FAA Requirements Engineering Management Handbook

4. Identify the Environmental Assumptions

SAnToS Laboratory
Kansas State University

Steps in the REMH

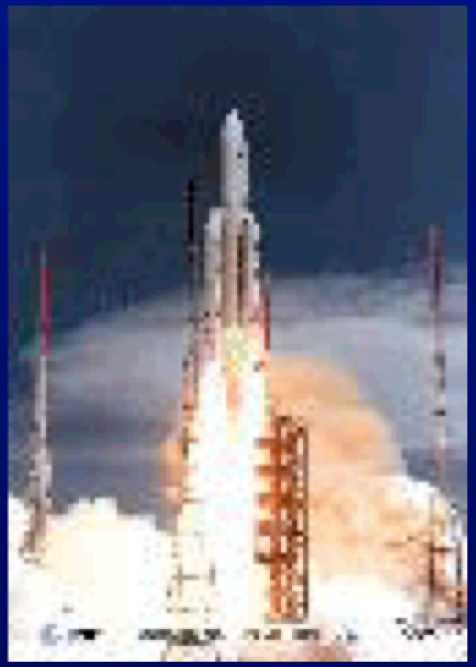
1. Develop the System Overview
2. Identify the System Boundary
3. Develop the Operational Concepts
4. **Identify the Environmental Assumptions**
5. Develop the Functional Architecture
6. Revise the Architecture to Meet Implementation Constraints
7. Identify System Modes
8. Develop the Detailed Behavior and Performance Requirements
9. Define the Software Requirements
10. Allocate System Requirements to Subsystems
11. Provide Rationale

Environmental Assumptions: Goals

What are we trying to achieve with this step in the requirements engineering process?

- Identify mathematical relationships between controlled and monitored variables
  - Simple: types, ranges, units of variables
  - Complex: mapping that fully describes system behavior
- Prevent one of the most common types of error
- Enable safe reuse of components

Ariane 5



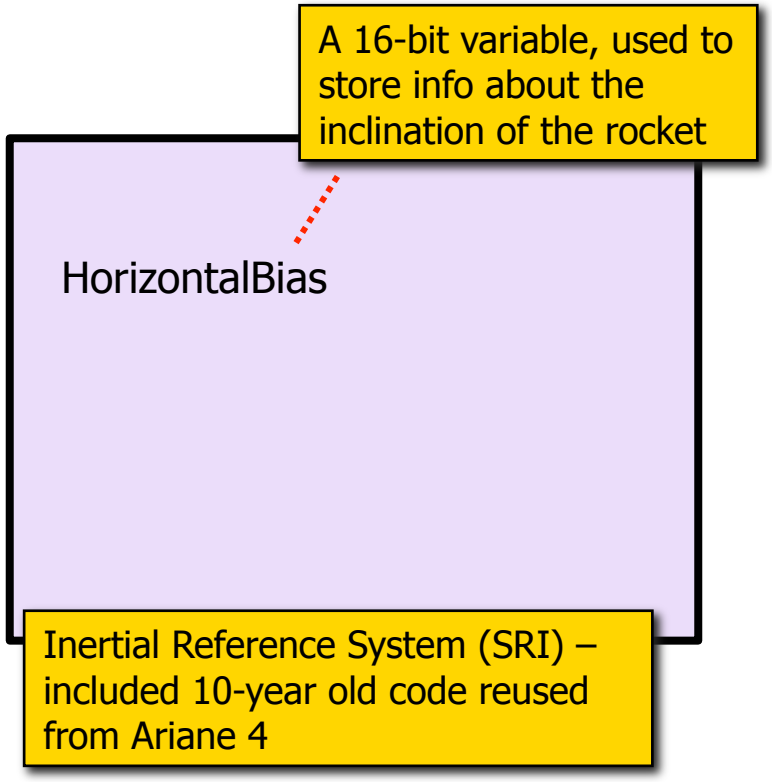
- A European rocket designed to launch commercial payloads (e.g.communications satellites, etc.) into Earth orbit
- Successor to the successful Ariane 4 launchers
- Ariane 5 can carry a heavier payload than Ariane 4

Excerpt above from Ian Sommerville – "Software Engineering Case Studies"

Ariane 5

On June 4, 1996, the maiden flight of the European Ariane 5 launcher crashed about 40 seconds after takeoff. Media reports indicated that the amount lost was half a billion dollars -- uninsured.

