instructs the MCS to uplink the correct command files in the correct order with the correct file names. The re-use of existing tools and a rapid prototyping development approach meant the new tool could be adapted on a weekly (or more frequent!) basis as the ops. concept evolved and expanded.

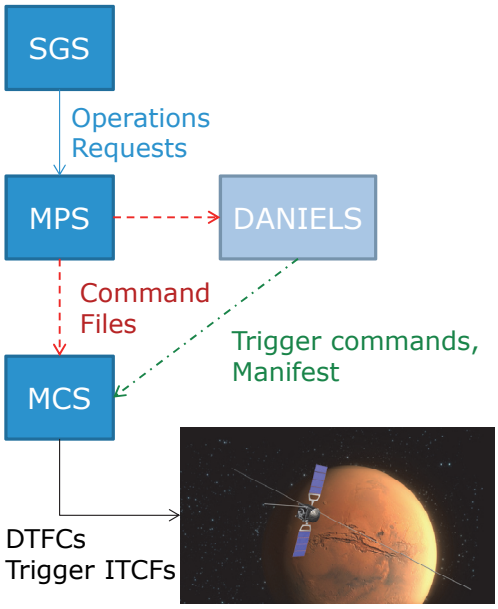

Figure 5. FAST Mission Planning Concept

After the MPS has processed the requests from SGS, the command files are grouped by "activity type" and their loading scheduled on a just-in-time basis. These trigger commands are passed to the MCS for uplink, which is scheduled according to the "Manifest" file also generated by DANIELS.

Photo: ESA, C. Carreau

Ultimately the functionality of the ad-hoc tool will be replaced by the integration of additional functions into the core mission planning system, but for now retains a critical role in the FAST Ops. concept. The "MPS 2012" system has already taken over the process of adding the disable/enable SSID commands. The "upstream" mission planning tools[4] are otherwise unaffected.

H. Ground / Command Product Checking Tools

With roughly one hundred files to check per week and many constraints to check, additional operations support tools were created. These have ranged from one-off shell scripts to modify generated command products until the formal MPS could be updated, to more complex modeling of the execution of activities and trigger commands. The generic Finite State Machine core has been re-used for some of these tools, as most of the checks fall into the domain of state checking ("only allow transition X if model Y is in state Z...").

New tools have been written to automate the checking of commanding products as much as possible, following the general automation principles for MEX[5]. DANIELS performs checks on overlaps between triggers and activities, and also models the MTL fill level to ensure each DTCF can be fully contained within the short MTL (otherwise the

Figure 6. FAST related Checking & Uplink Verification Tools

Timeline view, MTL fill level and Product Checking & Uplink Confirmation tools give visual feedback to the operations engineers and automate much manual checking.

remaining commands would be lost). On the principle that two independently written tools are unlikely to have the same bugs, these checks are performed by an additional tool run by the spacecraft operations engineer responsible for that week's command delivery (Figure 6).

The necessity for new tools is driven by change in ops. concept which brought in new safety constraints that had to be adhered to, such as only one DTCF executing at a time. MEX's existing tool infrastructure[6] (generic timeline tool and generic finite state machine engine) meant that only minor modifications were necessary to integrate new rules meaning that the main difficulty was in defining what needed to be checked to ensure safety of FAST ops.. The key goal at all times was also to ensure no less checking than had been done previously was being applied.

I. Ground / Spacecraft Monitoring

New monitoring tools had to be created to monitor progress of FAST operations (and any possible failures). These new tools compliment the checking tools mentioned above, to ensure that what was planned was executed. The first step was to create definitions of what signs would indicate a problem with FAST operations: failed DTCF execution events, SSMM file count not as expected, SSID status not as expected, and so on. Due to the just-in-time nature of the new ops. concept, these checks had to work on the earliest possible basis to be effective, rather than waiting for routine monitoring. Extra diagnostics added on-board (such as various SSMM packets diagnostic report packets) at the start of each pass to facilitate this, along with Out-Of-Limit sets on the routine TM to monitor the process of the operations and alert the spacecraft controller to a problem as soon as possible.

V. Summary & Conclusions

The most significant conclusion is that it is entirely possible to run the full science mission using only 117 TCs. MEX has already reached 100% of science operations, and future planning / OBCP developments hold much scope for increasing the science operations further still (see Figure 7).

By implementing a just-in-time and transactional loading scheme, combined with careful planning on the ground, it was possible to work around the transient SSMM problems. Importantly, it is still necessary to rely on the correct functioning of the SSMM, but transient problems cannot spread beyond the initial impact.

It has been demonstrated that by judicious use of existing spacecraft capability, software patches are not immediately required. While the retry patch may allow resumption of the nominal MTL, we are rapidly reaching a point where there is no value to doing so. Also the new FAST approach brings additional benefits in terms of routine operability (more flexible via the activity granularity), of potential for automation (more pre-programmable) and even safety (covers practically all possible failures that could come from the SSMM). That being said, the patch remains a goal, rather as a backup solution than to solve the already well-solved problems that occurred in 2011, and to provide more options in the future, should further degradations or constraints arise on the aging Mars Express.

