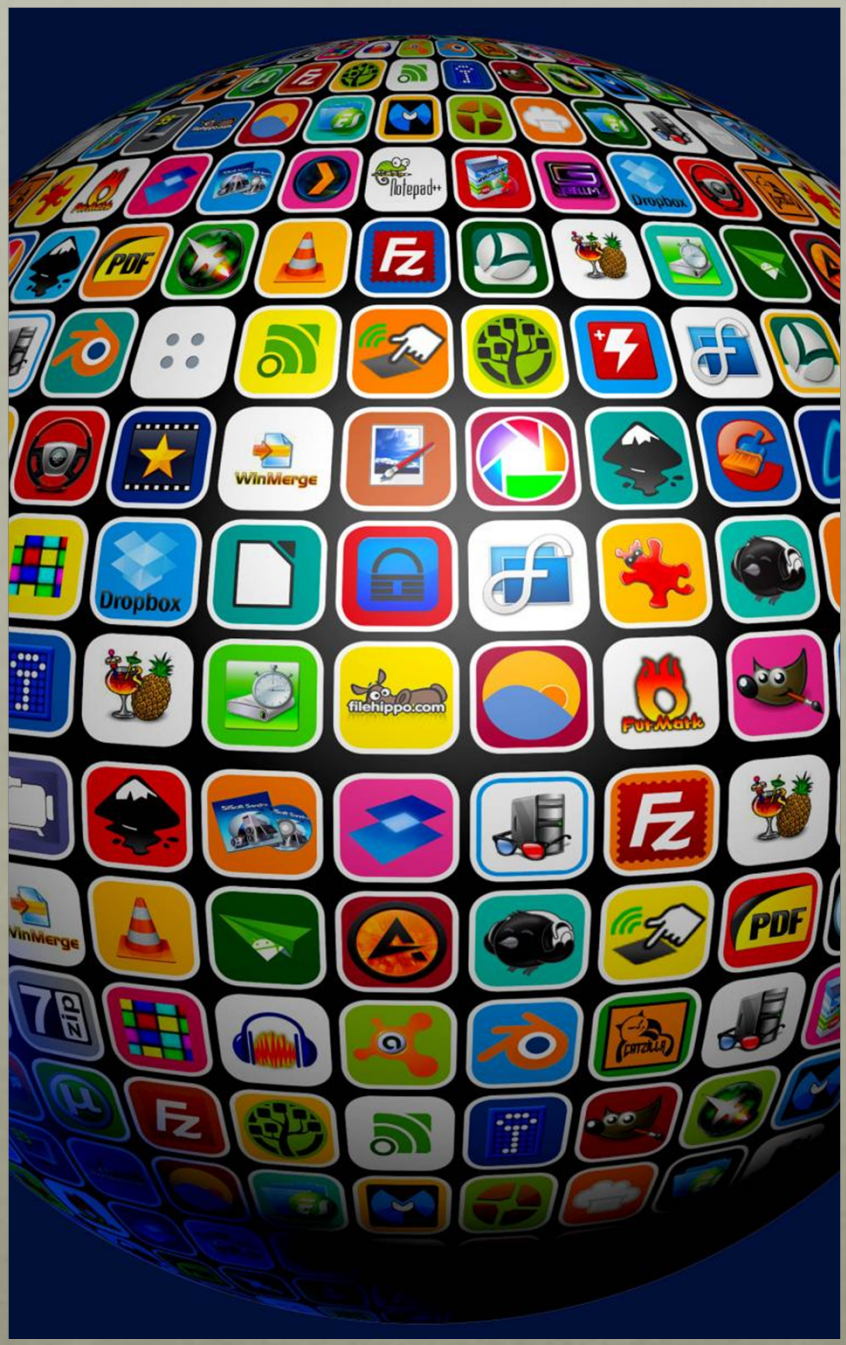
SOFTWARE HAZARD & REQUIREMENTS ANALYSIS (CON'T)

Chapter 15

By: Venessa Woodson

TABLE OF CONTENTS



15.4.5 OUTPUT SPECIFICATION COMPLETENESS

- Complete specification of the behavior requires its value & time.
- Outputs should be reasonable.
- Special Requirements for the specification of outputs:

  - Environmental Capacity

  - Data Age

  - Latency

ENVIRONMENTAL CAPACITY CONSIDERATIONS

- Output Capacity
- Output Overload
- Output load limitations may be required
- Differences in input and output capacity
- When input and output capacities differ, there is a need for multiple periods for which discrete load assumptions are specified.

DATA AGE

- Few, if any, input values are valid forever.
- Control decisions must be based on data from current state.
- Data Obsolescence considerations
- Data Age applying to human-computer interface action sequence

LATENCY

- The duration of this latency interval
- The influence of latency requirements
- Latency factor
- Its affect on human-computer interface

15.4.6 Output to Trigger Event Relationships

- Basic feedback loops
- The importance of feedback
- The design of process control systems
- Every output to which a detectable response is expected induces at least 2 requirements.
- Stability requirements

15.4.7 Specification of Transitions Between States

- These transitions are defined as the sequence of trigger events along the path.
- The requirements for these transitions include:
  - Reachability
  - Recurrent Behavior
  - Reversibility
  - Preemption
  - Path Robustness

REACHABILITY

- All specified states much be reachable from initial state
- What it means to be reachable
- Reachability Analysis

RECURRENT BEHAVIOR

- Most process control software is cyclic
- Desired recurrent behavior must be a part of at least one cycle
- Every cycle that has a start, must include a stop
- Inhibiting state

REVERSIBILITY

- What is reversibility
- Output commands should usually be reversible

PREEMPTION

- Preemption requirements
- With preemption, activating a multistep sequence requiring the use of a resource involved in another transaction can lead to three cases.

PATH ROBUSTNESS

- A state can fulfill its reachability requirements and still deal with the robustness of the path which will have an affect on a particular state
- The more failure modes the requirements state machine specification has, the less robust
- Solution

15.5 CONSTRAINT ANALYSIS

- Transitions must satisfy software safety requirements and constraints
- What is constraint analysis
- Examples of software related hazards
- Some hazardous states are unavoidable but it is possible to minimize the risk associated with the hazard
- A completely safe system may not be possible

15.6 CHECKING THE SPECIFICATION AGAINST THE CRITERIA

- Criteria for completeness of states, inputs and outputs & their relationship are checked for any type of specification
- Criteria is checkable depending on:

  - Formality of specification

  - Size of specification

  - Availability of software tools

- Some criteria is enforced by using a specification language

LESSON

No system is perfect so there are many requirements, specifications, constraints and testing that should be taken into consideration to minimize the risks and hazards in software.