Requirements Eng (2007) 12:41–54
DOI 10.1007/s00766-006-0039-4

ORIGINAL RESEARCH

Using obstacle analysis to identify contingency requirements on an unpiloted aerial vehicle

Robyn Lutz · Ann Patterson-Hine · Stacy Nelson · Chad R. Frost · Doron Tal · Robert Harris

Received: 16 March 2006 / Accepted: 26 September 2006 / Published online: 31 October 2006

Abstract This paper describes the use of Obstacle Analysis to identify anomaly handling requirements for a safety-critical, autonomous system. The software requirements for the system evolved during operations due to an on-going effort to increase the autonomous system's robustness. The resulting increase in autonomy also increased system complexity. This investigation used Obstacle Analysis to identify and to reason incrementally about new requirements for handling failures and other anomalous events. Results reported in the paper show that Obstacle Analysis complemented standard safety-analysis techniques in identifying undesirable behaviors and ways to resolve them. The step-by-step use of Obstacle Analysis identified potential side effects and missing monitoring and control requirements. Adding an Availability Indicator and feature-interaction patterns proved useful for the analysis of obstacle resolutions. The paper discusses the consequences of these results in terms of the adoption of Obstacle Analysis to analyze anomaly handling requirements in evolving systems.

Keywords Contingency requirements · Obstacle analysis · Safety-critical software · Requirements evolution · Autonomy · Anomaly handling

R. Lutz (✉)
JPL/Caltech and Iowa State University,
226 Atanasoff Hall, Ames, IA 50011, USA
e-mail: rlutz@cs.iastate.edu

A. Patterson-Hine · C. R. Frost
Ames Research Center, Mail Stop 269-4,
Moffett Field, CA 94035, USA
e-mail: apatterson-hine@mail.arc.nasa.gov

C. R. Frost
e-mail: cfrost@mail.arc.nasa.gov

S. Nelson
NelsonConsulting/QSS, Ames Research Center,
Moffett Field, CA 94035, USA
e-mail: NelsonConsult@aol.com

D. Tal
USRA/RIACS at NASA Ames Research Center,
Moffett Field, CA 94035, USA
e-mail: dt97@cornell.edu

R. Harris
255 Group, Inc. at Ames Research Center,
Mail Stop 262-2, Moffett Field, CA 94035, USA
e-mail: trebor@trebor.org

1 Introduction

This paper describes the use of Obstacle Analysis to identify anomaly handling requirements for a safety-critical, autonomous system. The software requirements for the system continued to evolve during operations due to an on-going effort to increase system robustness. The objective of the requirements evolution was for the software to handle more faults and anomalous situations autonomously. The resulting increase in autonomy also increased complexity. One risk was that the added software complexity and interactions would result in missing, inconsistent, or poorly understood requirements for handling anomalies. Obstacle Analysis was undertaken to mitigate that risk.

The software for the system was developed in incremental builds. Requirements evolved rapidly with autonomous features being added regularly. Autonomy is the capability of a software system to make control

decisions on its own. An advantage of autonomy in this system was that it allowed the system to react faster than with human-in-the-loop controllers to failures, anomalous situations, and changes in environment. With autonomy, safe operation of the system could continue even when the human controller was unavailable.

Autonomy can also contribute to system robustness by detecting and responding to a broader class of anomalies than just failures. The requirements for anomaly handling in many safety-critical, autonomous systems encompass not only traditional fault protection and responses to undesired events [1] but also unexpected environmental or operational scenarios that could contribute to hazards.

These broader classes of anomalies that must be anticipated and handled are called ''contingencies'' [2]. Contingencies include, but go beyond, traditional fault protection. They are obstacles to the fulfillment of the system's high-level requirements that can arise during real-time operations. Contingency handling involves requirements for detecting, identifying, and responding to contingencies.

The application of obstacle analysis in this paper was to an unpiloted aerial vehicle (UAV) called a rotorcraft (described in next Section). The system was safety-critical in that it was required to take off and land autonomously. Initially flight and landing occurred in constrained airspace, but eventually will occur in populated areas. UAVs are also being developed for safety-critical applications such as imaging high-risk environments (e.g., volcanoes and forest fires); detecting accidents in highway traffic, and assisting search and rescue operations for lost hikers or downed pilots [3].

The fact that the vehicle was already operational (flying) during most of the process made an early understanding of contingencies and of their potential effect on safe flight important to the project. To achieve the required levels of system robustness, a structured approach was needed for investigation of contingency requirements.

Accordingly, we drew on the KAOS framework for goal-oriented obstacle analysis developed by van Lamsweerde and Letier. They defined a goal as a set of desired behaviors and an obstacle as a set of undesirable behaviors that impeded a goal [4]. Their goal-oriented techniques for obstacle analysis have been previously demonstrated on critical systems such as ambulance dispatch and the robotic production cell with good results.

The underlying rationale for the choice of goal-oriented obstacle analysis for the requirements analysis of the rotorcraft was that contingencies are either obstacles to achieving goals or are indications that the goals are unrealizable with the available agents. The requirements evolution in this system was toward more autonomy. Incremental autonomy, which involves replacing human agents with software agents, produces new sub-goals to achieve autonomy, new obstacles associated with those sub-goals, and additional sub-goals to resolve those obstacles, as well as new alternatives to resolving previous obstacles. All of these must be investigated if the system is to remain robust.

In the system described here, incremental autonomy meant that something previously not done automatically now was done by the software. In some cases the function had previously been done manually by operator control, while in other cases something that previously could not be done at all was now done automatically.

For example, collision avoidance (e.g., of the rotorcraft with simulated buildings) initially was done via remote control by a pilot steering the airborne rotorcraft remotely from the ground. Later, collision avoidance was done by calculating a path around the buildings before each flight began and then autonomously executing the planned path during flight. Still later, the path-calculation requirements incorporated new objects that appeared during flight (such as another, hovering rotorcraft). Future software will autonomously plan a path during flight based on real-time processing of images taken by the rotorcraft's cameras and on software that autonomously detects changes in the imaged scene. As this example demonstrates, any approach to contingency analysis needed to be readily extensible and maintainable. We describe in the Implications For Requirement Evolution section the benefits and limitations of obstacle analysis in this regard.

One advantage of autonomy is that it adds flexibility to a mission, e.g., allowing it to take advantage of unanticipated science opportunities that would be missed if observations had to wait for human interaction. The work described here is not concerned with this sort of adaptive re-planning for gain, but solely with negative contingencies that can place the system in a hazardous state. Some of the results appear to be applicable to intelligent systems that re-plan for optimization, but that investigation is beyond the scope of the work described here.