A. Mission re-habilitation thanks to FAST – Performance Figures

The Mars Express mission shows quite some dynamics in its performance figures along time even in nominal phases due to the variability of the conditions (distance Mars-Earth impacting the data return, distance Mars-Sun impacting the energy available, Mars surface illumination impacting the set of operated instruments, presence of eclipse or radio-occultations, etc.). However the multi-year average performance can be summarized by two key figures that constitute a reference (100%) normally achieved or exceeded: 4.3 observations per 7-hour orbit (measure of operations density); and 1.5 science pointing per orbit (measure of operations diversity).

Figure 7, normalized with respect to the multi-year average, synthetizes the loss of performance following the SSMM problems in August-October 2011, the recovery by progressive introduction of the new FAST method from November 2011 (one instrument at a time, however saving the North Polar Cap campaign by the radar) until January 2012, and the stability thereafter.

The speed at which the new operations concept was conceived and implemented is remarkable. To put it into perspective, a similar 3-month dip in science operations occurs once every two years due to solar conjunction severing communications with the spacecraft. The new ops. concept involved developing, testing and operationalizing new ground software, onboard software and commissioning units in Martian orbit (SSMM-B and HRSC-B) that had lain dormant since launch.

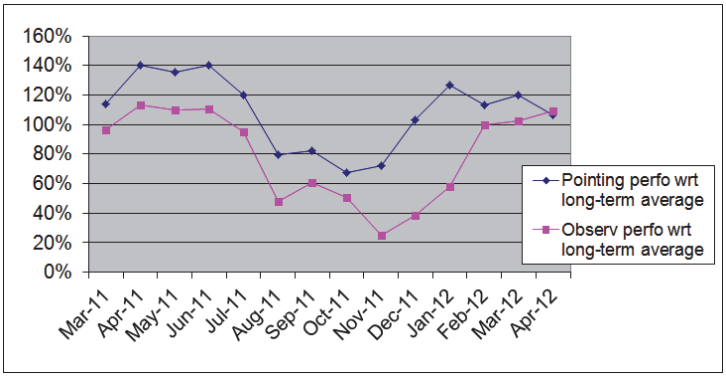

Figure 7. Performance of MEX Before & After SSMM Anomaly

Actual observation and pointing performance with respect to the long-term mission average, in terms of numbers of each successfully performed by the spacecraft. The big dip from September to November is due to the SSMM anomaly halting science operations.

It should also be noted that by implementing the FAST approach, MEX has become significantly more robust to SSMM problems (the cause of most of MEX's 26 safe modes since launch). Such an anomaly no longer causes a safe mode and three days' of mission loss, but instead a 3-second data gap while the onboard protections resets and restores the link (using a planned event-driven recovery OBCP). The FAST concept ensures that such a delayed SSMM reconnection is always safe, from spacecraft commanding perspective. This is a 100 000-fold reduction in mission loss due to SSMM anomalies, resulting in increased science return and decreased stress on the FCT.

B. Lessons Learned

Lessons to have come out of this experience affect all aspects of spacecraft operation. As always when triggered by a hardware anomaly, importance of software in spacecraft operations for implementing workarounds and reconfigurations has been confirmed.

It was surprising to find that the DMS software had apparently little robustness to transient communication errors between units. An explanation may be that the existing "too quick" retry mechanism relies on performance requirements as stated in the specification, but that the units involved may just marginally fulfill, leading to interlocks and failures on a few occasions – by definition, the ones that we see. It is certainly recommendable for future onboard software to provide a very solid functionality for "retry" if it relies on communication across a bus or network. A software patch will correct this for MEX in due course.

Development of ground tools, from the formal core Control and Planning Systems to informal checking tools and a somewhat grey-area in between, has been key to the successful and speedy return to full science. The ability to quickly prototype new concepts and approaches in-house certainly hastened the return to science, and the proven concepts will feed back into the formal software. Close support and flexibility from external software support teams also contributed greatly toward the success.

Lastly, having an in-house development capability for OBCPs was vital. MEX no longer has industry support for onboard software developments, and having the development environment and the skills available to use it was a critical enabling factor.

C. Future Work

Further development of OBCPs is the main focus of the future work. It falls into two categories: command volume reduction and performance enhancement.

The smaller the number of commands required to perform an activity the better, as it allows for more complex operations for the same number of TCs, and more flexibility in scheduling them, leading better mission return for the same operational effort. Furthermore, the reduction of the number of TCs overall optimizes the space/ground command link by requiring a shorter uplink time.

The other side of the OBCP coin is to enhance the performance of the spacecraft. This can be in the frame of robustness / error handling, or utilizing onboard autonomy to permit more effective use of the spacecraft.

