AN ANALYSIS OF CAUSATION IN AEROSPACE ACCIDENTS

Kathryn A. Weiss, Nancy Leveson, Kristina Lundqvist, Nida Farid and Margaret Stringfellow,
Software Engineering Research Laboratory, Department of Aeronautics and Astronautics,
Massachusetts Institute of Technology, Cambridge, MA

Abstract

After a short description of common accident models and their limitations, a new model is used to evaluate the causal factors in a mission interruption of the SOHO (SOlar Heliospheric Observatory) spacecraft. The factors in this accident are similar to common factors found in other recent software-related aerospace losses.

Introduction

Accident models underlie all efforts to engineer for safety; they are used to explain how accidents occur. An underlying assumption, therefore, is that accidents follow common patterns and are not simply random events. The explanations of the etiology of accidents embodied in accident models forms the basis for investigating accidents, preventing future ones and determining whether existing systems are suitable for use.

When investigating mishaps, accident models help identify which factors will be considered; the models impose patterns on an accident and thus influence both the data collected and the factors identified as causative. Hence, models are a way to organize data, setting priorities in accident investigations that may either narrow or expand the consideration of certain factors. The most common model used is a simple chain of events model, but such a model is inadequate for explaining accidents in complex systems. Adding hierarchical abstraction reduces some of the limitations.

Chains of Events

The most common accident models include multiple events related by a forward chain over time. The events considered almost always involve some type of component failure, human error or energy-related event. There may be other relationships represented by the chain in addition to a chronological one, but any relationship is almost always a direct, linear one represented by the notion that the preceding event or condition must have been present for the subsequent event to occur.

Various events in the chain may be given labels such as proximate, primary, basic, contributory or root cause. Unsafe conditions may be included in the chain or may be represented as factors that link events. Whether the beginning point is an event or a condition simply reflects an arbitrary decision about where to stop the backward chaining. Although the first event in the chain is often labeled the initiating event, the selection of an initiating event is arbitrary and previous events and conditions could always be added. Stop rules are not usually formulated explicitly and involve pragmatic and subjective decisions, which depend on the objective of the analysis.

Subjectivity is not only found in the selection of events and conditions, but also in the links between them. The same event can give rise to different types of links, depending on the mental representations the analyst has of the production of this event. The selection of a linking condition will greatly influence the cause ascribed to the accident, yet many are usually plausible and each fully explains the event sequence.

The countermeasures to prevent accidents considered as chains of events usually involve either removing the events or conditions or adding enough simultaneous conditions or events that the likelihood of the chaining factors being realized is very low. Thus, the emphasis is on eliminating events or on breaking the accident sequence.

Hierarchical Models

If the goal of accident modeling is to better understand accident processes to determine how to engineer safer systems, then eliminating or manipulating indirectly related factors is necessary.

Achieving this goal requires that the accident model must not limit our consideration of the factors affecting the loss event.

In this paper, a model that describes accidents using three levels of hierarchical abstraction is used, each level providing a different model of the accident. Level 1 describes the mechanism of the accident – the chain of events. Level 2 includes the conditions or lack of conditions that allowed the events at the first level to occur. At this second level, the causes may be over specified; not all conditions may have to be met before the accident will occur.

The factors at the third level are often referred to as the root causes or systemic factors of an accident. Systemic factors affect general classes of accidents; they are weaknesses that not only contributed to the accident being investigated but also can lead to future accidents. Responses to accidents tend to involve fixing only a specific causal factor while leaving the more general or systemic factors untouched. Blame is more likely to be placed on operator errors or on specific component failures than on such systemic factors as poor training, inadequate risk management or flaws in the organizational culture. The hierarchical model can be used to extend prevention strategies so that future accidents resulting from similar systemic factors do not occur.

Limitations in Using Accident Reports

Before evaluating a recent aerospace accident report using the hierarchical model, it is important to understand the limitations of such reports and the difficulties inherent in learning how to prevent accidents from them. When technology changes rapidly or when radical new designs are introduced, previous accident data may be irrelevant. In addition, the data gathered by investigators may involve filtering and subjectivity and the collection process itself can taint the information acquired, thus limiting its applicability in preventing similar accidents.

Filtering

Everyone involved in an accident investigation rarely perceives all the causes as identical. Such conflicts are typical in situations that involve

normative, ethical and political considerations on which people may legitimately disagree. One group may consider some conditions unnecessarily hazardous; yet another may see them as adequately safe and necessary. In addition, judgments about the cause of an accident may be affected by the threat of litigation or by conflicting interests.

Examining physical evidence may not be any less subjective. Filtering and bias in accident reports can occur due to individual interpretations of events, both by the individuals involved in the events and by the accident analysts. Individuals may be unaware of their actual goals and motivation or may be subject to various types of pressures to reinterpret their actions. Their own mental models or additional goals and pressures may influence explanations by analysts not involved in the events.