The paper describes our approach to using obstacle analysis as a structured way to reason incrementally about the new requirements and their alternatives. The contribution of the paper is to report results showing how obstacle analysis complemented standard safety-analysis techniques in identifying undesirable behaviors and how to resolve them. The lightweight, step-by-step use of Obstacle Analysis identified potential side

effects and missing monitoring and control requirements. Adding an Availability Indicator and feature-interaction patterns proved useful for the analysis of obstacle resolutions. The results suggest that Obstacle Analysis is an effective and readily adoptable technique for analyzing anomaly handling requirements in evolving systems.

The rest of the paper is organized as follows. Section 2 briefly describes the application domain. Section 3 discusses our approach. Section 4 presents the results of our use of obstacle analysis to identify contingency requirements. Section 5 discusses the implications of these findings in terms of requirements evolution and incremental autonomy. Section 6 puts the results in the context of recent, related work. Section 7 describes the verification of the contingency requirements on the UAV using tool support and simulation. Section 8 provides concluding remarks.

2 Rotorcraft application

This paper describes experience using obstacle analysis to identify contingency requirements on an UAV called a rotorcraft. The Autonomous Rotorcraft Project (ARP) is a NASA UAV project researching autonomous, low-altitude, flight systems.

Two small helicopters, originally developed for remote-piloted crop-dusting in farming regions, serve as the platforms. The autonomous system has an onboard attitude sensor (accelerometers and gyros), a GPS sensor, and a communication modem. The rotorcraft has three cameras—a stereo pair of cameras to provide input to a passive range estimation algorithm and a color camera to provide situational awareness. Ground support is housed in an instrumentation trailer with a GPS ground station, radio modems for communication with the aircraft, and video displays of the camera images. Additional description appears in [5].

We performed contingency analysis on two subsystems with safety-critical functionality (communications and vision) recommended by the project. Our involvement began about the time that the rotorcraft began regular autonomous flights within a constrained airspace with autonomous collision-avoidance path-planning around stationary objects such as simulated buildings. The size of the vision-related code at this time was about 36 K source lines of code. This number did not include open-source camera drivers or the messaging system. The project involved a tight-knit team of experts working together with strong technical leadership. Most of our knowledge of the system came from participation in weekly team meetings and from discussions with the experts on the team rather than from limited project documentation.

The project considered contingency analysis of the communications sub-system to be important because many UAVs currently rely upon flight termination (including hard landings commanded over the radio channel) to stop the vehicle in case of failure of the wireless communication channel. Improved software contingency handling for communications failure would make it possible for the UAV to fly to a safe rally point (a pre-designated location) and land normally. The project also considered contingency analysis of the camera sub-system (the cameras and range finders) to be important. This was because the cameras have mission-critical responsibilities during some operations and because the cameras provide backup position or ranging information when other components fail.

3 Obstacle analysis approach

Our approach in the work described here was to use a simplified version of the KAOS framework developed by van Lamsweerde and Letier for goal and obstacle analysis to guide the requirements analysis. The reader is referred to [4, 6, 7] for a detailed account of the goal-oriented approach. Our application of obstacle analysis to the problem was informal and manual. The use of obstacle analysis met the criteria for lightweight applications of formal methods to requirements modeling described by Easterbrook et al. [8] in that the obstacle analysis was applied in response to an existing development problem, applied selectively to only some critical portions of the requirements, offered only a partial solution without guarantees of completeness or correctness, and fed back into the development process to improve the product.

In the rest of this section we give a brief, step-by-step account of our adaptation of the obstacle analysis framework to the project. In the following sections we will describe the results of applying the obstacle analysis and evaluate our use of the goal-obstacle framework.

3.1 Step 1. Identify the goals

A goal defines a set of desired behaviors. Goal-oriented requirements engineering organizes goals in an AND/OR structure (a directed acyclic graph). The AND nodes refine the goals into sub-goals both of which must be satisfied, and the OR nodes provide alternative ways to meet the goals. Refinement continues until a sub-goal

(a terminal goal) can be achieved by an agent. Software requirements are terminal goals assigned to software agents.

3.2 Step 2. Identify the agents

Agents (e.g., human operators, hardware devices, or software components) are active objects to whom the implementations of the sub-goals are assigned (note that this definition of an agent differs from the notion of autonomous software agents. In the goal-oriented approach an agent may or may not be software, and may or may not be autonomous).

3.3 Step 3. Identify the obstacles

An obstacle describes a set of undesirable behaviors. For example, an obstacle to the goal ''Store Camera Images in Memory'' is ''Images Exceed Available Memory.'' This type of obstacle is called a ''non-satisfaction'' obstacle since it obstructs the satisfaction of a goal [4]. Obstacles cover a broad space of possible barriers to achieving required functionality. Contingencies are obstacles that can occur during real-time operations, including failures, and other anomalous events or scenarios.

Like goals, obstacles are organized and refined in AND/OR structures, and are associated with the goals they impede. The example in [4] uses a table to specify the goals, assigned agents, and obstacles for the system being analyzed (the London Ambulance System). Obstacles usually are associated with terminal goals, i.e., goals assigned to individual agents. Obstacle refinement patterns, described both formally and as heuristics of the form ''if the specification has such or such characteristics then consider such or such type of obstacle to it,'' are also described there. We report experience with these refinement patterns below.

3.4 Step 4. Identify alternative resolutions to the obstacle

Once obstacles have been identified, they need to be resolved. There are some standard strategies to resolve the obstacles [4]. For example, to eliminate the obstacle, we can consider getting rid of the goal that it obstructs, assigning a different agent so that the obstacle does not occur, adding a new goal to require that the obstacle be avoided, changing (or ''de-idealizing'') the goal, or changing the domain such that the obstacle can no longer occur. Another strategy is to just tolerate the obstacle. This might be done by adding a new goal (e.g., a new requirement for contingency handling) to mitigate the consequences of the obstacle, or just by deciding to accept the occasional occurrence of the obstacle.

3.5 Step 5. Select a resolution among the alternatives

Obstacle resolution involves evaluating and selecting from among the available alternatives. As we will see, this often involved the generation of new sub-goals to eliminate, reduce, or tolerate the identified contingency. These resolutions yielded new software requirements when assigned to software agents.

4 Results: contingency requirements from obstacle analysis

In this section we describe the results from the use of obstacle analysis to identify anomalies that could occur during operations and how they could be handled by software in the existing system. The results show that a key benefit came in the improved analysis of alternative solutions to contingencies.

4.1 Goal and agent identification

The first steps toward obstacle analysis were to identify the goals and agents. In this system the goals and agents were usually well-understood and already refined to the necessary level. As input to the obstacle analysis, we thus produced only those portions of the goal-graph about which there was some confusion or disagreement among developers. This was done in order to facilitate review of accuracy by experts.

For example, Fig. 1 shows the top nodes in a goal graph for three-dimensional collision avoidance that was developed for one such discussion (where there was confusion about details of the stereo world view at a lower level). For most goal specifications, however, we used architectural diagrams, state diagrams, and functional dependency graphs that we had earlier produced rather than producing a separate goal-graph.

