Use of a PRA in Supporting the Design of a GOES Weather Satellite and Ground System

PRINCE KALIA1*, ROBIN PAIR2, JOHN UHLENBROCK2, VIRGINIA QUANEY2 and YING SHI1

1 NASA Goddard Space Flight Center, 8800 Greenbelt Road, Greenbelt, MD 20771, U.S.A.
2 ARES Corporation, 1440 Chapin Avenue, Suite 390, Burlingame, CA 94010, U.S.A.

(Received on April 12, 2013, revised on April 17, and May 08, 2013)

Abstract: Probabilistic Risk Assessment (PRA) was initially adopted and implemented by NASA in the operational phase of human space flight programs and more recently for the next generation human and robotic space explorations as well as the key operational space missions. Since its first use at NASA, PRA has become recognized throughout the agency as a method of assessing complex mission risks as part of an overall approach to assuring safety and mission success. PRA is now included as a requirement during the design phase of both NASA next generation human space systems as well as high priority robotic/operational missions. This paper presents the application of the first comprehensive PRA during the design phase of the Geostationary Operational Environmental Satellite R-Series (GOES-R). This PRA is also unique in that it includes the first quantitative ground system analysis conducted at NASA. The design and operational changes resulting from the GOES-R PRA are discussed in detail in this paper.

Keywords: Probabilistic Risk Assessment, GOES weather satellite, ground system, operational risks, design support, fault management

1 Introduction

This paper presents a case study of the implementation of a Probabilistic Risk Assessment to support the design of the Geostationary Operational Environmental Satellite R-Series (GOES-R), a high-priority operational space mission. The GOES-R PRA includes analysis of the satellite (spacecraft and instruments), and the ground system. Through early incorporation into the design process, the GOES-R PRA not only represented a comprehensive and practical approach to addressing and mitigating operational risk, but became an integrated design tool that affected day-to-day design and operations decisions.

The rest of the paper is organized as follows: Section 2 introduces the GOES-R program; Section 3 presents a highlight of the effective collaboration between the GOES-R PRA and design teams; an overview of GOES-R PRA implementation is described in Section 4; Section 5 describes the successful use of fault trees as the value-driven evaluation tools for the GOES-R satellite PRA; Section 6 presents the risks identified by PRA for the Ground system; Additional basic failure contributions are listed in Section 7; Results and conclusions are described in Section 8 and Section 9 respectively.

2 Geostationary Operational Environmental Satellite R-Series

For almost 40 years, constellations of GOES weather satellites stationed high above Earth’s equator in geostationary orbit have provided nearly continuous imagery and data on atmospheric conditions and solar activity affecting Earth. The data products of these
GOES have led to improved weather and climate models, enabling more accurate and faster weather forecasting and better understanding of long term climate conditions [1].

The GOES satellites and ground systems are built and launched by NASA and operated by NOAA. Since the development and launch of the first GOES in 1974, these two organizations have pushed the technology to its current advanced state, as represented by GOES-R. GOES-R is a significant leap forward in weather forecasting technology with the next generation satellite and ground system. It offers a greater quantity of data products that are more accurate, of higher resolution, and available faster than those from previous GOES. As the primary instrument on GOES-R, the Advanced Baseline Imager (ABI) provides three times more spectral information, four times the spatial resolution and more than five times faster temporal coverage than the current GOES system. The ABI provides up-to-the-minute data related to weather, oceans, land, climate and hazards (including fires, volcanoes, hurricanes, and tornados) [1]. GOES-R provides not only improvements in instrument capabilities, but also new products and applications, along with faster data dissemination techniques and reduced product lag time.

3 Integration of the PRA Into the Design and Engineering Efforts

The GOES-R PRA was integrated with the program’s design and engineering efforts, effectively creating an iterative, risk-informed design process allowing for day-to-day design changes that include PRA considerations. The approach to develop the PRA as an integrated design tool can be broken down into three different implementation areas: (1) PRA team integration into the program’s recurring business activities, (2) applying design teams’ input to the PRA to ensure an up-to-date and useful product, and (3) utilizing the PRA team’s knowledge of risk and system interaction to inform the design teams’ products.

The following are specific examples of PRA involvement within each of these three integration categories and the benefits they provided to the GOES-R program.