Oversimplification

A second trap in identifying accident causes is oversimplification. Out of a large number of necessary conditions for the accident to occur, one is often chosen and labeled as *the* cause, even though all the factors involved were equally indispensable to the event's occurrence. A condition may be selected as the cause because it is the last condition to be fulfilled before the effect takes place, its contribution is the most conspicuous or the selector has some ulterior motive for the selection. Although it is common to isolate one condition and call it *the* cause (or the proximate, direct or root cause) and the other conditions contributory, there is no basis for this distinction. Most accidents involve a variety of events and conditions; identifying only a single factor as the cause can be a hindrance in preventing future accidents.

One reason for the tendency to look for a single cause is to assign blame, often for legal purposes. Blame is not an engineering concept; it is a legal or moral one. Usually there is no objective criterion for distinguishing one factor or several factors from the other factors that make up the cause of an accident. In any system where operators are involved, a cause may always be hypothesized as the failure of the operator to step in and prevent the accident. Virtually any accident can be ascribed to human error in this way. Even when operator

error is more directly involved, considering that alone is too limiting to be useful in identifying what to change in order to increase safety most effectively. The less that is known about an accident, the more likely it will be attributed to operator error. Thorough investigation of serious accidents almost invariably finds other factors.

All human activity takes place within and is influenced by the physical and social environment in which it takes place. Operator error cannot be understood or prevented without understanding the environmental factors that influence those actions. It is often very difficult to separate design error from operator error. In highly automated systems, the operator is often at the mercy of the system design and operational procedures. Because the role of operator error in accidents is so important, it must play a central role in any comprehensive accident model, but should not become the only factor considered. On the other hand, considering only immediate physical failures as the causes of accidents can allow latent design errors to go uncorrected and to be repeated. With the increasing role of software in complex systems, concentrating on physical failures alone and the use of redundancy to prevent them will become increasingly ineffective.

Large-scale engineered systems are more than just a collection of technological artifacts. They are a reflection of the structure, management, procedures and culture of the engineering organization that created them and the society in which they were created. Accidents are often blamed on operator error or equipment failure without recognition of the systemic factors that made such errors and defects inevitable. The causes of accidents are frequently rooted in organizational culture, management and structure. These factors are all critical to the eventual safety of the engineered system. Oversimplifying these factors limits the ability to prevent them.

The SOHO Accident

SOHO, or the SOlar Heliospheric Observatory, is a joint effort between NASA and ESA to perform helioseismology and monitor the solar atmosphere, corona and wind. ESA was responsible for the spacecraft procurement, final integration and testing. NASA was responsible for the launcher,

launch services and the ground segment system to support pre-launch activities and in-flight operations. The SOHO spacecraft was built in Europe by an industrial team headed by Matra Marconi Space (MMS).

SOHO was launched on December 2, 1995, was declared fully operational in April of 1996 and completed a successful two-year primary mission in May of 1998. It then entered into its extended mission phase. After roughly two months of nominal activity, contact with SOHO was lost June 25, 1998 [1]. The loss was preceded by a routine calibration of the spacecraft's three roll gyroscopes (labeled A, B and C) and by a momentum management maneuver.

The spacecraft roll axis is normally pointed toward the Sun, and the three gyros are aligned to measure incremental changes in the roll attitude. Gyro calibrations are performed periodically to accurately determine the draft bias associated with each of the three roll axis gyros. Once these biases are determined, the bias values are uplinked to the spacecraft computer where they are subtracted from the gyro measurement and used by the Attitude Control Unit (ACU) to determine the actual motion of the spacecraft and to maintain the correct orientation. The gyros are not required during most of the mission: they are used only for thruster-based activities such as momentum management, Initial Sun Acquisition (ISA) and Emergency Sun Reacquisition (ESR).

Momentum management, performed approximately every two months, maintains the reaction wheel speeds within prescribed limits. All three roll gyros are intended to be active for momentum management maneuvers. Emergency Sun Reacquisition (ESR) is a hard-wired, analog, safe-hold mode that, unlike the other control modes, is not operated under the control of the ACU computer. It is entered autonomously in the event of anomalies linked to attitude control. In this mode, a hard-wired control law using thrusters, sun sensors and Gyro A keeps the spacecraft pointed to the Sun with no roll. ESR is part of the Fault Detection Electronics, which uses Gyro B to detect excessive roll rates.

Once the spacecraft has entered the ESR mode, a recovery sequence must be commanded and executed under ground operator control to

proceed to the Mission Mode where science experiments are performed. The first step in this recovery sequence is the Initial Sun Acquisition (ISA) mode in which the ACU computer fires spacecraft thrusters to point the spacecraft toward the Sun under the guidance of an onboard Sun sensor.

Chain of Events Model

In the following chain of events, events were added to the proximate event chain (events immediately preceding the loss) in order to better understand the accident. The added events are labeled E0-n. While a proximate event chain is useful in understanding the physical accident mechanism, identifying all the causal factors, particularly those associated with management and system design, requires examining non-proximate events that may have preceded the accident by a large amount of time.

