

Using an Assurance Case to Support Independent Assessment of the Transition to a New GPS Ground Control System

Elisabeth A. Nguyen¹, William S. Greenwell¹, Myron J. Hecht²

The Aerospace Corporation

¹Chantilly, Virginia, USA; ²El Segundo, CA, USA

{enguyen, william.s.greenwell, myron.j.hecht}@aero.org

Abstract

We describe a specific application of assurance cases to the problem of ensuring that a transition from a legacy system to its replacement will not compromise mission assurance objectives. The application in question was the transition of the Global Positioning System (GPS) to a new ground-control system. The transition, which took place over five days, required uninterrupted control of the GPS satellite constellation while control was transferred from a 1970s-era mainframe to a distributed architecture. We created an assurance case so that the procedural documentation we had could be restructured into a form amenable to analysis. The analysis concluded that there were no major hazards; this conclusion was validated by a successful transition.

1. Introduction

On September 14, 2007, the U.S. Air Force replaced the ground-control system for the Global Positioning System (GPS) [1]. The new system, known as the Architecture Evolution Plan (AEP), replaced a legacy control system (referred to as Legacy) built on 1970s-era mainframe computers. Since GPS is used worldwide as a navigation aid, it was essential that the transition was executed without disrupting the GPS navigation signals.

The Air Force asked The Aerospace Corporation to analyze the AEP transition plan from a mission assurance perspective and document any risks that were discovered. The scope of this assessment was limited to the ground-control system as replacement of the system was intended to be transparent to the GPS satellites.

We chose to use an assurance case, expressed in the Goal Structuring Notation (GSN) [2], to structure the assessment. We had experience with assurance cases, and believed that GSN would support our assessment goals. This assurance case was unique in that it focused on the *transition* to the new system and not the system itself. Legacy was assumed to provide adequate service based on its service history. AEP was assumed to provide adequate service based on other analyses. The challenge we faced

in this work was in applying a technique intended for a *system* made up of *states* to a *process* made up of *steps*; the system states were not defined explicitly in our documentation, which consisted of operational procedures. Our solution was to define a series of phases composed of sets of process steps. In each phase, the system was defined as having a single state. The states we constructed reflected the gradual shift in responsibility from Legacy to AEP. We hypothesized that restructuring our procedural documentation into a state-based argument would make it easier to find risks in the transition plan.

The assurance case demonstrated to the Air Force that the transition posed no major mission assurance concerns. The most significant finding was lack of documentation for some procedures; we later established that the documentation was available in another form. The strength of the assurance case, along with the many other tests and analyses that were conducted to ensure continuity of service during and after the transition, contributed to the decision to proceed with the transition.

Some of the specifics of the system and its assurance case have been adapted for publication. The alterations abstract away some detail but do not alter the substance.

2. The GPS System

The GPS system includes: a constellation of at least 24 satellites, which provide time and position signals (*navigation messages*) to users [3]; a ground control system; and user GPS receivers. The transition involved the Operational Control System (OCS), part of the ground-control system, which consists of: (1) the Master Control Station (MCS), the central facility for satellite control; (2) *monitoring stations* that monitor the accuracy of the navigation messages; and (3) *ground antennas*, which receive telemetry (status information) from the satellites and upload commands or data when necessary.

Figure 1 shows a simplified view of GPS as a closed-loop system for minimizing navigation error. The navigation messages are received at the monitoring stations at precisely surveyed locations. At the MCS,

location errors and clock offsets are calculated from this data. Next, Kalman filters are used to predict future orbit and clock offsets. The MCS then transmits the predictions to the ground antennas, which upload the predictions to the satellites. The satellites then use these data to generate the navigation messages. The feedback occurs when the monitoring stations transmit measured signal parameters back to the MCS, which then recalculates the orbit and clock parameters for the next message cycle.