This exploitation of existing project artifacts worked well. The decision not to produce a complete goal-graph meant that the obstacle analysis was less rigorous, with no formal proofs of completeness possible. However, obstacle analysis explicitly supports the possibility of such lightweight applications as a way to guide inquiry into potential obstacles [4]. In our case, iterative project review of our specifications gave some assurance that we had adequately captured the goals and sub-goals.

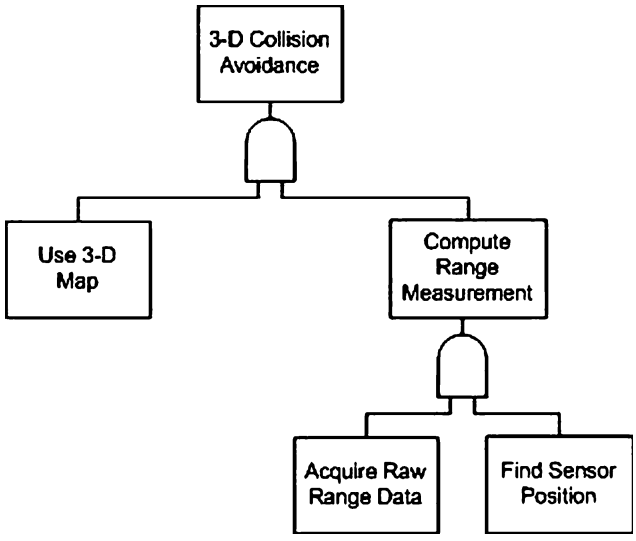

Fig. 1 Goal graph

What this means for other projects is that applying obstacle analysis techniques seemed to be a practical way to investigate software requirements for contingency handling even when the project had not previously used a goal-oriented approach. Existing project documentation and artifacts (e.g., fault trees and requirements specifications) may suffice as initial input to the obstacle analysis process. This, in turn, can enable even projects not developed using goal-oriented requirements engineering to benefit from the structured investigation of exceptional behavior performed during obstacle analysis.

With regard to agent identification, the rapid evolution of the system meant that both new software agents (autonomous features), as well as new hardware agents (sensors, cameras, range-finders, etc.) were regularly being integrated into the operational flight system. We discuss the effect of this on the obstacle analysis in Implications for Requirements Evolution section.

4.2 Obstacle identification

To help identify obstacles to the high-level requirements for communication and vision, we used Bi-Directional Safety Analysis [9]. We selected BDSA because it combines a forward analysis (from potential failure modes to their system effects) with a backward analysis (from the failures to their contributing causes). The forward analysis is similar to a Software Failure Modes, Effects, and Criticality Analysis (SFMECA). The backward analysis is similar to a Software Fault Tree Analysis (SFTA). The combination of the forward and backward analyses has proven to be a powerful way to identify and understand the causes of software-associated failures in systems. Previous uses of BDSA include validating fault protection software on two spacecraft and analyzing thruster failure modes on a third [9, 10].

We first performed a forward analysis of the communications and camera sub-systems, as requested by the project. The SFMECA structured the investigation of possible failures. For each input it considered the effect of its absence, corruption, or untimely arrival. The SFMECA also investigated what would happen if the software hung or failed in each state, or if a transition took it to a wrong state. The SFMECAs remained relatively small (e.g., 21 failure modes for one goal, 29 for another) because they focused on failure modes related to specific goals (e.g., two-way communication between the ground station and the UAV). Details of the technique appear in [9].

The SFMECA identified several contingencies. For example, one failure mode that could contribute to several hazardous scenarios was attaching incorrect identification data (vehicle pose, attitude, GPS position, etc.) to an image. The effect was that the identification data did not reflect the image content, so could mislead the software into an erroneous control decision. Another failure mode involved a failure of image compression that could result in running out of memory to store the images needed for safe, autonomous landing.

Table 1 shows an excerpt from the SFMECA for the data input ''Request for Image Processing'' received by the onboard camera software. The context is that a raw image is grabbed from the video camera stream and processed (e.g., compressed) onboard before being sent to the ground.

To investigate contingencies that did not involve the failure of single components, we also performed a backward analysis. SFTA is a graphical decomposition of a root node into its logical, component preconditions [9]. The fault trees took as root nodes the negations of communication and vision-related goals. In some cases the root nodes were hazards (e.g., collision) that negated high-level goals (e.g., collision avoidance). SFTA considered combinations of circumstances that could together cause a problem. By identifying alternate ways to get to an undesirable state, the SFTA helped guide analysis of fault detectability and propagation.

As an example, we consider a portion of the SFTA for the root node ''Stereo Imaging Failure,'' shown in Fig. 2. Both a left and a right image are required for stereo imaging. The root-node failure occurs when there is either a Left Image Failure or a Right Image Failure. However, the left camera is redundant in that

Table 1 SFMECA for the image-processing request

Item	Generic failure mode	Failure mode description	Effects	Criticality	Mitigation
Request for image processing	Absent	No processing command received	Raw image not compressed; buffer limit could be exceeded; downlink stressed	Minor	Use default processing; set default to ''compressed'' to limit memory usage and bandwidth
Request for image processing	Incorrect	Processing settings may be inappropriate for conditions	Poor quality; surveillance mission or autonomous landing may require usable image	Minor to major	Restrict processing choices based on available info about mission, resource constraints
Request for image processing	Timing	Requested processing applied to earlier/later image	Delay in getting usable image	Minor	Time-tag images to detect discrepancy

there is both a grayscale and a color camera on the left side. The left image failure thus occurs only when both these cameras fail. Furthermore, for each camera, an image failure may occur due to the image being too dark or to its being too bright (saturated). The SFTAs anchored the investigation into faults that might prevent the functional requirements, such as stereo imaging, from being satisfied.

As with the SFMECAs, the number and size of the SFTAs remained relatively small. This is because the SFTAs were built primarily to develop understanding and consensus regarding feasible causes of interference with the achievement of essential capabilities (such as adequate imaging to land autonomously). This approach (targeted use of SFTA to support investigation of project-selected critical failures rather than attempted coverage of all potential failures) had been previously piloted on spacecraft software with good results in terms of cost-effective robustness analysis [10].