E0-1: A deficiency report is written in 1994 stating that the SOHO control center was unable to display critical data in a convenient, user-friendly format, but the deficiency report was never resolved.

E0-2: In late 1996, a decision is made to minimize the operation of gyros when not necessary by: (1) despinning the gyros between the end of calibration and the start of the momentum maneuver and (2) calibrating gyros only every six months, not at each maneuver.

E0-3: On February 3, 1997 the Flight Operations Team modifies the predefined, stored sequences of ground-generated commands.

E0-4: The modified procedures are introduced into operations through a Mission Operations Change Request (MOCR) dated March 3, 1997. (The term "change request" must mean something different in NASA procedures as more common usage is for it to refer to a request before a change is made, not after.) No one outside the flight operations team was made aware of the change.

E0-5: In April 1997 and September 1997, the modified procedures are used to calibrate the gyros 24 hours before a momentum management maneuver (as was the usual procedure) without incident.

E0-6: An emergency sun reacquisition (ESR-3) is triggered by ground software problems in March 1998. A shortcut in the recovery from ESR-3 led to ESR-4. A resulting recommended comprehensive review of the software and procedures had not been implemented before the accident.

E0-7: A decision is made to compress the timeline of the operational procedures for momentum management, gyro calibration and science instrument calibration into one continuous sequence. The previous process had been to wait until the day after gyro calibration to begin the momentum management procedures.

E0-8: About a week before the accident, NASA is unable to independently substantiate the planned timeline of events in their simulator. Analysis of this simulation was still being evaluated as the proximate chain of loss-related events began.

E1: On June 24, 1998, a routine gyro calibration is performed using the compressed timeline.

E2: Following gyro calibration, Gyro A is deactivated in order to conserve its life while Gyro B and Gyro C remain active.

E3: The on-board software function that activates Gyro A, which is needed for ESR, is not enabled, and Gyro A remains deactivated.

E4: A momentum management maneuver takes place.

E5: Gyro B, which is used for fault detection, is incorrectly left in its high gain setting.

E6: On-board fault detection (which uses Gyro B for anomalous roll rate detection) triggers ESR-5 at 7:16 PM EDT after the incorrect gain leads to calculating a roll rate 20 times greater than the actual roll rate.

E7: As specified by the ESR design, the gyros are reconfigured such that Gyro A replaces Gyro C as the roll gyro used for the ESR thruster-based control mode, while Gyro B remains configured as the fault detection gyro.

E8: The high-gain setting of Gyro B is detected and corrected by ground operations. However, Gyro A's despun status is not detected.

E9: The attitude control system shifts to ISA mode as part of the normal ESR-5 recovery sequence and

begins integrating the gyro drift rate bias associated with the still despun Gyro A.

E10: After 15 minutes, the roll thrusters are fired to null the apparent but non-existent roll attitude error, resulting in a high roll rate. Although the spacecraft is Sun-pointing within nominal limits and has a power-positive and thermally safe attitude, the state of the spacecraft is precarious at this time: it has an anomalous roll rate and is depending on a deactivated gyro for roll control in both ESR and ISA modes.

E11: At 10:35 PM EDT, roughly one minute after the roll thrusters are fired, the roll rate is sufficiently high to trigger fault detection using the corrected Gyro B and ESR-6 is started.

E12: The flight operations team decides that Gyro B must be faulty because its output disagrees with Gyro A and therefore Gyro B is deactivated. This eliminates fault detection capability using Gyro B.

E13: As part of ESR-6, Ground Operations again commands the spacecraft to ISA mode. The attitude control system fires the roll thrusters in an attempt to null the attitude error associated with the electrical rate bias term of the despun Gyro A.

E14: The roll rate keeps increasing because Gyro B used by the fault detection electronics is turned off.

E15: The increasing roll rate results in pitch and yaw Sun-pointing errors that exceed a prescribed limit of five degrees, resulting in ESR-7 at 12:38 AM EDT.

E16: The spacecraft attitude diverges with resulting loss of attitude control, power and thermal control.

E17. Loss of telemetry occurs at 12:43:56 AM EDT, June 25, 1998.

Hierarchical Model

The hierarchical model adds two levels to the Level 1 basic accident chain above: (a) the Level 2 conditions enabling the events at Level 1 to occur and (b) Level 3 systemic factors, which are more general problems that can lead to similar but non-identical accidents in the future.