PRA Team Integration with Recurring Business Activities: Co-locating with the system designers and participating in regular project meetings allowed the PRA team to become part of an integrated design process. As a result, the PRA team had an increased awareness of the technical challenges and design changes being addressed by the project, developed a detailed understanding of the concept of operations, and cultivated key relationships that helped facilitate PRA development. The following list provides some examples of regular program activities in which the PRA team participated or provided inputs:

- Systems engineering staff meetings;
- System design team meetings;
- Reliability team and other integrated Safety and Mission Assurance (S&MA) meetings;
- System and subsystem design reviews;
- Engineering Change Board;
- Risk Review Board.

The benefit of PRA team participation at this level was that it enabled an effective PRA, reflective of current design and capable of providing immediate feedback as needed.

Applying Design Teams’ Input to the PRA to ensure an Up-to-date and Useful Product: Risk-based analyses, including PRA, are valuable because they encourage people to question how systems can fail. In general, PRA development was tied very closely to
design development. The design teams contributed to many key aspects affecting the PRA architecture, including:

- Definition of success and failure criteria at the system, functional, component and sub-component levels;
- Definition of failure consequences;
- Identification of system responses;
- Review of fault trees and model logic.

The benefit of encouraging a high degree of involvement with the design teams was a PRA product that reflected the current design and could be used as a feedback tool to evaluate risk when considering design changes.

Utilizing the PRA Team’s Knowledge of Risk and System Interaction to inform the Design Teams’ Products: The GOES-R PRA team contributed expertise to a number of other disciplines’ products by performing the following tasks:

- Detailed review of design documents and schematics;
- Review of requirements specifications;
- Participation in Fault Detection, Isolation, and Correction (FDIC) design meetings;
- Support of concept of operations definition;
- Support of development of the Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL);
- Review of Hazard Analysis;
- Review of Reliability Block Diagrams (RBDs).

The benefit of this cooperative, back-and-forth relationship was to encourage a risk-conscious culture by providing a voice to system failure and response in every program area. This relationship, between designers and risk analysts, increased the quality of documents created by both groups.

4 The GOES-R PRA

As an operational space mission of 15 years life, the failure of concern to the GOES-R program is the failure to meet the mission objectives. Specifically, the mission objectives of interest to the PRA are: maintaining the continuous ability to generate high quality weather data, maintaining satellite assets, and safely decommissioning the satellite at end of life.

The GOES-R PRA was developed as two different models: the ground system model and the satellite model. The two were separately developed, in part because they have fundamentally different modeling structures: the ground system is a repairable system; the satellite is not. Each model was structured with associated failure criteria to align with the mission objectives.

The GOES-R ground system model is unique in that it represents the first integrated ground system quantitative risk analysis of this scale conducted at NASA. The specific mission objectives of interest to the GOES-R ground system PRA are the continuous ability to generate and distribute GOES-R products to the user community and the ability to continuously command and control the satellite. Each objective corresponded to a failure scenario, which was assessed for both likelihood and consequence. The ground system is considered fully repairable; therefore, failures and events on the ground lead only to a temporary inability to meet mission objectives.

Three satellite scenarios were created to capture failures that resulted in (1) losing an instrument data stream, (2) degraded performance in a data stream, or (3) losing the ability
to safely decommission the satellite. These scenarios were associated with the three top-level mission objectives. Generally, satellite failures are more critical than ground system failures, since the satellite is not a repairable system. Similar to the ground system, each failure scenario was assessed for both its likelihood and consequence. Consequence was determined by which data streams were lost and the expected lost mission time resulting from each failure scenario.

Two separate analyses were developed for both the ground system and the satellite to quantify the probability and consequences of failing to meet mission objectives. The first analysis consisted of a traditional PRA model, utilizing events trees and fault trees to quantify the probability of failing to meet mission objectives. The second analysis was a Monte Carlo simulation analysis, used to quantify the expected time the system would remain in a failed state, based on either the predicted system repair time (for ground system failures) or the predicted failure time (for satellite failures). Collectively, the outputs from these models provided an overall mission risk picture.