The SFTAs also identified environmental and operational obstacles to fulfilling requirements. For example, a strong crosswind is an environmental

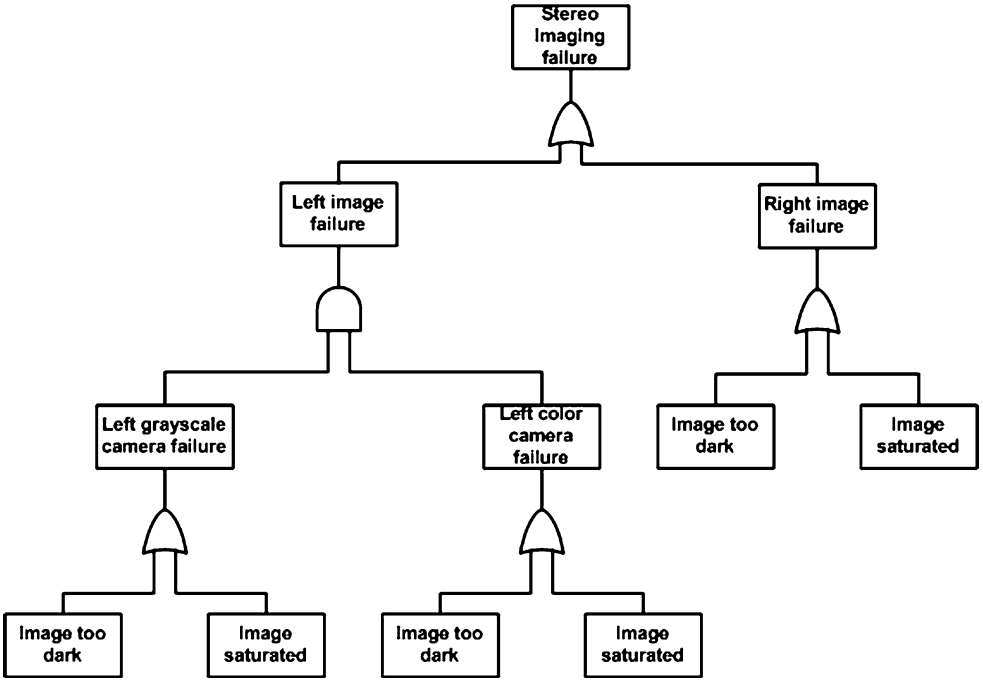

Fig. 2 SFTA for stereo imaging failure

obstacle that interferes with the camera's ability to take images, and thus with its ability to find a safe landing site. Similarly, accidentally leaving a lens cap on a camera is an operational obstacle that results in an all-black, useless image. Among other consequences, this also interferes with the rotorcraft's ability to land autonomously. Leaving the lens cap on is thus a contingency that must be considered. It has, in fact, occurred on other UAVs.

4.3 Obstacle resolution

4.3.1 Identification of alternative resolutions

Three sources were found to be useful in identifying alternative ways to resolve obstacles. The first two of these sources were the safety-analysis artifacts, the SFMECA and the SFTA. The third source was the generic obstacle resolution patterns described in Obstacle Analysis Approach section [4].

The SFMECA tables contained a ''Mitigation'' column that described ways to eliminate or mitigate the failure mode in each row. The SFTA also identified alternatives for resolving obstacles since finding a way to negate leaf nodes removed the occurrence of some obstacles. The SFTA thus encapsulated information about the goal being studied (the negation of the root node); potential obstacles to the goal (the leaf nodes of the fault tree); and insights into necessary detection mechanisms (how to determine the occurrence of the events or conditions in the nodes).

The obstacle resolution patterns also provided guidance in thinking about possible ways to handle obstacles. For example, one pattern refers to the situation where a condition persists for an interval prior to the obstacle's occurrence. In that case the obstacle can be anticipated and perhaps prevented.

The ''Agent Sub-stitution'' pattern was most frequently applicable to the autonomous handling of contingencies. This pattern captured how timeliness obstacles (such as when ground control cannot react quickly enough) could be resolved by transferring responsibility to onboard software.

4.3.2 Selection of a resolution among alternatives

Consideration of tradeoffs weighed heavily in the selection of obstacle resolutions in this application. For example, there were two different, onboard sensors, either of which could be used for range finding. However, they varied significantly in power consumption, precision, number of data points, range, and position on the vehicle. Selecting one over the other thus involved a tradeoff analysis either on the part of a ground operator or on the part of the on-board, recovery software. Other selections among alternative resolutions involved tradeoffs between color and increased memory, image compression and CPU usage, image quality and downlink bandwidth, and number of stored images vs. the size of images.

4.4 Deriving software requirements

In an example given earlier, where the obstacle to storing images was ''Images Exceed Available Memory,'' alternative resolutions included ''Reduce Number of Images To Be Stored'' and ''Reduce Size of Images To Be Stored'' (compression). Each of these resolutions itself involved refinement into several subgoals. For example, reduction of the number of images could be determined by how old the image was or by some other assigned or calculated priority measure. The calculated priority could be based on vehicle location, orientation, and camera-pointing angle or on the actual content of the image. The first option (prioritizing the images based on location, orientation, and pointing angle) yielded an approximation to the likelihood that the target of interest was captured in the image; the second option discarded images that did not include the target.

However, the first option was only feasible if the camera software could access the GPS data, which it currently could not. This is an example of what van Lamsweerde and Letier call the unrealizability problem, meaning that not all stated goals are realizable by agents in the system. They give some pragmatic conditions for unrealizability in [6]. For our application, the two most important conditions were Lack of Monitorability and Lack of Controllability. We also added a third condition, Lack of availability.

4.4.1 Missing monitorability requirements

One of the most useful results of the obstacle analysis approach was in identifying gaps between the capability of the assigned software agents to monitor for certain states or events and the need to have them do so. Most of the new software requirements found during the contingency analysis involved the dependency of certain detection, isolation, or recovery actions on specific capabilities that the software currently lacked. In terms of goal orientation, these goals were currently unrealizable. Most often these gaps involved data that the software needed to perform its functions, such as messages to which it needed to sub-scribe or resource usage states that it had to track. Identification

of missing monitor data also added visibility into the system state and defined the data prerequisites for future expansion of autonomy in those sub-systems.

4.4.2 Missing controllability requirements

Similarly, the obstacle analysis identified several instances in which the resolution involved the software being asked to set the values of variables that it did not control. For example, the software responsible for dynamically throttling the writing of images into memory based on their priority level must be able to control (i.e., change) the value of the priority threshold for grabbing images. Another example was that adjusting the jpeg quality of images in response to a low-light contingency (e.g., landing at twilight) can only be realized by software that controls the jpeg parameters. Both monitorability and controllability are important for establishing the software requirements needed for consistent increments in software autonomy.

4.4.3 Missing availability requirements

We also found it useful to add a third type of unrealizability condition, which we called an Availability Indicator. This was a textual annotation of an unrealizability condition attached to an associated alternative. The Availability Indicator addressed those situations in which the preferred alternative was not yet operational but soon would be. In particular, it documented whether the component on which a requirement depended had been installed at that point in time. In this paper we draw examples both from past software contingencies and from future, anticipated contingencies. However, in the rapidly evolving system it was essential to maintain rigor in checking consistency between a component's current availability and use of the software that depended on it.