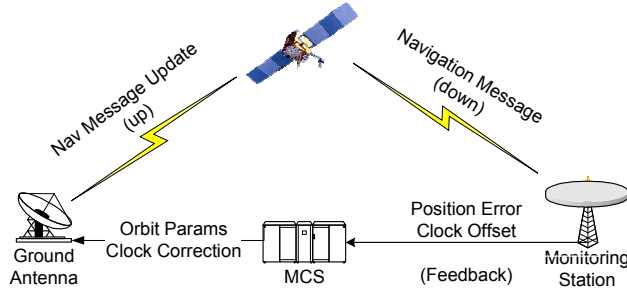


Figure 1. Simplified GPS Navigation Message Feedback Loop

The primary function of the OCS is to support the navigation message feedback loop. It also: (1) supports telemetry, tracking, and commanding of the satellites to keep them in the appropriate orbits; (2) provides data to the National Geospatial-Intelligence Agency (NGA), which also monitors the navigation signal, and to other

U.S. Government agencies; and (3) provides diagnostic data to the GPS satellite manufacturers.

Because of the importance of the navigation uploads, the OCS Kalman filter results contained in the upload message were a key issue of the study. Both Legacy and AEP use the same filtering algorithm, but they provide slightly different results under some circumstances. The concerns were that either AEP's implementation would not be sufficiently accurate, or the slight difference would cause a discontinuity in received data when the first AEP uploads to the satellites occurred. The assurance case also addressed the continuity and correctness of telemetry, tracking and commanding functions and data provided to external interfaces.

3. The OCS Transition

To maintain uninterrupted control of the GPS satellite constellation during the transition, taking the OCS offline was unacceptable. Instead, the transition entailed parallel operation of the Legacy and AEP systems as control was transferred incrementally to AEP. This process was called the Enhanced Phased Operations Transition (EPOT); it consisted of four increments, or *phases*. Each phase had specific entry and exit criteria. The EPOT phases, along with the assurance objectives that needed to be met for those phases, are listed in Table 1.

Table 1. EPOT Phases and Assurance Objectives

Phase	Phase Description	Assurance Objective
0	Legacy is the source of operational data, and AEP has not yet been physically connected to operational portions of the system.	None needed; Legacy is assumed to provide adequate service. AEP is silent and so cannot interfere.
1	Legacy is the source of operational data, but AEP is performing calculations to shadow Legacy. AEP shadows Legacy to provide sufficient time for AEP's Kalman filters to be synchronized with Legacy's and to provide a final test of AEP functionality.	Show why AEP will not hinder system operations at this point.
2	AEP is the source of operational data, but it does not yet have control of ground antennas or monitoring stations. Legacy can use ground antennas and monitoring stations to resume operation if AEP exhibits anomalies.	Argue that AEP will provide service; that Legacy will not hinder AEP; and that AEP can use NGA and alternate transmission facility instead of the monitoring stations and ground antennas.
3	AEP is the operational source of data, and operational control of ground antennas and monitoring stations is being transferred to AEP. At the end of the phase, AEP has complete control of interfaces.	Argue that AEP will provide service; that Legacy will not hinder AEP; and that AEP can use the mix of NGA, alternate transmission facility, monitoring stations, and ground antennas to provide service.

Parallel operation of the two systems required duplicating connections to outside data sources. Input from the monitoring stations was needed to provide signal error data to the Kalman filters running in both systems; NGA data was also available, but the filters needed to be trained on the same data to be comparable. During Phases 0-2, Legacy forwarded the monitoring station data to AEP. At the beginning of Phase 3, Legacy's monitoring

station connection was terminated so that the monitoring stations could be transferred to AEP control. At this point, the AEP Kalman filters would start to diverge from the Legacy filters because of the difference in data sources.

Only one version of the system could be connected to the ground antennas at a time. AEP used an alternate transmission facility for EPOT Phase 2 before assuming control of the ground antennas in Phase 3.

4. Transition Assessment

Our assessment was conducted by two of the authors and took three person-months. Other staff of The Aerospace Corporation assisted with the assurance case as needed, including two domain experts. One expert had 23 years of experience with the GPS ground control system; both had been involved in AEP’s development.

The assessment was conducted at a relatively high level of abstraction, both because of time constraints and because functional redundancy in the system and procedures meant that the correct operation of any particular system mechanism was not critical. The assessment considered the system as a whole; it was complemented by other, more focused studies and by transition rehearsals.

The assurance case went through multiple review cycles by software colleagues and domain experts until we were satisfied that no unaddressed argument goal posed a significant risk to transition success.