Level 2: Conditions

C1: For diagnostic purposes, SOHO was designed to store within its on-board computer the last three telemetry frames that precede entry into the safe mode. From this, the operators could have determined the status of the gyros. No information is provided in the report about why the deficiency report was not resolved. However, the feature was included in the new Mission Operations Center, which was still under testing at the time of the loss. (E0-1)

C2: The flight operations team modified the ground operations procedures as part of a ground systems reengineering effort to reduce operations costs for the SOHO extended mission, streamline the operations, minimize science downtime and conserve gyro life. Though some of these modifications were made at the request of the SOHO Science Team, they were not necessarily driven by any specific requirements changes. (All Events)

C3: Conservative use of gyros is important because their life is limited. Originally, gyro calibration was performed before each maneuver requiring thruster use, which occurred every six to eight weeks. The calibration took place 24 hours in advance of the maneuver and the gyros were left running from calibration start until the end of the maneuver, a period that spanned several days.

In late 1996, after about a year of operations and when the SOHO mission extension was under discussion, concern was raised that the gyros were being used more than expected. A European satellite, SAX, had experienced gyro anomalies. It was decided to minimize the usage of the gyros and avoid operating them when not necessary. (E0-2, E0-3)

C4: Gyro use and calibration depends on five predefined sequences of commands: IRU-WAKE activates the three roll gyros and disables the function that reactivates Gyro A at ESR triggering; A-CONFIG-1 and A-CONFIG-2 configure the gyros for the two calibration phases; A-CONFIG-N configures the gyros back to their usage mode for maneuvers; IRU-REST despins and switches off Gyros B and C, despins and puts Gyro A in warm standby, and re-enables the software function that respins the standby Gyro A when an ESR is triggered.

Three command sequences were modified: IRU-WAKE, IRU-REST and A-CONFIG-N. IRU-

WAKE and IRU-REST previously turned on or turned off, respectively, all three gyros. In this change, they were modified to be more flexible and allow turning on or off individual gyros as required.

In addition, a new function was introduced into A-CONFIG-N to despin Gyro A but, unlike IRU-REST, it erroneously did not reenable the software function that respins Gyro A when entering an ESR. The SOHO User's Manual calls for use of IRU-WAKE and IRU-REST for gyro management. Therefore, there was no reason to introduce a new function into A-CONFIG-N to despin Gyro A: IRU-REST should have been used all the time. (E0-3)

C5: The procedure change was discussed between the flight operations team and ESA/MMS personnel. Through e-mail exchange, the MMS resident engineer communicated that each time Gyro A is despun, the automatic software function "Gyro Setting at ESR" must be re-enabled. (E0-3)

C6: A Mission Operations Change Request (MOCR), which introduced the modified procedures, is an internal flight operations team document not normally distributed to NASA, ESA or MMS. No one outside the flight operations team was made aware of the introduction of the changed procedures into operations. (E0-4)

C7: The first two gyro calibrations after the February 1997 changes were introduced used the modified IRU-WAKE and IRU-REST command sequences but not the modified part of A-CONFIG-N, which was not needed. (E0-5)

C8: The software and procedures were not reviewed after ESR-3 and ESR-4 because higher priority had been assigned to other tasks. (E0-6)

C9: The flight operations team had an aggressive operations plan scheduled from the morning of June 24th through June 29th that was driven by Deep Space Network scheduling and science planning. This ambitious plan included the calibration of three gyros, momentum management, a yaw maneuver that exceeded previously established positional offset bias constraints, a 24-hour roll maneuver, phased reaction wheel maintenance, a station keeping maneuver and the loading of a star sensor software patch. The plan was to execute this timeline using the SOHO core team with no augmented staff. The planned activities were

intensive and there was no contingency time built into the schedule. (E0-7)

C10: The plans for the June 24, 1998 calibration were originally the same as the two previous times the new procedures were used, but were changed because of the Deep Space Network scheduling problem. It was decided to perform wheel momentum management right after gyro calibration without waiting the usual day between the two procedures. In this case, it was not necessary to despin any of the gyros, but the updated script for the day directed the flight operations team to despin Gyro A using the option implemented in the new A-CONFIG-N procedure. This option had never been used before. (E0-7)

C11: Many operational procedures are grouped to minimize the impact on science downtime. Previously the grouped operational procedures had been conducted in discrete blocks, each executed during a 12-hour shift. The continuous sequence in the compressed timeline required a new script and the use of paths within the modified command procedures for the first time. (E0-7, E1)

C12: Simulation was used to validate the ambitious timeline for the week, but the NASA simulation results differed from those obtained in an ESA simulator run and indicated that problems existed in the planned timeline. Analysis of the differing simulation results continued as the timeline execution was in process. This, in itself, indirectly affected the accident scenario because the technical support staff was distracted by the on-going simulation evaluation rather than focusing on the spacecraft recovery efforts. (E0-8)

C13: The simulator had not been updated with all changes to SOHO's on-board software. (E0-8)

C14: The new script used the new option implemented in A-CONFIG-N to despin Gyro A instead of IRU-REST. This option had never been used before. (E3)

C15: The software enable function had not been included as part of the modification to A-CONFIG-N due to a lack of system knowledge of the person who modified the procedure. (E3)