For example, one obstacle to the goal of wireless communication that was encountered during operations was interference from other wireless devices in the vicinity. Several alternative resolutions existed to this obstacle: a return to remote (human) piloting, ignoring the risk (what is called ''live with it'' in [4]), creating an operational policy to not use the wireless channel in crowded environments, or switching communications to an alternate medium. This last alternative was the best, but required additional hardware and software that were not yet available.

In some cases, the resolution itself evolved. Here, in the short-term, the required response to detection of wireless interference was for the system to return to human control. In the long-term, once the new hardware agent and software agent are in place, the required response will be to switch communication to an alternate medium.

A single obstacle also sometimes spawned multiple new software requirements to achieve detection and resolution. For example, mitigating the obstacle where images exceed available memory involved both image compression and a ''cancel'' command to reverse acquisition of requested images that were no longer needed. In other cases one resolution could remove several obstacles. This was the case, for example, with the addition of accelerometer data on a previous helicopter [11].

4.4.4 Comparision of effort levels

In [12], van Lamsweerde gives a typical distribution of effort for a medium-sized Goal-Oriented Requirements Engineering project. A medium-sized project is defined there, perhaps optimistically, as 3–8 person months for all requirements engineering activities. Under this definition, our project is considered a large rather than a medium-sized project. We here compare that distribution with our estimated level of effort on similar tasks. Because we did not log hours spent on these sub-tasks, the comparison here is rank-ordered and anecdotal. Note that, to better match the tasks and project size listed in [12], we only report on level of effort prior to the requirements verification using automated tool support and simulation (reported below in Verifying the Contingency Requirements section).

- In [12], ''Modeling goals, objects, agents and operations'' took the most time (33%). In large part because we could leverage artifacts such as Software Fault Tree Analyses and Software Failure Modes, Effects, and Criticality Analyses (see Obstacle Identification section), the modeling itself was not as time-consuming for us. We would rank it second in level of effort.
- There, the second-highest effort level (27%) was ''Transcripts, summaries, and elicitation from additional sources.'' Unlike the projects in [12], we were working with a small, cohesive project and did not have to produce a formal requirements document in a prescribed format. Documentation was not as time-consuming and most of our additional sources were present in group meetings. We rank it fourth in level of effort.
- The third-highest effort level was ''Interviews'' (16%) in [12]. Because we depended heavily on the domain expertise of project members, most of

our understanding of goals and obstacles came from group discussions. We would thus also rank this as third in the level of effort.
- The fourth-highest effort level in the earlier projects was ''Others.'' There was no description of the tasks contained in ''Others,'' so there is no basis for comparison. We exclude it here.
- The most striking difference from the projects in [12] is that while ''Model validation with stakeholders, negotiation of alternatives, revision, and documentation'' was ranked fifth there (9%), we would rank it first. In particular, understanding, and correctly expressing the alternative choices for resolving obstacles took a great deal of effort and iteration. In addition, while the earlier projects aimed at a single delivery, we were supporting the rapid evolution of an operational system toward greater autonomy, so updates were on-going.

To summarize, the most striking contrast between the typical project in [12] and ours was that a greater percentage of our time was spent with domain experts to understand the obstacles and feasible alternatives, as well as to understand the implications of future, incremental autonomy. The value of this comparison appears to lie primarily in its indication that lightweight, flexible use of obstacle analysis to leverage existing project artifacts can save time for the project, and that, for safety-critical, autonomous systems, the thorough analysis of alternatives for obstacle resolution is difficult and time-consuming.

5 Implications for requirements evolution

Systems that experience requirements evolution after deployment challenge the continued adequacy of previous anomaly handling strategies. When the evolution is toward additional autonomy, the challenges are multiplied. In this section we discuss some ways in which obstacle analysis can help and some areas in which more work is needed.

5.1 Validity of existing requirements must be maintained

When requirements changed, a key use of obstacle analysis was to confirm that previously existing software requirements to detect, isolate, and respond to contingencies were still valid. This involved checking that for every previously identified obstacle to a goal that could still occur, the previously identified resolution (usually a derived software requirement) could still handle the obstacle. For example, when the capability was added for autonomous pivoting of the vehicle around a target, we had to check that the current handling of the obstacle ''communication lost'' remained valid.

5.2 Evolution tends toward more autonomy

In general, the evolving requirements produced greater autonomy. Enhancements to the rotorcraft provided new ways to detect, identify, or respond to existing contingencies. Often these enhancements resulted in new sub-goals (added autonomous functionality) and in new ''OR'' branches for the obstacle resolution model (new alternatives for how to handle contingencies). Most typical was the replacement of a sub-goal leaf node assigned to a human agent by a sub-goal tree with the new leaf nodes assigned to software agents.

Simple hardware agents (e.g., a camera affixed in place) tended to be replaced by more sophisticated hardware agents (e.g., articulated stereo cameras that swivel up and down) that made feasible new, alternative monitoring sub-goals for contingency detection, or alternative control sub-goals for contingency recovery. New software agents (e.g., the capability to dynamically add collision-avoidance targets to the path-planning calculation) offered improved autonomous capabilities for responding to contingencies and resulted in more recovery options.

5.3 Autonomy adds complexity

As more autonomy was required, new obstacles and dependencies were also introduced. That is, with the addition of new agent capabilities came the possibility of new contingences. For example, the addition of a new laser brought with it the failure modes of the laser to be considered, as well as whether these failure modes were detectable on the ground and by onboard software. Some new agents also resulted in new requirements for calibration before use.

More interestingly, the evolving requirements entailed the need to identify new feature dependencies (e.g., between the fidelity of color images and passive-range algorithms). While the focus of incremental autonomy tended to be on what was *gained* in terms of more robust handling of contingencies, contingency analysis also looked at the potential *risks introduced* by the new software complexity. Contingency analysis investigated the failure modes for new agents, new opportunities for feature interactions, and new possibilities for conflicts among goals (most commonly in terms of resource contention).

Additional issues such as mixed-initiative control (where the rotorcraft receives inconsistent commands from the onboard software, the ground software, and the remote, human pilot), sensor fusion problems (where the replacement of a single sensor by a suite of perhaps heterogeneous sensors requires the software to compose the data and handle data inconsistencies), and coordination problems (where a fleet of rotorcraft must coordinate their movement and resource usage), were not obstacles in the current system but are potential, future obstacles. Our experience to date leads us to anticipate that obstacle analysis can scale to address the additional complexity in these interactions.

An unexpected finding was that sometimes the requirements for autonomy were reduced. In these cases some existing autonomous features were disabled and some control was moved from the onboard software to human ground control. This reduction of autonomy usually occurred temporarily for a demonstration or test of a new component or features. Since these instances often did not involve a simple rollback to a previous version but instead used a pruned version of the current software, verification that the reduced requirements still maintained the required obstacle handling had to take place.