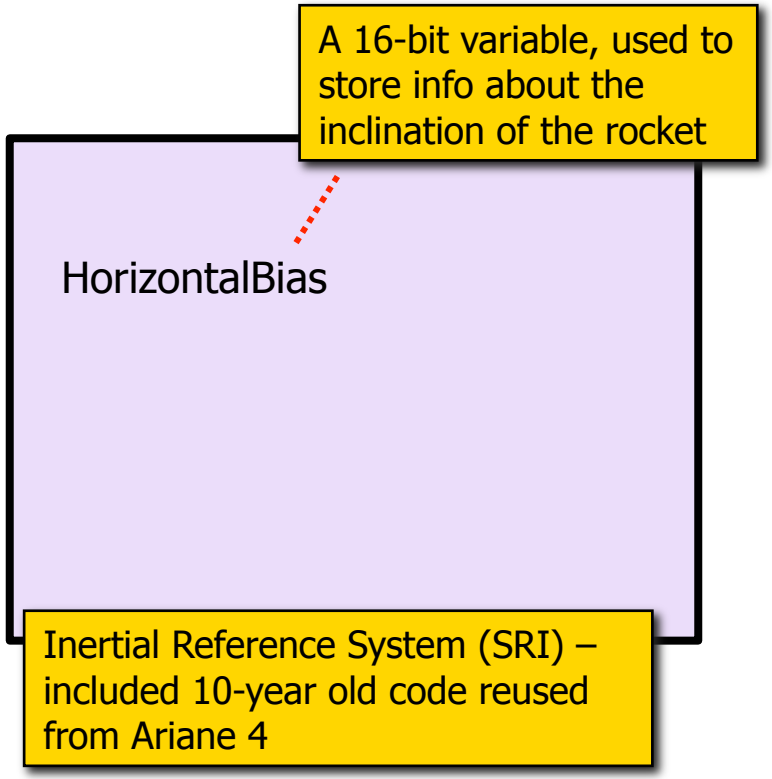
- Issues involved reuse of system module called Inertial Reference System (SRI)
- Before lift-off certain computations are performed to align the SRI.
- Normally they should be stopped at -9 seconds, but in the unlikely event of a hold in the countdown resetting the SRI could, at least in earlier versions of Ariane, take several hours; so the computation continues for 50 seconds after the start of flight mode -- well into the flight period.
- After takeoff, of course, this computation is useless;



Ariane 5

The SRI failed due to an uncaught exception

- A monitored variable (64-bit) was read and stored in the HorizontalBias variable (16-bit)
- In the Ariane 4, a detailed analysis revealed that the 64-bit value could always be converted to 16-bit, and so there was no local exception handler declared (to reduce computation load)
  - *This environmental assumption was not clearly documented*
- But Ariane 5, was a bigger rocket had a different trajectory behavior.



Environmental Assumptions: Artifacts

What artifacts should we produce as a result of this step?

- List of environmental assumptions and supporting rationale

Discussion

- Should we aim for more environmental assumptions or fewer?
- What types of env. assumptions might we encounter in…
  - a flight control system?
  - a blood pressure measurement system?
- In general, what are examples of different categories of env. assumptions?
- How do env. assumptions impact system life cycle?
- Consider Arianne 5 failure…

4 Identify the Environmental Assumptions

4 Identify the Environmental Assumptions: Every system makes specific assumptions about the environment in which it will operate. Some of these assumptions are nothing more than the types, ranges, and units of the inputs it will accept and the outputs it will produce. Often, correct behavior of the system is dependent on more complex assumptions about its environment. *These are actually requirements levied by the system on its environment.* Identification of a system's environmental assumptions is essential for maintenance and to enable reuse. Failure to identify the environmental assumptions and the subsequent misuse of the system is a common cause of system failure.

4.1 Define the type, range, precision, and units required for all monitored and controlled variables as part of the system's environmental assumptions.

4.2 Provide rationale that documents why the environmental assumptions are included.

4.3 Organize environmental assumptions together with the external entity they constrain so it is easy to identify all the obligations placed on each external entity.

4.4 If an environmental assumption defines a relationship among several external entities, **define an external entity responsible for ensuring the assumption is met** and associate the assumption with that entity.

4.5 Define a status attribute for each monitored variable. Each value of the status variable should correspond to a different system behavior. The initial status of the monitored variable should ensure that the monitored variable is not used until it is sensed at least once.

Assumptions / Contracts

- Assumptions form the basis of a conceptual contract
- In some sense…
  - Environmental assumptions are analogous to preconditions
  - Requirements are analogous to postconditions

4.1 Define the Type, Range, Precision, and Units

- No system can accept an infinite range of inputs
- At some point earlier in requirement engineering, type, range, precision, units need to be specified for monitored/controlled variables.

Example

Table 8. Environmental Assumptions for the Current Temperature Monitored Variable

Name	Type	Range	Units	Physical Interpretation
Current Temperature	Real	[68.0..110.0]	°F	Current air temperature inside Isolette

Note: Units could easily be Celsius instead (conversion is trivial) – but knowing which is critical

4.2 Provide Rationale for Assumptions

- Rationale provides a basis for discussing whether or not an assumption can be changed.
- It also assists in future maintenance changes / additions.

Example

- The Current Temperature will be provided to the Thermostat in degrees Fahrenheit.

  Rationale: Consistency with environmental-assumptions operator interface (EA-OI)-1 (All temperatures will be displayed in degrees Fahrenheit.).

- The Current Temperature will be sensed to an accuracy of ±0.1°F.

  Rationale: A precision and accuracy of 0.1°F is necessary to ensure the Thermostat can turn the Heat Source on and off quickly enough to maintain the Desired Temperature Range.

