Safety-Critical Systems

Prof. Dr. Jan Peleska
Universität Bremen — TZI
Dr. Ing. Cornelia Zahlten
Verified Systems International GmbH

Overview

1. The Notion of Dependability
2. Safety-Related Standards and V-Models
3. Modelling Safety-Critical Systems
4. Hazard Analysis and Risk Assessment
5. Design Criteria for Safety-Critical Systems
6. Validation, Verification and Test of Safety-Critical Systems

Dependability – General Definition

Our objective: Development and verification of safety-critical reactive systems that continuously interact with their environment and control (parts of) the environment in order to perform the user-required services and enforce the required safety properties.

- **Dependability:** The trustworthiness of a computer system such that reliance can be justifiably placed on the service it delivers.
- **Service:** System behaviour as it is perceived by its users.
- **User:** Another system (human or physical) interacting with the target system.

Dependability Attributes

- **Availability:** readiness for usage
- **Reliability:** continuity of service
- **Safety:** avoidance of catastrophic consequences on the environment
- **Security:** prevention of unauthorised access and/or handling of information

  Security attributes:

  - confidentiality
  - integrity
  - availability

Dependability – Faults – Errors – Failures

- **Failure:** delivered service no longer complies with specification
- **Error:** part of the system state which is likely to lead to subsequent failure
- **Fault:** cause of an error

Dependability – Fault-Tolerance versus Fault-Avoidance

Classification of methods achieving dependability:

- **Fault-Tolerance:** provide a service complying with the specification in spite of faults
- **Fault-Avoidance (Fault-Prevention):** a-priori prevention of fault occurrence or introduction
- **Fault-Removal:** reduce the presence (number, seriousness) of faults
- **Fault-Forecasting:** estimate the present number, the future incidence, and the consequence of faults

Our Favourite Approach: Fault-Tolerance on HW level — Fault-Avoidance on specification and SW level !

Dependability — Safety versus Liveness Properties

In computer science, specifications are classified as containing

- **Safety Properties S:** Any sequence of events or transitions etc. violating S contains a prefix all of whose infinite extensions violate S. (S always holds)
- **Liveness Properties L:** Any arbitrary finite sequence of events can be extended to an infinite sequence satisfying L. (L finally holds)

For safety-critical real-time systems, all dependability requirements should be specified as safety properties: Liveness properties can only guarantee that a service will FINALLY be delivered, which is not sufficient in the context of hard real-time systems.

Dependability — Classification of System Behaviour

System state space is partitioned into three areas. System execution is regarded as sequence of state transitions, possibly accompanied by visible actions (input/output).