5.4 Additional obstacle-refinement patterns needed

Two areas in which existing obstacle analysis techniques provided only limited guidance for the system studied were: (1) in analyzing failure isolation and (2) in identifying feature interactions. With regard to failure isolation, it was often easier to determine that a failure had occurred (detection) than it was to figure out precisely what had happened and how to prevent it from propagating (isolation). For example, if downlink communication stopped, it was easy to detect that a failure had occurred but could be quite difficult to isolate the problem. We are thus working to extend the obstacle refinement patterns to more explicitly address failure isolation issues in this domain.

With regard to detecting interactions as new features are added, we found that guidelines described by Doerr for identification of feature interaction in product lines were readily extensible to our application [13]. An example of a guideline that was useful here is that, if feature B uses feature A, then all features that also use feature A must be identified (to illustrate, Doerr gives an example from the mobile phone domain, where both sending a short message and placing a call use the network component. To avoid conflicts, it is important to identify that both features use the same component). Doerr's guidelines supplement the patterns for finding divergence among goals (i.e., inconsistencies among goals at a boundary condition) [4] in identifying feature interactions.

6 Related work

The investigation reported here built on previous results in requirements evolution. However, our effort differed from most earlier work in that we focused on the requirements evolution of a safety-critical system during post-deployment operations.

Much of the existing work in requirements evolution addresses the pre-implementation phases of a system. Goal-oriented requirements engineering techniques have been widely used to identify, specify, and reason about software requirements and non-functional goals [14]. Anton and Potts, for example, have used goals and obstacle analysis to refine evolving requirements in a developing system [15]. There have also been studies describing agile approaches for handling rapidly evolving systems (e.g., the evolutionary prototyping in [16]). Such approaches are recommended for market-driven domains such as e-commerce rather than for critical systems.

Requirements evolution post-deployment has been studied primarily from the viewpoint of how it can be managed. The focus has been on establishing processes to scope or evaluate proposed changes, e.g., in terms of traceability [17] or change-impact studies. Similarly, maintenance methods have tended to focus on classifying and managing requirements changes rather than on analyzing changes [18, 19].

Feather and Fickas have instead proposed monitoring operational systems for mismatches that develop between the assumptions underlying requirements and the current environment. They, like us, used goal-oriented requirements engineering to model possible alternative behaviors. They described ''remedial evolutions,'' somewhat similar to our evolving obstacle resolutions, when such mismatches occur [20]. Much earlier, Heninger reported assembling a list of ''feasible changes'' on the A-7 project that might be able, in the future, to invalidate current fundamental assumptions about the system [21]. An example of a feasible change was ''computer self-test might be required in the air (at present it is required only on the ground).'' Berry, Cheng and Zhang have proposed a goal-based structuring mechanism for investigating requirements for dynamically adative systems [22]. In other goal-oriented work on requirements for evolving systems, Hui, Liaskos, and Mylopoulos have described a

framework for reasoning about personal, customizable software [23].

The domain of concern in most requirements evolution work has been the business environment rather than critical systems, as here. DeLemos, however, modeled an operational system in which requirements evolution (automating the self-destruct feature of a rocket) was structured so that architectural components remained unchanged while their interactions adapted to the changed requirements (specifically, automating the self-destruct feature of a rocket) [24]. Lutz and Mikulski also showed how requirements evolved during operations to compensate for safety-critical anomalies caused by hardware degradation or the occurrence of rare events in seven spacecraft systems [25, 26].

Several recent papers described autonomy requirements, including fault handling, for existing or planned space missions [27, 28]. Other researchers, motivated by problems with fault identification on rovers, have presented improved algorithms for fault detection or responses. For example, Dearden et al. generated contingency plans for rovers in the presence of uncertainty regarding timing and resources [2]. Verma, Langford, and Simmons present an algorithm for estimating the dynamic state of a system (e.g., fault identification) from noisy measurements of continuous variables [29]. The algorithms in these studies suppose that requirements for fault and contingency monitoring and handling (the problem addressed in this paper) are already defined.

A few researchers have specifically addressed safety in autonomous systems. For example, Fox and Das described the deployment of software agents for intelligent decision-making in safety-critical medical applications [30]. The issue of adjustable autonomy was raised by Schreckenghost et al. in the context of space life support systems where a human may need to override autonomous control when an anomaly occurs [31]. A European Space Agency ESTEC project investigated how to ensure safety and dependability of autonomous space software, based on lessons learned from non-space autonomous domains [32]. Among their recommendations is a ‘‘safety bag’’ or safety supervisor that checks constraints at execution time, while Failure Detection, Identification and Recovery (FDIR) is handled by a separate module.

The work described here also builds on previous work in vehicle health management. Patterson-Hine et al. investigated potential failures or malfunctions of engine and thruster components on a helicopter, together with the effects on the system and the visibility into faults obtainable on the ground [11]. Whalley et al. sub-sequently described the challenges involved in using vehicle health modeling of a UAV to assist in automated transition from remote control of the vehicle to computer control [5]. Achieving the transition will require improved contingency analyses and helped motivate the work described in this paper.

7 Verifying the contingency requirements

The verification of the identified contingency requirements on the rotorcraft involved both model-based static analysis and dynamic simulation of auto-generated code implementing the requirements. Since we were especially concerned with the monitorability, controllability, and availability of the contingency requirements, we used the Testability Engineering and Maintenance System (TEAMS) toolset from QSI [33]. The TEAMS has strong support for the diagnosability analysis of models, thus allowing verification that all the data channels needed to monitor and control behavior (sensor inputs and command outputs) currently are available in the system. Our use of TEAMS to analyze the contingencies is described more fully in [34].

Testability Engineering and Maintenance System is a commercial tool developed to support the modeling and diagnosability of avionics and other systems. It won a NASA Space Act Award and has been successfully used in development of the second-generation reusable launch vehicle [35]. Given the toolset's potentially widespread use at NASA, investigation of the feasibility of integrating obstacle analysis with it was of special interest.

The contingency requirements for stereo imaging in the Camera Sub-system of the rotorcraft were described in a manually constructed TEAMS model. The top-level model, a graphical portion of which is shown in Fig. 3, shows the three cameras (left and right grayscale and left color), the vision-processing computer, and the range-processing components (not discussed here). The model was hierarchical with each component refined at successively lower levels into sub-components. The lowest level of each sub-component also represented possible failures (run-time obstacles) associated with that sub-component. Test points were placed in the model to indicate where data was available to monitor for the occurrence of the various failures, and commandable recovery actions were associated with the results of the monitoring activity. For example, if the image from the Color Camera was too bright to provide adequate stereo imaging, the resolution was to desaturate the camera.