- The Current Temperature will cover the range of at least 68.0° to 103.0°F.

  Rationale: This is the specified range of operation of the Isolette. The lower end of this range is useful for monitoring an Isolette that is warming to the Desired Temperature Range. The upper end is set 1° greater than the Upper Desired Temperature to ensure that the Current Temperature will be sensed across the entire Desired Temperature Range.[7]

4.3 Organize Assumptions Constraining a Single Entity

- Organize environmental assumptions by putting them with a more detailed description of the external entity they constrain
  - This makes reviewing constraints easier

Example

A.3.1 ISOLETTE.

An Isolette is an incubator for an Infant that provides controlled temperature, humidity, and oxygen (if necessary). It encompasses the Thermostat, the Temperature Sensor, the Operator Interface, and the Heat Source. The following environmental assumptions are made by the Thermostat about the Isolette.

- EA-IS-1: When the Heat Source is turned on and the Isolette is properly shut, the Current Temperature will increase at a rate of no more than 1°F per minute.

  Rationale: If the Current Temperature can increase at a rate of more than 1°F per minute, the Thermostat may not be able to turn the Heat Source off quickly enough to maintain the Desired Temperature Range unless the allowed latency specified for the Heat Control is reduced.

- EA-IS-2: When the Heat Source is turned off and the Isolette is properly shut, the Current Temperature will decrease at a rate of no more than 1°F per minute.

  Rationale: If the Current Temperature can decrease at a rate of more than 1°F per minute, the Thermostat may not be able to turn the Heat Source on quickly enough to maintain the Desired Temperature Range unless the allowed latency specified for the Heat Control is reduced.

4.4 Organize Assumptions Constraining Several Entities

Some environmental assumptions define more complex relationships between several environmental variables. For example, below are possible constraints on operator inputs..

- The Lower Desired Temperature will always be ≥97°F.

  Rationale: Exposing the Infant to temperatures lower than 97°F may result in excessive heat loss and drop in heart rate secondary to metabolic acidosis.

- The Lower Desired Temperature will always be less than or equal to the Upper Desired Temperature minus 1°F.

  Rationale: If the Lower Desired Temperature is greater than or equal to the Upper Desired Temperature, it is unclear if the Heat Source should be on or off. This may result in excessive cycling of the Heat Source.

- The Upper Desired Temperature will always be ≤100°F.

  Rationale: Exposing the Infant to temperatures greater than 100°F may result in an incorrect diagnosis of fever, resulting in aggressive evaluation (blood culture and lumbar puncture) and treatment for infection.

4.4 Organize Assumptions Constraining Several Entities

Other environmental assumptions related monitored variables to controlled variables…

With which entity should these assumptions be associated?

- When the Heat Source is turned on and the Isolette is properly shut, the Current Temperature will increase at a rate of no more than 1°F per minute.
- When the Heat Source is turned off and the Isolette is properly shut, the Current Temperature will decrease at a rate of no more than 1°F per minute.

4.4 Organize Assumptions Constraining Several Entities

- Assumptions that span multiple entities should be organized under a (potentially new) external entity
- Generally, assumptions should be grouped with the entity responsible for their being met

However, these assumptions raise a problem of which external entity they should be associated with. They are not really assumptions about the Temperature Sensor, nor are they assumptions about the Heat Source. Rather, they span both of those entities. A useful heuristic is that they should be grouped with the entity that is responsible for ensuring that they are met. This would be the Isolette itself, which includes the Temperature Sensor, the Heat Source, and the Thermostat. For this reason, the requirements specification should include an external entity for the Isolette containing these environmental assumptions. An example of this can be found in appendix A.3.1.

4.5 Define a Status Attribute for Each Monitored Variable

- Not all monitored variables may be equally trustworthy
- Variables might be:
  - Out of date / stale (e.g. a sensor's reading is too old)
  - Inapplicable (e.g. some sensor values should not be relied on while the system is booting)
- Correct these problems by associating a status with each variable.
  - Each status should correspond to a different system behavior that occurs when acting on the variable (e.g., valid, stale, and unknown)

Summary

Main points…

- Environmental assumptions should identify all environmental behaviors the system depends on to operate correctly
  - Enables components to be developed independently (compositional construction)
- Associate assumptions with the entity responsible for their being met
  - Enables one to more easily identify what assumptions might be violated in the system is used in a different environment
- The fewer assumptions about the environment, the better.
  - A robust system will have fewer dependences on the environment that a fragile one will
  - But almost every system has some sort of assumptions

Acknowledgements

- The material in this lecture is based almost entirely on
  - *FAA* DOT/FAA/AR-08/32*, Requirements Engineering Management Handbook.* David L. Lempia & Steven P. Miller.
- Material on Ariane 5 adapted from the following sources…
  - Nice set of notes giving relationship to software contracts
    - http://archive.eiffel.com/doc/manuals/technology/contract/ariane/
  - Ariane 5 video
    - http://www.youtube.com/watch?v=kYUrqdUyEpI
  - Ian Sommerville – "Software Engineering Case Studies"