5 The Role of Fault Tree Analysis in the GOES-R PRA

As part of the satellite PRA development, a qualitative, fault tree-based, operational risk identification process was implemented. This process utilized a team of Subject Matter Experts (SMEs) from multiple disciplines to evaluate every critical function identified in the concept of operations for potential failure modes. Fault trees provided the hierarchy to document operational and functional failures leading to undesirable outcomes. The end of each fault tree branch included a disposition to document design features, margins, redundancies, FDIC, or other project activities that showed how the GOES-R design addressed the risk. These fault trees were created for each mission phase and proved to be a valuable tool for identifying risks and discovering gaps in the concept of operations. They also drove the implementation of fault protection and operational requirements and ensured PRA model completeness. These fault trees became the foundation for the satellite PRA model and were directly responsible for a number of design changes which included:

• Identification of fault management requirements necessary for the satellite to respond to a low-likelihood, high-consequence, off-nominal situation;
• Identification of propulsion system failures that could not be responded to during operations, requiring redesign;
• Identification of single point failures, requiring command and control interface reconfiguration to increase reliability and achieve acceptable redundancy;
• Identification of launch configurations that precluded the use of potential backups for off-nominal situations resulting in a launch configuration change;
• Identification of a component overvoltage condition that could propagate to downstream components, resulting in overvoltage protection implementation.

Figure 1 is a generalized excerpt from a vehicle control qualitative fault tree, describing the On-Orbit Operations phase that was utilized in the process described above. Only one fully developed fault tree branch is shown here to provide some detail and context.
As seen in Figure 1, at the end of the failure decomposition (i.e., leaf of the tree), dispositions documented how the system will detect and/or respond to each potential failure. Ultimately, this fault tree development process was valuable because it provided a means to impact the day-to-day design and operational decisions made by the project. By surfacing risks and encouraging a risk-conscious culture, the qualitative fault tree technique had a positive impact on the program.

6 Ground System Risks

Given that the GOES-R ground system is designed to be highly redundant and to withstand multiple independent failures, a primary concern for the project is failures which could eliminate most or all available redundancy simultaneously. Failures affecting facility operations at one or more sites could severely handicap the ground system for extended periods of time. The ground system PRA included an analysis of natural hazards and facility failures leading to a failure to meet mission objectives.

The GOES-R ground system consists of three, geographically diverse ground stations in the eastern United States. Using historical data, each ground station was assessed for its susceptibility to natural hazards. Natural hazards were considered for their potential effect at each ground site independently, as well as for potential impacts affecting multiple sites simultaneously. The natural hazards identified as posing a potential threat to one or more ground stations included:

- Tropical weather (hurricanes);
- Snow accumulation;
- Flooding;
- Seismic events;
Additional natural hazards were considered for analysis, including tsunamis, sea level rise, and volcanoes; however, there was not significant historical evidence that any of these events would pose a threat to the GOES-R mission.

In addition to the natural hazards, each ground station considered failures affecting the ground station facility or infrastructure. Facility and infrastructure failures were assumed to independently impact each ground station with the same likelihood. The failures in this category included:

- HVAC and cooling failures;
- Power failures (including commercial power grid failure and failure of redundant backup generators and batteries);
- Telecommunications failures;
- Structure fire events.

The facility and infrastructure failure probability distributions were derived from a variety of sources, including historical data, generic failure and reliability databases, and nuclear industry estimates from the Nuclear Regulatory Commission (NRC). Both telecommunication failures and widespread commercial power grid failures were considered for their potential capability to affect multiple ground stations at once.

Although the probabilities for natural hazards and facility failure events were found to be low, the resulting downtime from any one of these events could be significant (longer than a month in the most severe cases). Therefore, the natural hazard and infrastructure failure events represent significant ground system risk drivers. Rather than leading to a specific design change, presenting this risk driver led the program to identify emergency response actions and contingency plans.

7 Additional Basic Failure Contributions

In addition to the natural hazard and infrastructure failures listed above, the following sources of failure were included as inputs to the PRA models. The provided descriptions introduce the methods by which they were quantified and modeled.

**Hardware Failures:** GOES-R hardware failures were modeled at the lowest functional level; generally, the component level (defined as the Line Replaceable Unit (LRU) level in the ground system). The GOES-R ground system is a fully redundant and repairable system with multiple operational configurations available. As such, independent ground system hardware failure was not a risk driver. However, the satellite is a non-repairable system; thus, hardware failures were among the top risk drivers for the satellite.

**Software Failures:** Due to the data available, software failures were handled slightly differently for the satellite and ground system. A satellite-level software risk estimate was modeled based on operational data from eight prior missions. Incorporating software failure criticality assumptions based upon mission complexity allowed prediction of satellite failure due to software error.

