Tiako, P. F. (ed.):
Designing Software-Intensive Systems: Methods and Principles,
Idea Group Inc., Hershey, USA 2008, pp. 161-221, ISBN 978-159904699-0

Chapter VII
Choosing Basic Architectural Alternatives

Gerhard Chroust
J. Kepler University Linz, Austria
Erwin Schoitsch
Austrian Research Centers (ARC), Austria

Dependability Properties

With the growth of the field of dependable computers, especially in safety critical controls, certain key attributes gain special importance. To some extent they are already covered by the ISO9126 (ISO/IEC, 2001a) but need special attention which is for example, the intention of IEC 61508-98/00 (IEC, 1998). There is no full consent yet. An extended set of dependability attributes follows (Laprie et al., 1992; Redmill, 1988; Schoitsch, 2003b; Sonneck & Schoitsch, 2003). The compound term "dependability" is the central notion. It consists of availability, reliability, safety, security (confidentiality, integrity, authenticity), maintainability, and survivability:

• **Dependability:** The collective term for availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance (IEC, 1990, IEC TC 56). The term was extended (Laprie et al., 1992; van der Meulen, 2000, 1995) to cover all principal characteristics in connection with safety-related systems: "Trustworthiness of a computer system such that reliance can be justifiably placed on the service it delivers." Thus, dependability is an umbrella term for a set of subproperties: availability, maintainability, reliability, safety, security (including confidentiality, integrity, authenticity), and survivability (robustness).

• **Availability (Readiness for use):** The ability of a functional unit to be in a state to perform a required function under given conditions

at a given time instance time or over a given time interval, assuming that the external resources are provided (ISO/IEC, 1996).

• **Maintainability (Easiness of maintenance):** From a hardware/software systems perspective, this includes more than just the preservation of the status quo of a system (as in ISO/IEC, 1996). It includes enhancements

functions to fulfil new requirements, for example, upgrades and adaptations (Arthur, 1988; Sommerville, 2007). In the system context (and context of the dependability definitions of Laprie et al., 1992) it can be defined as *"The ease with which a (software, hardware) system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment* (IEEE, 1990; for details, see Redmill, 1989; Schoitsch, 1997).

• **Reliability (Continuity of service):** The probability that an item can perform a required function under given conditions for a given time interval (IEC, CENLEC). The ability of a functional unit to perform a required function under given conditions for a given time interval (ISO/IEC, 1996).

• **Safety (freedom from unacceptable risk):** Freedom from (likelihood of) those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment (Department of Defense, 1993).

• **Security:** Dependability with respect to unauthorized access or information handling (deliberate (malicious) interaction!). Normally, subproperties to be included are availability, confidentiality, integrity and authenticity of information.

• **Survivability:** (capability to withstand a hostile environment) The capability of a system to avoid or withstand a hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission (van der Meulen, 2000; Department of Defense, 1992). This includes any kind of impairment especially from the environment, including security attacks and so forth.

Further essential properties are:

• **Fault tolerance:** The ability of a functional unit to continue to perform a required function

in the presence of faults or errors (IEC, 1998).

• **Risk:** (combination of probability of concurrency and severity of harm): The combination of frequency, or probability, and the consequence of a specific (or combination of) hazardous events (IEC, 1998).

• **Hazard:** a potential source of harm (IEC, 1998).

• **Predictability**: The ability to provide a correct forecast of the behaviour of a system or component in space and time under given conditions for all foreseeable operational states (in dependable embedded real-time sytems, it normally means that the behaviour in space and time can be statically defined beforehand by proper configuration of the system).

• **Responsiveness:** The ability of a functional unit to react to a given event according to requirements, and under stated conditions (generalized from Redmill, 1989).

• **Timeliness ("in time"):** Ability of a system or component to perform its required function before its deadline.

• **Robustness:** Capability of a system to withstand hostile environment, intended or unintended malicious (mis-)use. Robustness can be seen as a combination of reliability, survivability, safety and security).