C16: The incorrect gain for Gyro B was due to an error in another predefined command sequence not the one that failed to reactivate Gyro A. No other

information is provided in the accident report about the source of this error. (E5)

C17: The operations script specifically states that Gyro A should be spinning upon entry into safe mode and instructs the operator to evaluate the three telemetry frames that had been stored prior to the anomaly before proceeding toward recovery. A deficiency report had been written 4 years earlier involving this capability to read the telemetry frames but never resolved (see C1). (E8)

C18: Because the functionality of A-CONFIG-N had been changed and not effectively communicated, a casual review of a script comprised of procedure names would not have indicated that Gyro A had been spun down. (E8)

C19: Operations were being conducted from a new integrated Mission Operations Center (IMOC), which was still under testing. The newly configured IMOC included the feature that showed the telemetry frames in such a way that the despinning of Gyro A should have been detected. The flight operations team was in the new IMOC when the first safe-mode entry (ESR-5) was triggered. However, an IMOC-related ground system software change caused a reaction wheel to be commanded to an incorrect speed and the frozen data was not displayed. After ESR-5, the flight operations team retreated to the old SOHO control center. (E8)

C20: After ESR-5, the attention of one of the key technical experts present was diverted from the spacecraft emergency situation by a request to uplink commands to an instrument to maintain thermal balance. The main focus of the operations team was on returning to the challenging timeline to minimize science downtime. (E8 to E17)

C21: Due to the compressed timeline, the ESA technical support manager, the MMS engineer and the flight operations team did not have the time available to analyze the results of the gyro calibrations. (E8)

C22: Recovery after ESR-3 and ESR-4 had been accomplished without long-term spacecraft impact. The report concludes that this success led to overconfidence by the operations team in their ability to recover from an ESR and a lack of appreciation of the seriousness of safe mode entries. Perhaps as a result, in ESR-5 and ESR-6

the operations team did not take advantage of the 48 hour minimum safe mode design and initiated recovery almost immediately after each of the two emergency safe mode entries that occurred prior to the loss of the spacecraft. (E9, E14, E15)

C23: The second safe mode trigger (ESR-6) occurred while the MMS engineer was trouble-shooting discrepancies between NASA and ESR simulator results for the upcoming science maneuver, and responding to a science investigator's need to service his instrument. These caused a distraction; yet no one directed that the plan should be aborted until all of the problems could be better understood. In their haste to restore the spacecraft to performing science as quickly as possible, inappropriate decisions were made. This type of perseveration to plan is common in accident scenarios and is a well-known cognitive psychology phenomenon. (E11)

C24: The ground control personnel were unaware of the anomalous roll rate or the deactivation of Gyro A. The operations team did notice that Gyro A indicated zero roll rate while Gyro B indicated a variable non-zero rate. These discrepancies were not checked with other telemetry points from real time or history data. For example, they did not notice the lack of correlation between the thruster firing activity and variations in Sun sensor data and the continued zero rate error indication of Gyro A. The MMS engineer and the flight operations team mission manager concluded Gyro B had to be shut down. (E12)

C25: Standard procedure requires a Material Review Board (MRB) review before such a critical action as shutting down Gyro B declaring a key component failed can be taken. The MRB would have provided a formal process for senior management and engineering staff to review and decide on the risks involved. An MRB was not convened. The accident report does not suggest the reason for this. (E12)

C26: The gyroscopic cross-coupling torques caused by pitch and yaw thruster firings and the absence of true roll rate indications led to instability of the ESR controller. (E16)

C27: It is not possible to determine whether the loss of telemetry was due to insufficient power or a loss of communication link caused by spacecraft

attitude. It was later realized that three of four battery discharge regulators were disconnected from the bus. This condition had occurred several months before but nobody had noticed this change in the spacecraft configuration. The limited access to battery discharge current that resulted may have limited the duration of the telemetry transmission in the minutes after the loss of attitude control. (E17)

Level 3: Systemic Factors

In a previous report, the systemic factors involved in five spacecraft accidents (Ariane 501, Challenger, Mars Climate Orbiter, Mars Polar Lander and Titan IVB-32/Milstar) were identified using this hierarchical model [2]. Although the various accident investigation boards tended to concentrate on different aspects, the number of common factors is striking. In this section, the systemic factors related to the Level 2 conditions for the SOHO loss are described and related to similar factors in the other losses.