4.1. Goal and Approach

The goal of the transition assessment, derived from the GPS Transition Plan [3], was to show that the transition would be conducted so as to minimize the operational impact to GPS users (that is, navigation and external interface users). An argument for assurance of the transition plan was not explicitly documented prior to this effort; however, the high-level structure of the argument could be gleaned from several sources [3, 4]. We constructed an assurance case to document the implicit argument for the effectiveness of the transition plan and supplemented the preexisting argument with our own observations. Specifics of the assurance case, including most of the evidence used to support its claims, are based on a checklist that provides detailed steps to be performed during each transition phase.

To create the argument structure, we derived a set of system states from the checklist and then argued that the system was safe (1) when it was in each state, and (2) during each transition between states. Our strategy in creating the states was to consider not just the Legacy system or the AEP system, but the combined Legacy-AEP super-system for ground control.

Creating super-system states enabled us to represent the gradual transfer of responsibility between systems as a set of sequential state changes. Our super-system configurations are composed of a set of variables whose values represent which system—Legacy or AEP—is responsible for carrying out each system function. It also includes variables whose values represent how recently the Kalman data for each system was updated by the monitoring stations, so that we could ensure that stale data was not used to provide service to an interface.

We created a matrix to relate procedural steps from the checklist to the system state variables we identified. This ensured that we had not missed any transient states. For example, we found a state where both Legacy and AEP controlled an interface; we then verified that operational procedures would preclude a conflict. We partitioned the matrix into regions in which the values of the state variables remained fairly stable as the transition proceeded. This partitioning gave rise to a sequence of system configurations in which responsibilities were clearly assigned to either Legacy or to AEP. Figure 2 provides an example of where a partition boundary was drawn (with some columns elided for reasons of space). The sequence of configurations aligned with the phases set out in the transition plan, validating our analysis and providing additional confidence in the plan.

4.2. Decomposition Strategy

The transition phases were chosen by the contractor to align with significant events during the transition. Our state variable analysis also indicated a correspondence

Steps to be performed during transition	Individual super-system state variables					Super-system configuration (phase) system is in at transition step
Action	Monitoring Data	Satellite Uploads	NGA	Kalman Data - Legacy	Kalman Data - AEP	System Configuration
[Procedure step]	Parallel L-band, NGA backup	Legacy control, AEP shadow, AFSCN backup	Legacy, AEP shadow	Fresh	Fresh	Legacy operational; AEP shadows operations (Phase 1)
[Procedure step]	Parallel L-band, NGA backup	Legacy control, AEP shadow, AFSCN backup	AEP, Legacy shadow	Fresh	Fresh	AEP operational; Legacy controls MSs (Phase 2)

Figure 2. Excerpt from Matrix Relating Procedural Steps to State Variables

between transition phases and the division of system responsibilities. Together, these factors suggested that the phases were an appropriate dimension along which to decompose the assurance case.

In addition to the transition plan, however, there was also a contingency “fallback” plan in which operations could revert to Legacy in the event of unforeseen problems. To account for the fallback plan in the assurance case, we first decomposed the argument into two convergent branches: one arguing that the transition would be successful and another arguing that fallback to Legacy was possible from any step in the transition. We then decomposed each branch by transition phase.

We describe the first branch of the assurance case in Section 5. While our analysis revealed no evidence that fallback would be problematic, we were unable to obtain sufficient documentation on fallback to complete this branch of the argument. We recommended, however, that the lack of argument for fallback was not a high enough risk to warrant postponing the transition, for three reasons. First, fallback was only a contingency plan and would not be needed at all if the main branch of the argument (normal transition) held. Second, if both normal transition and fallback experienced problems, the satellites would be able to operate adequately for enough time that the problem could likely be solved. Third, fallback scenarios were executed successfully during EPOT rehearsals.

5. Assurance Case

We expressed the EPOT assurance case in the Goal Structuring Notation (GSN) [2]. GSN enables graphical depiction of an argument structure. In GSN, an initial top-level assurance goal is decomposed, using strategies, into subgoals, repeating the decomposition process until the argument can be supported by direct evidence. We believe that representing the argument graphically makes its structure more explicit and, hence, more amenable to analysis than it would be in a textual form [2]. The elements of GSN used here are shown in Figure 3.