The vast majority of software in the ground system is Off The Shelf (OTS) software packages. For each ground system software package, a software reliability prediction was produced by estimating the Source Lines of Code (SLOC) and predicting the number of deployed defects by applying software reliability statistics based on the ground system’s software development, test, and deployment characteristics. The predicted numbers of defects were extrapolated into a software failure rate for each software package. As with hardware, critical software failures in the ground system result in a repair action, modeled
as a Mean Time to Software Restore (MTSWR). MTSWR distributions were based on test and historical data.

Independent software failures were not identified as a ground system risk driver due to high levels of system redundancy. Due to a failure criterion of permanent satellite failure, software failures were a minimal risk to the satellite, due to the lack of critical maneuvers performed autonomously and multiple failure depths available to safe mode.

**Common Cause Failures**: Common Cause Failures (CCFs) were modeled in a similar fashion for both the satellite and the ground system. All redundant components and systems were assessed for CCF risk contribution. CCFs can disable multiple levels of redundancy and lead to system failures. As a result of this phenomenon, CCFs were the largest risk contributor on the ground system and a significant contributor to the satellite hardware risk.

**Human Errors**: Human errors were considered in both the GOES-R satellite and ground system analyses. Within the GOES-R operational parameters, the opportunity for human error is generally minimal. The majority of critical operations are nominally automated and human system interaction is limited to highly controlled procedures and failure responses. With respect to the concept of operations, two scenarios were identified as potential areas for human error: erroneous satellite commanding and ground system operational failover from the primary ground station to the backup site.

Erroneous commanding describes a command sent by the ground system to the satellite, which is either an incorrect or faulty command or a command sent at the incorrect time. In both cases the erroneous commanding may be attributable to human errors. Historical command error data from seven previous missions was collected to estimate the likelihood of satellite failure due to erroneous commanding. Assumptions were applied to the data to include only those erroneous commands which would result in a permanent satellite failure. All erroneous commands were assumed to lead to loss of satellite.

Operational failovers from the primary GOES-R ground station to the backup site can be configured in one of two ways – human input required for the transition and a fully automated transition. The ground system analysis models both operational configurations. To calculate the probability of human error when human input is required, the PRA utilized the human reliability estimation tool Cognitive Reliability Error Analysis Method (CREAM). The CREAM methodology is accepted practice for human error estimation at NASA and has historically proven to provide a reasonable estimate for human error probability. This type of human error event was assumed to have a relatively quick resolution, as feedback to the failure would be immediate and correcting the problem would not require significant time or resources.

Erroneous commanding was not a risk driver for loss of satellite. However, automating the ground station failover process (i.e., removing all operator involvement from the process) was determined to decrease the probability of failing to meet ground system mission objectives by as much as 50%.

**Micro-Meteoroids**: Components external to the satellite were assessed for vulnerabilities and a probability of failure due to micro-meteoroid penetration was calculated for each vulnerable component. This systematic assessment identified a number of significant risks and additional protections were implemented as a result.
8 Results

**Ground System:** Due to the multiple layers of redundancy built into the GOES-R ground system, common cause failures, and other types of failures that invalidate multiple redundant components at once, contribute the most risk. The leading system risk drivers for temporary loss of ground system capabilities include: 1) common cause server failures affecting all sites; 2) common cause server failures at the primary operational ground station combined with operator error during station failover to the backup ground station; and 3) site outages due to natural hazards or infrastructure failures at a single ground station combined with common cause server failure at the backup ground station. Although in each case the root failure cause affects the site availability, the overall predicted GOES-R ground system availability remains very high due to the level of redundancies. The high availability indicates that in all likelihood the GOES-R ground system will not experience any of these critical failure combinations during mission life; however, if any of these failure combinations do occur the incurred downtime could be significant, ranging from 30 minutes to over two weeks.

**Satellite:** The risks to the GOES-R satellite are similar to other earth observing satellites and fall within expectations based on historical satellite failures. Among the satellite’s capabilities, the systems contributing the most risk are the largest and most complicated systems including the instruments, attitude/orbit control systems as well as the computer systems controlling the satellite and satellite-to-ground communication systems. Micro-meteoroids also present a significant risk to GOES-R and other satellites as exposed components are susceptible to the space environment. Software, deployments, thermal and power systems represented a relatively lower system risk. Although deployment mechanism carries a low risk over the mission duration, the worst case consequence could be a mission lost. If solar panel deployment fails or is partially deployed could affect all subsequent mission operations due to inadequate/no power to vital systems.