Flaws in the Safety Culture

Overconfidence and Complacency

Most preventable accidents involve overconfidence and complacency. Success is ironically one of the progenitors of accidents. In SOHO these factors led to inadequate testing and review of changes to ground-issued commands, a false sense of confidence in the team's ability to recover from an ESR, the use of challenging schedules, responses to emergencies without taking the designed-in time to consider their options, etc. (C1, C9, C20, C22)

Discounting or Not Understanding Software Risks

Accidents involving software often occur within an engineering culture that has unrealistic expectations about software and the use of computers. Changing software, like the command sequences for SOHO, is extremely difficult and error-prone. The modifications to the SOHO command procedures were subjected to very little testing and review, perhaps because they were believed to be minor. In fact, changing software without introducing errors or undesired behavior is much more difficult than building correct software initially. (C2, C4, C8)

Assuming Risk Decreases over Time

In the Titan IVB-32/Milstar loss, the Titan Program Office decided that because software was "mature, stable, and had not experienced problems in the past," they could use the limited resources available after the initial development effort to address hardware issues. In several other accidents we studied, quality and mission assurance as well as system engineering was also reduced or eliminated during operations because it was felt they were no longer needed or the resources were needed more elsewhere.

During SOHO operations, there was a lack of analysis of prior ESRs, inadequate staffing of operations, no apparent mission assurance and quality assurance functions, inadequate attention paid to changes, etc. The SOHO Mission Management Plan required that the NASA Project Operations Director be responsible for programmatic matters, provide "overall technical direction" to the flight operations team, and interface with the ESA technical support director. The position had been de-scoped over time by NASA from a dedicated individual during launch and commissioning to one NASA individual spending less than 10% of his time tracking SOHO operations. ESA was to retain ownership of the spacecraft and to be responsible for its technical integrity and safety, but they were understaffed to perform this function in other than routine situations. It is very common to assume that risk is decreasing after an extended period of success and to let down one's guard.

Inadequate Emphasis on Risk Management

A recommendation common to several of the spacecraft reports was to pay greater attention to risk identification and management. For example, a report on the Mars Climate Orbiter loss concluded that the pressure of meeting the cost and schedule goals resulted in an environment of increasing risk in which too many corners were cut in applying proven engineering practices and in the checks and balances necessary for mission success. For SOHO, the critical pressures involved meeting science objectives – safety was frequently given a lower priority. The compressed timeline eliminated any time to handle potential emergencies – contingency planning was inadequate. Protections built into the process, such as review of

critical decisions, were bypassed. And key personnel were distracted from spacecraft recovery efforts by continuing analysis of the simulation results. After the previous two SOHO spacecraft emergency retreats to safe mode, the software and procedures were not reviewed because higher priority had been assigned to other tasks. (C1, C2, C8, C9, C12, C20, C21, C23, C25)

Incorrect Prioritization of Changes

Several recent aircraft accidents have involved problems for which software fixes had been created but for various reasons had not been installed on the specific airplane involved. The reasons for this omission are complicated, and sometimes involved politics and marketing (and their combination) as much as complacency and cost factors. A deficiency report on the SOHO interface to telemetry data had been submitted four years earlier but never resolved. Perhaps the change had been put off because a new IMOC was planned. With only the information provided in the SOHO accident report, it is not possible to determine whether all the changes made to the command structure were critical, but the report does say that none were triggered by requirements changes. Certainly, A-CONFIG-N did not need to be changed to despin Gyro A. (C1, C4)

Slow Understanding of the Problems Associated with Human-Automation Mismatch

Commercial aviation is the first industry where shared control of safety-critical functions between humans and computers has been widely implemented. The very difficult problems that result, such as those associated with mode confusion and deficiencies in feedback and situational awareness are slow to be recognized and acknowledged. It is more common simply to blame the pilot for the accident than to investigate the aspects of system design that may have led to the human error(s). Similar problems exist with the design of automation for ground control of spacecraft and astronaut-automation interaction. The SOHO report, although critical of the ground personnel decisions and actions, does not investigate why these mistakes were made. A hint that there was a problem is the lack of response to the deficiency report from the operations team about the difficulty in using the telemetry data. (C1, C24, C27)

Ineffective Organizational Structure

Diffusion of Responsibility and Authority

In almost all of the spacecraft accidents, there appeared to be serious organizational and communication problems among the geographically dispersed partners. Responsibility was diffused without complete coverage and without complete understanding by anyone about what all the groups were doing. SOHO had the same problems.

ESA was to retain ownership of the spacecraft and to be responsible for the technical integrity and safety of the spacecraft and science instrumentation at all times. In practice, the level of support was not adequate to retain full responsibility for the spacecraft health and safety: They were under-staffed to perform this function in other than routine situations. The NASA position of Project Operations Director had been de-scoped and reduced to one individual spending 10% of his time. The flight operations team was apparently able to change procedures without proper review. A transfer of management authority to the SOHO Project Scientist resident at GSFC left no manager, either from NASA or ESA, as the clear champion of spacecraft health and safety. Instead, the transfer encouraged management decisions that maximized science return over spacecraft risk. The decision authority structure for real-time divergence from agreed-upon ground and spacecraft procedures was far from clear. (C1, C5, C6, C8, C21, C23, C25)

Low-level status or Missing System Safety Program

As noted in the Challenger accident report, safety was originally identified as a separate responsibility by the Air Force during the ballistic missile programs of the 50s and 60s to make sure that safety is given due consideration in decisions involving conflicting pressures and that safety issues are visible at all levels of decision making. Having an effective safety program cannot prevent errors of judgment in balancing conflicting safety, schedule, budget, and science constraints, but it can at least make sure that decisions are informed and that safety is given due consideration. In the SOHO report, no mention is made to any formal safety program.