5.1. Top-Level Argument

The top-level argument for the EPOT assurance case is shown in Figure 4. It begins with the top-level goal—**GTopLevel**—that EPOT will be conducted so as to minimize the operational impact to users. The argument then decomposes the top-level goal into two subgoals. **GContinuityOfService** supports EPOT correctness, and **GFallbackPossible** supports the capability to fall back. These goals are, in turn, supported by their respective branches of the argument, described below.

5.2. Argument Leg Supporting EPOT Adequacy

This argument leg uses system context to define “adequacy” as service that is consistent with the service provided by Legacy. The argument is then decomposed by EPOT phase. **StEPOTPhaseDecomp** refers to these phases; the phases themselves inform the strategy, so they are included as context in **CEPOTPhases**. This decomposition strategy produces three more subgoals.

GEPOTPhase_i is a replicated subgoal (denoted by 0..3 on the arrow from the strategy) representing the four different generated subgoals that correspond to the four different phases of EPOT. **GPhaseTransitions** ensures that service is not interrupted during state transitions. For reasons of space, we present only the interesting findings from the remainder of the argument for these goals.

GPhaseDecompValidity shows that decomposing the argument based on the phases was appropriate. The detailed state analysis described above was used to support this goal; that analysis is included as evidence (as noted in the diagram by its Aerospace report number).

Three argument branches show adequacy for specific transitions (**GPhaseTransitions**). (1) Phase 0 to 1 and 1 to 2 transfers: service is adequate because Legacy provides service throughout. (2) Phase 2 to 3 transfer: service is adequate because the transition is immediate. (3) A separate, convergent argument strengthens the previous two by showing that all of the transition intervals are shorter than the allowable outage time.