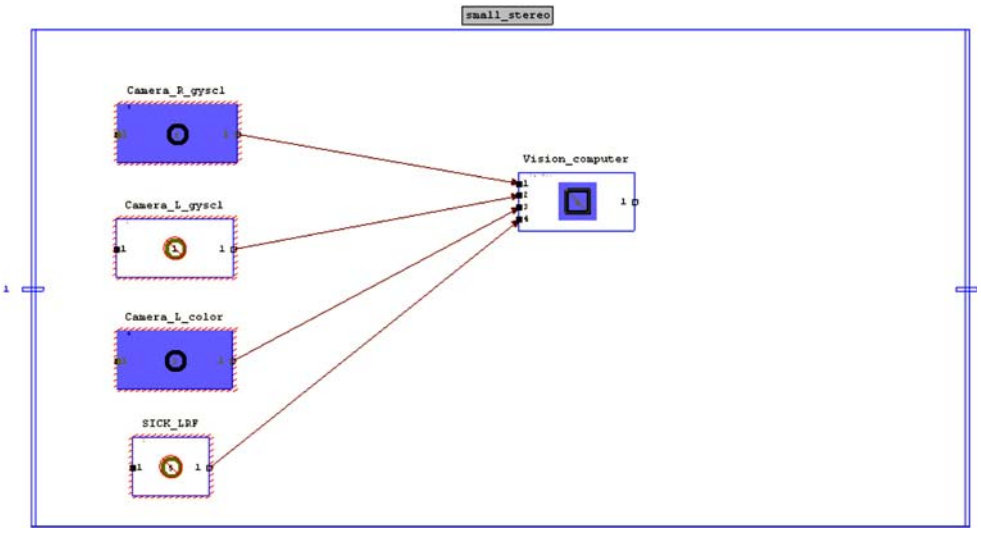

Fig. 3 Top-level TEAMS model

Testability Engineering and Maintenance System automatically produced a diagnostic tree from the model that showed an optimized sequence of checks for the system's correct functioning together with the action to take if a check failed. The optimization was based on user-assigned parameter values such as priority or resource-usage of the check.

Figure 4 shows a small portion of the diagnostic tree that was generated by the tool. The labeled box "5" refers to the continuation of this part of the Diagnostic Tree on other windows. If, with the Right Image having failed, we check the Left Image and find that it is good (left branch of Fig. 4) then we have isolated the problem to the Right Camera. However, if the Left Image is also bad (right branch), then the Stereo Processing is isolated as the problem source. We used the tool's diagnostic-tree capability to help verify the adequacy of the modeled requirements for monitoring and resolving contingencies. Failures or anomalies that could not be distinguished from each other in the as-modeled system were identified by the tool as an ambiguity group.

If a failure lacked monitorability (i.e., could not be uniquely identified with the available data), it appeared in an ambiguity group. For example, at one point the as-modeled system lacked the monitoring capability to distinguish inadequate stereo imaging due to a camera's dirty lens from inadequate stereo imaging due to a range-calculation failure. Stereo imaging, it will be remembered, is a sub-goal of safe, autonomous landing, and both dirty camera lenses and stereo range calculation are obstacles to this sub-goal. The diagnostic tree confirmed that these two obstacles were not distinguishable in the modeled system at that point in time. Similarly, inspection of the diagnostic tree could reveal run-time obstacles that were adequately identified but that had no associated resolution (e.g., due to lack of controllability).

To perform dynamic verification of the requirements, we developed a translator that took the diagnostic tree produced by TEAMS and available in XML format, and output it in the language of APEX, the rotorcraft's autonomous reactive planner [5]. This permitted a demonstration of hardware-in-the-loop simulation of the contingency monitoring and contingency-handling requirements.

The checks and resolution actions for handling some key obstacles to stereo imaging, expressed in the TEAMS model's diagnostic tree and auto-translated into the planner's language, were executed on the rotorcraft while it was functioning but on the ground. Some obstacles to stereo imaging in the demonstration were the left grayscale camera failing; the backup, left color camera being too dark for good imaging; and the color camera becoming saturated (too bright). Obstacles were simulated (e.g., by manually covering the lens

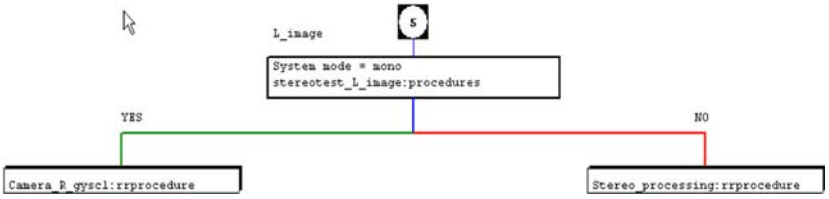

Fig. 4 Excerpt from a Diagnostic Tree

cap to cause an all-black image) and the adequacy of the monitorability, controllability, and availability requirements for these contingencies was verified. This simple verification, while it found no additional requirements issues, showed the feasibility of integrating early obstacle analysis with sub-sequent tool-based modeling and automated output to the system's reactive planner.

8 Conclusion

The results reported here indicate that the use of obstacle analysis to reason about software requirements for handling contingencies has several advantages. Obstacle analysis gives a structured way to reason incrementally about new alternatives for handling contingencies that can occur during operations. The capacity for incremental reasoning is especially important in systems that are both currently operational and evolving rapidly to add autonomous features.

Obstacle analysis also supports evaluation of the continued validity of existing software contingency requirements as the system and the requirements evolves. The cyclical nature of goal-oriented requirements engineering, in which new goals are introduced to resolve an obstacle, but must then also be included in an iterative analysis for new risks, is a good match with safety-critical systems whose requirements continue to evolve after deployment.

We made several minor adjustments to the standard form of obstacle analysis to better fit our focus on contingencies. First, we found that existing safety-analysis artifacts (SFMECA and SFTA) were useful and efficient baselines for identification and refinement of obstacles. This suggests that it may be relatively easy for projects that already produce traditional safety-analysis documentation to adopt obstacle analysis to supplement their existing analysis techniques. Second, we added to the analysis of alternative obstacle resolutions an explicit indicator of whether the required agent was currently available. This was because some alternatives for contingency detection and handling were not currently feasible in the system, but would be so in the near future. Third, we found a need for additional attention to feature dependencies and to fault-isolation problems, and are working to extend the obstacle-refinement patterns in those directions.

The objective of the requirements evolution was for the software to handle more faults and anomalous situations autonomously. By supporting the identification of software contingency requirements, obstacle analysis contributed to the building of a more robust system.