Limited Communication Channels and Poor Information Flow

In the Titan, Challenger, and Mars Climate Orbiter accidents, there was evidence that a problem existed before the loss occurred, but there was no communication channel established for getting the information to those who could understand it and to decision makers or, alternatively, the problem-reporting channel was ineffective in some way or was simply unused.

All of the accidents involved one engineering or operations group not getting the information they needed from another group. SOHO had similar communication problems between the operations team and technical experts. For example, when a significant change to procedures was implemented, an internal process was used (MOCR forms) and nobody outside the flight operations team was notified. The functional content of an operational procedure, A-CONFIG-N was modified without updating the procedure name and without appropriate documentation and review of the changes. Although the procedure change was discussed between the flight operations team and ESA/MMS personnel, safety-critical information (i.e., that each time Gyro A is despun, the automatic software function must be re-enabled) was provided through an email exchange. (C5, C6, C18)

Ineffective Technical Activities

Flawed or Inadequate Review Process.

General problems with the review process were mentioned in all the accident reports. For SOHO, the changes to the ground-generated commands were subjected to very limited review. The flight operations team placed high reliance on ESA and MMS representatives who were quite knowledgeable on the spacecraft design. However, there were only two of them and neither was versed in the computer language (TSTOL) used to define the commands. Consequently, the level of verification that the ESA and MMS personnel could provide was limited. There does appear to have been a simulation of the compressed timeline, but the analysis of a problem detected during simulation was still going on as the new procedures were being used. No information is provided about whether the simulation was capable of detecting the error in A-CONFIG-N. (C6, C8, C12, C21, C25)

Inadequate Specifications

Software-related accidents almost always are due to misunderstandings about what the software should do. Almost all the accident reports studied refer to poor specification practices. The Ariane accident, for example, notes that inadequate specification practices and the structure of the documentation obscured the ability to review the critical design decisions and their underlying rationale. Complete and understandable specifications are not only necessary for development, but they are critical for operations and the handoff between developers, maintainers, and operators. Good specifications that include requirements tracing and design rationale are critical for long-lived systems.

Although little is said in the accident report about the specifications for SOHO, there is mention that no hard copy of the command procedure set existed and the latest versions were stored electronically without adequate notification of procedure modifications. The report also says that the software enable command had not been included in A_CONFIG_N due to a lack of system knowledge of the person who modified the procedure. Such information, particularly about safety-critical features, obviously need to be clearly and prominently described in the system specifications. (C15, C18)

Inadequate System and Software Engineering

For any project as complex as those involved in the accidents we studied, good system engineering is essential for success. In some of these accidents, system-engineering resources were insufficient to meet the needs of the project. In others, the process was flawed and nobody seemed to be in charge of it. The SOHO operations phase appeared to have all of these problems, although system engineering is not mentioned directly in the report. Surprisingly, although most of the accidents studied involved software design in some way, very little information is provided in the reports about the software development process and why the software problems were introduced or not detected during development. Almost all the emphasis in the reports is on operations. Relying on operations to detect and handle software design errors (of course in SOHO operations introduced the errors). (C6, C12, C16)

Software Reuse Without Appropriate Analysis of its Safety

Two of the spacecraft accidents, Titan and Ariane, involved reused software originally developed for other systems. The problem was not the reuse itself but that the software was used without an adequate safety analysis of its operation in the new system context. Testing alone is not adequate to accomplish this for software.

Unnecessary Complexity and Software Functions

One of the most basic concepts in engineering critical systems is to "keep it simple." The seemingly unlimited ability of software to implement desirable features often, as in the case of most of the spacecraft accidents we studied, pushes this basic principle into the background. The Ariane 5 and Titan IVB-32 accidents clearly involved software that was not needed, but surprisingly the decision to put in or to keep these features (in the case of reuse) was not questioned in the accident reports.