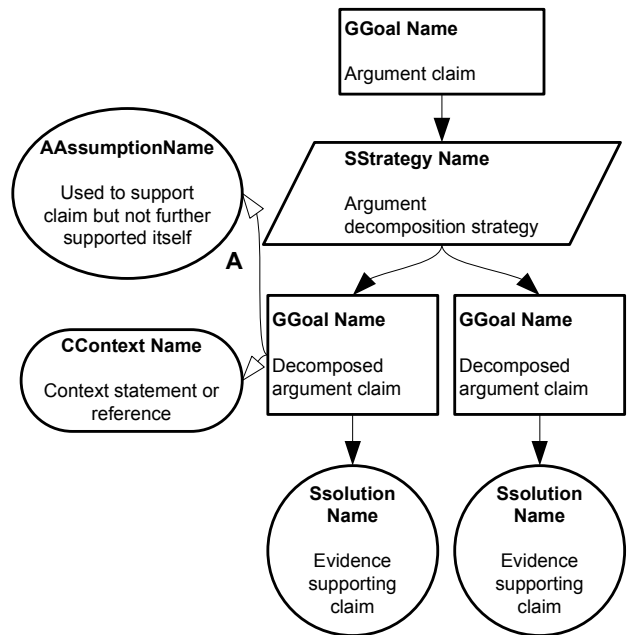


Figure 3. GSN Elements in Assurance Case

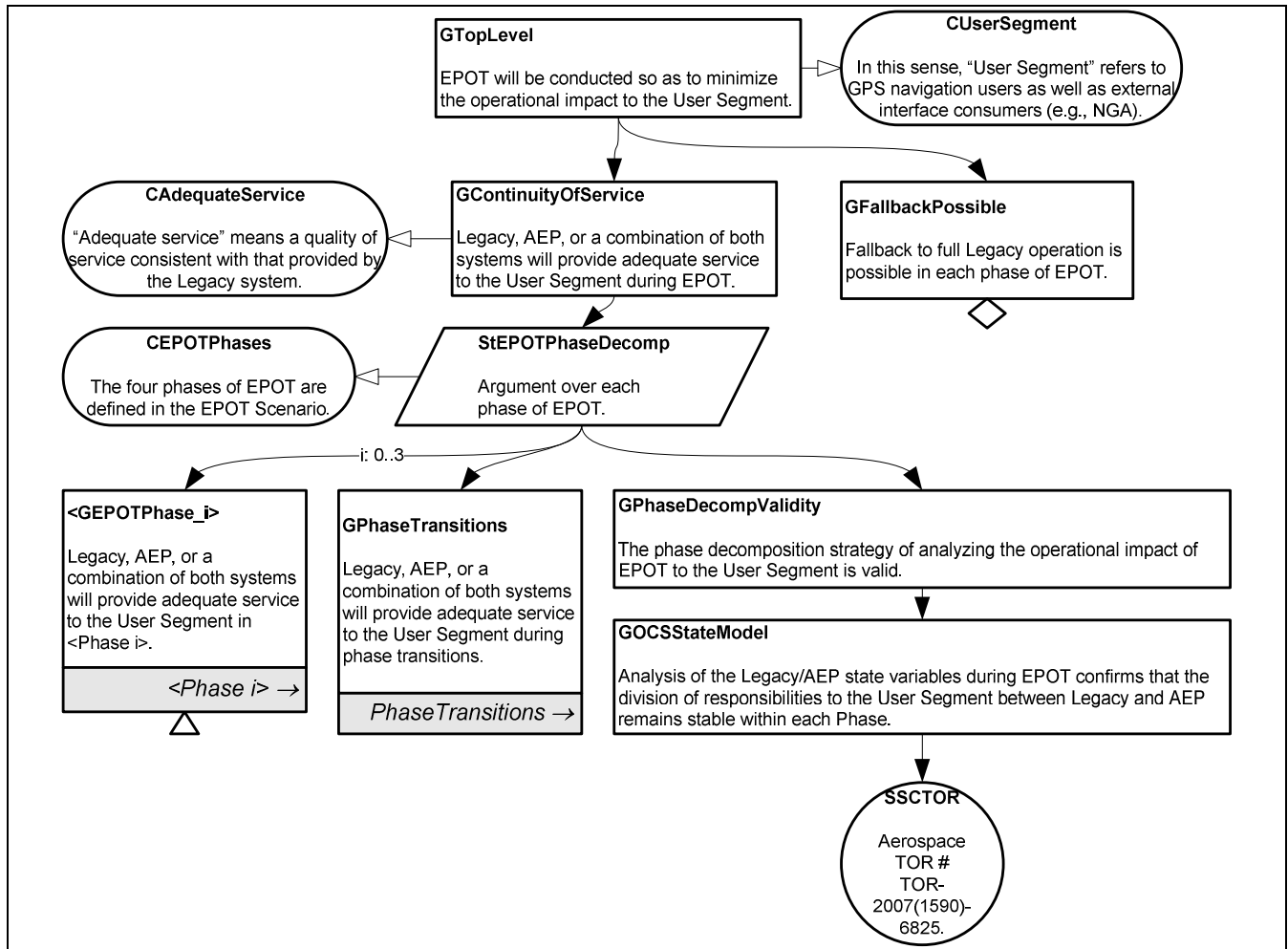


Figure 4. Top Level Argument

5.3. Argument Findings

We identified several issues using the assurance case; all of these issues were resolved after further interaction with our experts.

- Phases 0 and 1: We were unable at first to show that AEP would not interfere with Legacy operations. A domain expert helped us address this goal by describing the interfaces and the communication mechanisms between Legacy and AEP.
- Phase 2: The argument that Legacy will not hinder AEP at first appeared to be missing, but our experts explained that the argument was based on the system's physical connection structure.
- Phase 2: We were concerned about how and when AEP took control of some of the external interfaces. The concern was resolved by further explanation from our experts, and by the outcome of transition rehearsals designed to catch any such omissions.

- Phase 3: We were concerned that the mix of NGA and monitoring station data might lead to a higher divergence in the Kalman filter data than was permissible. Our experts explained that, while the sources used by Legacy and AEP might be different, they were tracking the same value (i.e., the GPS signal); the precision might differ, but the values were not expected to diverge beyond a certain point. This theory was tested and validated during transition rehearsals, and was documented as an argument assumption.