Acknowledgments The research described in this paper was carried out in part at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautic and Space Administration and funded by NASA's Office of Safety and Mission Assurance Software Assurance Research Program. The first author's research is supported in part by National Science Foundation Grants 0204139, 0205588, and 0541163. The authors thank Matt Whalley and the other members of the Autonomous Rotorcraft Project team for sharing their expertise and enthusiasm. The authors thank QSI for assistance with the TEAMS toolset. The first author also thanks Martin Feather and Axel van Lamsweerde for insightful feedback on an early draft.

References

1. Parnas DL, Wurges H (2001) Response to undesired events in software systems. In: Hoffmann DM, Weiss DM (eds) Software fundamentals, collected papers by David L. Parnas, Addison-Wesley, Reading, pp 231–246
2. Dearden R et al (2002) Contingency planning for planetary rovers. In: Proceedings of the 3rd Int'l NASA workshop planning and scheduling for space, Houston
3. Johnson T, Sutherland H, Bush S (2001) The TRAC mission manager autonomous control executive. In: Proceedings of the IEEE aerospace conference, Big Sky, MT, USA
4. van Lamsweerde A, Letier E (2000) Handling obstacles in goal-oriented requirements engineering. IEEE TSE 26(10):978–1005
5. Whalley M, Freed M, Takahashi M, Christian D, Patterson-Hine A, Schulein G, Harris R (2003) The NASA/Army autonomous rotorcraft project. In: Proceedings place of American helicopter society 59th annual forum, Phoenix, AZ, USA
6. Letier E, van Lamsweerde A (2002) Agent-based tactics for goal-oriented requirements elaboration. In: Proceedings of the 24th ICSE. ACM Press, New York, pp 83–93
7. Letier E, van Lamsweerde A (2002) High assurance requires goal orientation. In: Proceedings of the international workshop requirements for high assurance system, Essen, Germany
8. Easterbrook S, Lutz R, Covington R, Kelly J, Ampo A, Hamilton D (1998) Experiences using lightweight methods for requirements modeling. IEEE Trans Softw Eng 24(I):4–14
9. Lutz R, Woodhouse R (1997) Requirements analysis using forward and backward search. Ann Softw Eng 3:459–475
10. Lutz R, Shaw H-Y (1999) Applying adaptive safety analysis techniques. In: Proceedings of the 10th international symposium software reliability Eng (ISSRE'99), Boca Raton, FL, USA
11. Patterson-Hine A, Hindson W, Sanderfer D, Deb S, Domagala C (2001) A model-based health monitoring and diagnostic system for the UH-60 Helicopter. In: Proceedings of the American helicopter society 57th annual forum. AHS, Washington
12. Van Lamsweerde A (2004) Goal-oriented requirements engineering: a roundtrip from research to practice. In: Proceedings of the 12th IEEE international requirements engineering conference, Kyoto, Japan
13. Doerr J (2002) Requirements engineering for product lines. Diploma thesis, University of Kaiserslautern
14. Mylopoulos J, Chung L, Yu E (1999) From object-oriented to goal-oriented requirements analysis, CACM 31–37

15. Anton A, Potts C (1998) The use of goals to surface requirements for evolving systems. In: Proceedings of the 20th ICSE, Computer Society, Silver Spring, pp 157–166
16. Carter A, Anton A, Dagnino A, Williams L (2001) Evolving beyond requirements creep: a risk-based evolutionary prototyping model. In: Proceedings of ISRE, Toronto, Canada, pp 94–101
17. Cleland-Huang J, Chang C, Christensen M (2003) Event-based traceability for managing evolutionary change. IEEE Trans Softw Eng 29(9):796–810
18. Bennett K, Rajlich V (2000) Software maintenance and evolution: a roadmap. In: Finkelstein AF (ed) The future of software engineering. ACM Press, New York, pp 75–87
19. Lehman MM, Ramil JF (2001) Rules and tools for software evolution planning and management. Ann Softw Eng 11:15–44
20. Feather M, Fickas S (1995) Requirements monitoring in dynamic environments. In: Proceedings of the ICRE, York, UK, pp 140–147
21. Heninger K (2001) Specifying software requirements for complex systems: new techniques and their application. In: Hoffmann DM, Weiss DM (eds) Software fundamentals, collected papers by David L. Parnas. Addison-Wesley, Reading, pp 111–135
22. Berry DM, Cheng BHC, Zhang J (2005) The four levels of requirements engineering for and in dynamic adaptive systems. In: Proceedings of the workshop on the design and evolution of autonomic application software, St Louis, MO, USA
23. Hui B, Liaskos S, Mylopoulos J (2003) Requirements analysis for customizable software goals-skills-preferences framework. In: Proceedings of the 11th IEEE international requirements engineering conference (RE'03), Monterey Bay, CA, USA, pp 117–126
24. deLemos R (2000) Safety analysis of an evolving software architecture. In: Proceedings of the 5th IEEE International symposium high assurance systems, Computer Society, Silver Spring, pp 159–167
25. Lutz R, Mikulski I (2003) Operational anomalies as a cause of safety-critical requirements evolution. J Syst Softw 65(2):155–161
26. Lutz R, Mikulski I (2004) Empirical analysis of safety-critical anomalies during operations. IEEE TSE 30(3):172–180
27. Brat G, Drusinsky D, Giannakopoulou D, Goldberg A, Havelund K, Lowry M, Pasareanu C, Venet A, Visser W, Washington R (2004) Experimental evaluation of verification and validation tools on Martian rover software. Formal Methods Sys Design 25(2–3):167–198
28. Chien S et al (2001) Onboard autonomy on the three corner sat mission. In: Proceedings of the international symposium AI, robotics, and automation for space. IEEE, Montreal
29. Verma V, Langford J, Simmons R (2001) Non-parametric fault identification for space rovers. In: Proceedings of the international symposium AI and robotics in space, Montreal, Quebec, Canada
30. Fox J, Das S (2000) Safe and sound, artificial intelligence in hazardous applications. AAAI Press, Menlo Park
31. Schreckenghost D, Malin J, Thronesbery C, Watts G, Fleming L (2001) Adjustable control autonomy for anomaly response in space-based life support systems. In: IJCAI-01 workshop autonomy, delegation and control: interacting with autonomous agents, Seattle, Washington, USA
32. Software product assurance for autonomy on-board spacecraft, European space agency ESTEC. ftp.estec.esa.nl/pub/tos-qq/qqs/SPAAS/StudyOutputs
33. Qualtech Systems Inc, http://www.teamqsi.com
34. Lutz R, Patterson-Hine A, Bajwa A (2006) Tool-supported verification of contingency software design in evolving, autonomous systems. In: Proceedings of the 17th IEEE international symposium software reliability engineering (ISSRE'06), Raleigh, NC, USA
35. Dixon RW, Hill T, Williams KA, Kahle W, Patterson-Hine A, Hayden S (2003) Demonstration of an SLI vehicle health management system with in-flight and ground-based subsystem interfaces. In: Proceedings of the IEEE aerospace conference, Big Sky