For SOHO, there was no reason to introduce a new function into A-CONFIG-N to despin Gyro A; IRU-REST could have been used all the time. In addition, in the new continuous timeline, there was no need to despin Gyro A between gyro calibration and the momentum maneuvers. Tradeoffs were obviously involved here, although ignorance may also be part of the problem. While it is always dangerous to second-guess in hindsight such tradeoffs, it is important to understand them so that better decisions can be made in the future. Unfortunately, the accident report does not provide enough information to understand the decision making process that occurred or the options that were considered. The fact that Gyro A was safety-critical during ESR means that the decision-making process should have been a rigorous one. (C4, C10)

Inadequate System Safety Engineering

Judging from the information included in the accident reports, none of the projects, including SOHO, appear to have had adequate system safety engineering. In fact, the reports are all surprisingly silent about their safety programs instead of being prominent element. More information is needed to determine whether system safety engineering techniques were not used on these projects or whether they were used but were ineffective. For

SOHO, a hazard analysis surely would have shown that roll rate and the status of gyros A and B were critical and this information could have guided the design of feedback channels to the operators about their status. A rigorous System Safety process would have triggered special safety analysis when changes were made to the operational procedures involving safety-critical components. In addition, a strong System Safety program would have ensured that high priority was given to the analysis of previous ESRs, greater controls were placed on safety-critical operational procedures, and that safety-related open problem reports, such as that involving the difficulty in reviewing telemetry data, were tracked and resolved. (C5, C8, C10, C12)

Test and Simulation Environments that do not Match the Operational Environment

A general principle in testing aerospace systems is to "fly what you test and test what you fly." This principle was violated in all the aerospace accidents, including SOHO. The test and simulation processes must reflect accurately the system design and environment. Although following this principle rigorously is often difficult or even impossible for spacecraft, no reasonable explanation was presented in the reports for some of the omissions in the testing for these systems. Testing of the SOHO procedures was primarily performed using a simulator, but the simulator had not been maintained with all on-board software changes that had been implemented on the spacecraft, essentially making such testing useless.

It is always dangerous to conclude that poor testing was the "cause" of an accident. After the fact, it is always easy to find a test case that would have uncovered a known error, but it is usually difficult to prove that the particular test case would have been selected beforehand even if testing procedures were changed. By definition, the cause of an accident can always be stated as a failure to test for the condition that was determined, after the accident, to have led to the loss. However, in the accidents we studied, there do seem to be omissions that reflect poor decisions related to testing. (C13)

Deficiencies in Safety-Related Information Collection and Use.

Researchers have found that the second most important factor in the success of any safety

program (after top management concern) is the quality of the hazard information system. Both collection of critical information as well as dissemination to the appropriate people for action is required. In all but one of the spacecraft accidents, the existing formal anomaly reporting system was bypassed (in Ariane 5, there is no information about whether one existed), and informal email and voice mail was substituted. Dissemination of safety-critical information was haphazard at best. In the SOHO accident report, critical information about Gyro A was provided informally to the flight operations team via email.

Operational Personnel Not Understanding the Automation

Neither the Mars Climate Orbiter nor the Titan mission operations personnel understood the system or software well enough to interpret the data they saw as indicating there was a problem in time to prevent the loss. The SOHO report says that the software enable function had not been included as part of the modification to A-CONFIG-N due to a lack of system knowledge of the person who modified the procedure. The flight operational team was not sufficiently versed regarding details of the spacecraft design and its idiosyncrasies, and this problem became worse as turnover occurred and there was no time for new personnel to take advantage of training sessions.

Complexity in the automation combined with poor documentation and training procedures are contributing to this lack of understanding, which is becoming a common factor in aircraft accidents. Accidents, surveys, and simulator studies have emphasized the problems pilots are having in understanding digital automation. (C15)

Inadequate and Ineffective Cognitive Engineering and Feedback

For spacecraft and highly automated aircraft, ground controllers and pilots rely on indirect information about the object they are controlling. Their effectiveness depends on the information they are given and the format in which it is presented. Many of the problems found in human automation interaction lie in the human not getting appropriate feedback to monitor the automation and to make informed decisions.

Several places in the SOHO report hint at the controllers not having the information they needed about the state of the gyros and the spacecraft in general to make appropriate decisions. Unfortunately, not enough information is included to determine where the problems lay. In general, a hazard analysis can be helpful to those designing displays. The misdiagnosis of Gyro B as the bad one and subsequently deactivation raises many important questions that are not answered in the report. More understanding about why such mistakes are made and what information could help as well as how to display it in a way that it can easily be interpreted is needed.

Cognitive engineering, particularly that directed at the influence of software design on human error, is still in its early stages. Human factors experts have written extensively on the potential risks introduced by the automation capabilities of glass cockpit aircraft. Among those identified are over reliance on automation, shifting workload by increasing it during periods of already high workload and decreasing it during periods of already low workload, being "clumsy" or difficult to use, being opaque or difficult to understand and requiring excessive experience to gain proficiency in its use. (C1, C17, C24, C27)

Conclusions

We have demonstrated the use of a hierarchical accident model to help understand accidents using the SOHO mission interruption as a case study. In the process we identified some systemic factors involved in this loss and compared them to those we have identified in other recent aerospace accidents. The similarities and parallels should help in focusing efforts to prevent future accidents.

Bibliography

[1] NASA/ESA Investigation Board, 31 Aug. 1998, "SOHO Mission Interruption"

[2] Leveson, Nancy, 25 June 2001, "Evaluating Accident Models Using Recent Aerospace Accidents, Part I: Event-Based Models"