GSN's explicit provision for documenting assumptions was considered to be very useful by our colleagues. They observed that undocumented assumptions about interfaces frequently cause problems in systems.

5.4. Assurance Case Summary

A summary of the elements of the assurance case is shown in Table 2 to indicate the argument's size. We also

include statistics for the major revisions of the argument to show how our interaction with colleagues and experts improved the argument. *Initial* represents the initial draft of the assurance case. *V2* represents the revision after we had incorporated comments; it is slightly smaller because of some restructuring for clarity, but it contained more detailed arguments. *Final* represents the final state of the argument, although we changed the conclusions and recommendations but did not create a new version of the assurance. We include it here to emphasize that there were no significant known risks when the transition occurred.

Table 2. Assurance Case Summary

	Initial	V2	Final
Goals	119	113	113
Unsatisfied goals	14	7	0
Assumptions	1	6	6
Strategies	1	1	1
Context elements	18	21	21
Solutions	40	39	39

6. Conclusions

The study identified no major risks to the AEP transition, and the transition was completed successfully. Although it is possible that the study missed major risks which simply did not materialize, the transition's success provides validation of the study's result.

We were able to use the safety case to identify risks much more effectively than we were able to use the procedural documentation to do the same. Because we were assessing risks derived from the computing system's operation, rather than risks that the procedures could not be carried out, the procedures were only an indirect indicator of the subject of the study. The system states used in the assurance case provided a direct subject. Also, the assurance case enabled us to create and present our argument in a structured fashion; the act of creating the argument forced us to be more structured in our thinking.

The main drawback of using a graphical notation to represent the assurance case is that it encouraged us to spend time rearranging the depiction of the argument structure for clarity and elegance. The branching of the diagrams makes them somewhat hard to read and difficult to present so that reviewers can follow them easily. Presentation ability is key because the size of the argument, the amount of domain knowledge needed to follow it, and the details that were not easily captured in the available structures of the notation. A modified process combining graphical and textual elements might improve our results.

We also used the assurance case to communicate with our experts, explaining the problems we had found. We

then used it to produce a briefing that led, in part, to the decision to proceed with the transition. We feel that this validates our hypothesis that an assurance case is an appropriate tool to use in assuring a system transition.

We have shown how assurance cases can be used to support the upgrade of an influential, long-running system. They could also be used to support other forms of maintenance activity; the super-system model where, for instance, phases of maintenance are used to structure the argument might be used for a database update.

Finally, while assurance cases are generally created by a system's developers, in this instance we created it to help us decide whether the system transition plan would be approved. This shows the potential for assurance cases created by *regulators*, even if the case is not presented initially as part of an acceptance package.

Acknowledgments

This work was sponsored by the GPS Wing of the United States Air Force Space and Missile Systems Center under Contract FA8802-04-C-0001. We appreciate the interest and encouragement of Zane Faught and Robert Jackson of the The Aerospace Corporation's Navigation Division and Tri Caodo of the GPS Systems Engineering department; the extensive assistance provided by our AEP and OCS domain experts, Paul DeNaray and Preston Prouty; and valuable input from Eltefaat Shokri, Gail Haddock, Steven Meyers, Peter Eggan, Clyde Moseberry, and Robert Pettit.

References

1. Branum, Don, "50th SW completes transition to new GPS control system," Air Force Space Cmd. News Release, Sept. 19, 2007, available at <http://www.afspc.af.mil/news/story.asp?storyID=123068750>
2. Weaver, R. A., and T. P. Kelly. "The Goal Structuring Notation - A Safety Argument Notation." Proc. Of Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004.
3. SMC Public Affairs Office. "GPS Fact Sheet." U.S. Air Force Space and Missile Center, August, 2007, available online at <http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5311>
4. United States Air Force, "Global Positioning System (GPS) Operational Control Segment (OCS) Enhanced Phased Operations Transition (EPOT) Operations Plan Global Positioning System Operational Control System," V. 5.0, 1 May 2005.
5. United States Air Force, "Global Positioning System (GPS) Operational Control Segment (OCS) Architecture Evolution Plan (AEP) Operational Safety, Suitability, and Effectiveness (OSS&E) Assurance Plan," V. 5.2.1, 7 December 2006.