These are not necessarily mutually exclusive goals. It can happen than an OBCP to manage an operation might also do so more effectively, as well as in fewer TCs, as it can react much faster than the ground operators can.

Finally, we are considering the use of OBCPs to enhance the abilities of the onboard software specifically for FAST. The OBCP environment on MEX is sufficiently powerful to enable a “second MTL” to be run, via an OBCP, to schedule the execution of activity DTCFs. This would remove the trigger commands from the short MTL, and free up about 30 commands (25% of the short MTL) for more functional commands, e.g. allowing more complex instrument operation. Additionally, it would allow the uplink of all triggers in one go, rather than spread throughout the week, to match the once-a-week loading of the activity files themselves, and be a significant step towards the automation, in the control room, of all other routine passes.

Appendix A
Acronym List

APR	Array Power Regulator
AOCS	Attitude and Orbit Control System
AOCMS	Attitude and Orbit Control Management System
AOS	Acquisition Of Signal
ASPERA	(MEX Science Instrument) Energetic Neutral Atoms Analyzer
DANIELS	Delayed Activity Numbering, Invoking, Evaluating and Listing Software
DMS	Data Management System
DTCF	Delayed-execution TC File
ESA	European Space Agency
ESAC	European Space Astronomy Centre
ESOC	European Space Operations Centre
ECSS	European Cooperation on Space Standardization
FAST	File-based Activities on Short Timeline
FCT	Flight Control Team
FDIR	Fault Detection, Isolation and Recovery
FSM	Finite State Machine
HRSC	(MEX Science Instrument) High Resolution Stereo Camera
HV	High Voltage
IR	InfraRed
ITCF	Immediate-execution TC File
MARSIS	(MEX Science Instrument) Sub-surface Sounding Radar Altimeter
MCS	Mission Control System
MEX	Mars Express
MPS	Mission Planning System
MTL	Mission Time Line
OBCP	Onboard Control Procedure
OMEGA	(MEX Science Instrument) Visible and Infrared Mineralogical Mapping Spectrometer
PFS	(MEX Science Instrument) Planetary Fourier Spectrometer
RAM	Random Access Memory
SGS	Science Ground Segment
SPICAM	(MEX Science Instrument) Ultraviolet and Infrared Atmospheric Spectrometer
SSID	Sub-Schedule Identifier
SSMM	Solid State Mass Memory
TC	Telecommand
TM	Telemetry
TT&C	Telemetry, Tracking and Commanding
TWTA	Travelling Wave Tube Amplifier
WOL	[Reaction] Wheel [Momentum] Off-Load
X-TX	X-Band Transmitter

Appendix B
Glossary

Apocenter	The point of farthest excursion between two bodies in an elliptical orbit (also known as apoapsis).
Mission Time Line	An onboard schedule of commands to execute at a given time
Pericenter	The point of closest approach between two bodies in an elliptical orbit (also known as periapsis).
Short MTL	An implementation of the MTL purely within DMS RAM, which is unaffected by SSMM errors.
Solid State Mass Memory	12 Gigabit onboard memory unit, used to store science, telemetry and commanding data.
Sub-Schedule	Commands within the MTL can be assigned to a Sub-Schedule, which can then be used to disable or enable the whole sub-schedule with one command.
Trigger Command	An "Execute Delayed TC File" command, scheduled in the MTL to "trigger" the execution of a specific TC file which loads the contents into the MTL for later execution.

Acknowledgments

We are grateful for the effort, cooperation and flexibility of the entire Science Ground Segment team at ESAC, Spain, the various instrument teams, and also the software support teams at ESOC.

References

[1]M. Shaw, A. Moorhouse, M. Denis, R. Porta, Z. Mounzer, "File transfer, Mass Memory and Mission Time Line – providing spacecraft remote commanding at Mars", *AIAA SpaceOps. Conference Proceedings 2006,* Rome.

[2]P. Choukroun, M. Denis, P. Schmitz, M. Shaw, "Evolving ESA Mars Express Mission Capability with On-Board Control Procedures", *AIAA SpaceOps. Conference Proceedings 2010,* Huntsville.

[3]D. Lakey, et al. "Multi-Mission End-to-End OBCP Configuration Control", *AIAA SpaceOps. Conference Proceedings 2012,* Stockholm.

[4]E. Rabenau, M. Denis, S. Peschke, "Mars Express Mission Planning – Expanding the Flight Box in Flight", *AIAA SpaceOps. Conference Proceedings 2010,* Huntsville.

[5]M. Shaw et al., "Mission automation and autonomy: In-flight experience derived from more than 8 years of science operations in orbit about Mars", *AIAA SpaceOps. Conference Proceedings 2012,* Stockholm.

[6]T. Ormston, D. Lakey and M. Denis "Product Verification on Mars Express – Routine Validation to Ensure Routine Success", *AIAA SpaceOps. Conference Proceedings 2012,* Stockholm.