9 Conclusions

The application of PRA on GOES-R demonstrated the value a PRA can bring to the design of a system by providing an early overall understanding of risk drivers. The GOES-R PRA resulted in a more reliable design and operational system prepared to respond to a variety of potential anomalies. Integrating the PRA team and analysis techniques into the execution of the project facilitated a risk-conscious culture and provided an organized venue for analyzing and quantifying risk. Logically assessing all identified failure sources within a fault tree and event tree model structure was closely tied to mission objectives. This approach led to concrete design and operational changes and by identifying and addressing risk drivers during design, rather than operations. The following list generically captures the PRA findings and resulting corrective actions:

- Identification of off-nominal situations that required unique responses and the on board fault management software required to do so;
- Identification of failures that could not be quickly responded to, and therefore required redesign;
- Identification of command and control interfaces that were reconfigured to increase reliability;
- Identification of launch configurations that precluded the use of potential backups for off-nominal situations;
• Identification of single point failures that required command and control interface reconfiguration;
• Identification of failures that could propagate across functional and component boundaries resulting in design modifications;
• Quantification of micro-meteoroid risk and implementing simple micro-meteoroid protections;
• Quantification of CCFs and natural hazards risk drivers across ground stations resulting in operational preparedness and emergency response planning;
• For Ground Systems, human error was assessed as a dominating contributor to success of ground operations providing opportunity to Operations team to automate the operations to the extent possible.

Thus the GOES-R PRA as a subset of project decision tools, strengthened capabilities to minimize uncertainties for various mission scenarios to better understand risk, do something about key risk drivers and prudently help mission success.

Acknowledgement: We would like to acknowledge Jason Emperador, Dr. Ming Li, Dr. Mark Kaminskiy, Pires Thiago and Rebecca Dibari for their support of the GOES-R PRA development. We also would like to acknowledge GOES-R project management team, especially Pamela Sullivan and Mike Donnelly, and subsystem leads for their great support of the PRA task. Special thanks to all the reviewers of the GOES-R PRA reports for their valuable comments and recommendations.

References

Prince Kalia is the Goddard Space Flight Center (GSFC) Reliability Manager responsible for management and oversight of the GOES-R PRA. His previous experience includes providing leadership to the Space Shuttle Solid Rocket Booster PRA efforts as part of his Safety and Reliability responsibilities. He also provided S&MA leadership to NASA’s SMART Buyers Design Team to help finalize the design architecture of the Launch Abort System for the Crew Exploration Vehicle, and Reliability and Maintainability discipline facilitation for the Constellation Program.

Robin Pair conducted the ground system analysis as a Harris support contractor. She is a Senior Risk Analyst with ARES Corporation and has conducted risk assessments on various NASA programs from 2007 to present. Prior to working as a Risk Analyst, she taught high school math in South Florida. She received her Bachelor’s of Science in Industrial and Systems Engineering from the Georgia Institute of Technology.

John Uhlenbrock was the lead analyst for the satellite and conducted the satellite analysis as a Lockheed Martin support contractor. He is a Systems Engineer and Risk Specialist with ARES Corporation, having 8 years experience performing Probabilistic Risk Assessment on a variety of NASA and Department of Energy (DoE) programs. He has supported the development of satellite and ground stations PRAs as well as PRAs for human-rated NASA missions and nuclear waste handling for the DoE.

Virginia Quaney conducted the satellite analysis as a Lockheed Martin support contractor. She is a Risk Analyst with ARES Corporation and has conducted risk and
reliability assessments on various NASA and Department of Defense (DOD) programs from 2010 to present. She received her Bachelor’s of Science in Aeronautics and Astronautics from the Massachusetts Institute of Technology.

**Ying Shi** is a Software Reliability and Safety Engineer at NASA Goddard Space Flight Center, providing technical supports for various projects related to reliability, safety analyses and Probabilistic Risk Assessment. She joined the GOES-R team as the project reliability engineer in 2008. She received her Ph.D. in Software Reliability Engineering from the University of Maryland and her M.S. in Reliability Engineering from the University of Arizona. She is a member of IEEE and IEEE Reliability Society.