From Dependability to Resilience

Jean-Claude Laprie
LAAS-CNRS — Université de Toulouse — 7, Avenue Colonel Roche 31077 Toulouse, France
<laprie@laas.fr>

Definition of resilience

Resilience (from the Latin etymology resilire, to rebound) is literally the act or action of springing back. As a property, two strands can historically be identified: a) in social psychology [Claudel 1936], where it is about elasticity, spirit, resource and good mood, and b) and in material science, where it is about robustness and elasticity.

The notion of resilience has then been elaborated:

- in child psychology and psychiatry [Engle et al. 1996], referring to living and developing successfully when facing adversity;
- in ecology [Holling 1973], referring to moving from a stability domain to another one under the influence of disturbances;
- in business [Hamel & Välikangas 2003], referring to the capacity to reinvent a business model before circumstances force to;
- in industrial safety [Hollnagel et al. 2006], referring to anticipating risk changes before damage occurrence.

A common point to the above senses of the notion of resilience is the ability to successfully accommodate unforeseen environmental perturbations or disturbances.

A careful examination of [Holling 1973] leads to draw interesting parallels between ecological systems and computing systems, due to:

a) the emphasis on the notion of persistence of a property: resilience is said to "determine the persistence of relationships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist";
b) the dissociation between resilience and stability: it is noted that "a system can be very resilient and still fluctuate greatly, i.e., have low stability" and that "low stability seems to introduce high resilience";
c) the mention that diversity is of significant influence on both stability (decreasing it) and resilience (increasing it).

The adjective *resilient* has been in use for decades in the field of dependable computing systems, e.g. [Alsberg & Day 1976], and is more and more in use, however essentially as a synonym of *fault-tolerant*, thus generally ignoring the unexpected aspect of the phenomena the systems may have to face. A noteworthy exception is the preface of [Anderson 1985], which says "The two key attributes here are dependability and robustness. […] A computing system can be said to be *robust* if it retains its ability to deliver service in conditions which are beyond its normal domain of operation".

Fault-tolerant computing systems are known for exhibiting some robustness with respect to fault and error handling, in the above sense, i.e., for situations exceeding their specification. Examples are the tolerance of a) elusive software faults thanks to loosely-coupled architectures [Gray 1986], or of b) errors that escaped detection and thus did not trigger recovery [Kanoun et al. 1991]. This of course should not lead to forget that, contrariwise, total coverage with respect to the specified faults is hardly achievable.

A total change of scale is needed when moving to the future large, networked, evolving systems constituting complex information infrastructures — perhaps involving everything from super-computers and huge server "farms" to myriads of small mobile computers and tiny embedded devices. Such systems are in fact the dawning of *ubiquitous systems*, and we will use this term as a shorthand for portraying our target systems

With such ubiquitous systems, what is at stake is to maintain dependability, i.e., the ability to deliver service that can justifiably be trusted [Avizienis et al. 2004], in spite of continuous changes.

Our definition of **resilience** is then:

> The persistence of service delivery that can justifiably be trusted, when facing changes.

The definition given above builds on the initial definition of dependability, which emphasizes justifiably trusted service. In a similar spirit, the alternate definition of dependability, which emphasizes the avoidance of unacceptably frequent or severe failures, could be used, leading to an alternate definition of resilience:

> The persistence of the avoidance of failures that are unacceptably frequent or severe, when facing changes.

From what precedes, it appears clearly that a shorthand definition of resilience is:

> The persistence of dependability when facing changes.

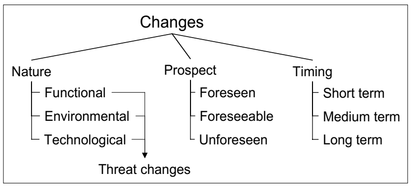
The changes can be classified according to three viewpoints, or dimensions:

- Their nature, which can be functional, environmental, or technological, where the latter can concern either or both hardware and software.
- Their prospect, which can be:
  - foreseen, as in new versioning,
  - foreseeable, as in the advent of new hardware platforms,
  - unforeseen, as drastic changes in service requests or new types of threats.
- Their timing, which can be:
  - short term, e.g., seconds to hours, as in dynamically changing systems (spontaneous, or 'ad-hoc', networks of mobile nodes and sensors, etc.),
  - medium term, e.g., hours to months, as in new versioning or reconfigurations,
  - long term, e.g., months to years, as in reorganizations resulting from merging of systems in company acquisitions, or from coupling of systems in military coalitions.

It has to be emphasized, in the context of dependability, that the changes can concern, or induce changes in the threats the system is facing. The threat changes can have their source in the changes to the system or its environment, taken either a) in isolation, such as, for technological changes, the ever increasing proportion of transient hardware faults that goes along with the progress of integration, or b) in combination, such as the ever-evolving and growing problem of attacks both by amateur hackers and by professional criminals, that may result from environmental and technological changes. Finally, the changes can themselves turn into threats, as in the case of mismatches between the modifications that implement the changes and the former status of the system.

Figure 1 summarizes schematically the classes of changes.

Figure 1 - Change classification



Technologies for resilience

As ubiquitous systems are under continuous changes or evolutions, a central property they should exhibit, via appropriate technology, is **evolvability**, i.e., the ability to successfully accommodate changes. Within evolvability, an important topic is *adaptivity*, i.e., the capability of evolving while executing.

As our definition of resilience retains the notion of justified confidence, **assessability**, in both senses of verification and evaluation, comes immediately second. Classically, verification and evaluation are performed off-line, pre-deployment. Such an approach falls obviously short in the case of evolving systems, for which assessment has to be performed at run-time, during operation.

Computing systems have already pervaded all activities of our life, and this will still be even more true with ubiquitous systems, hence the importance of **usability**.

Ubiquitous systems being highly complex systems, heterogeneity and diversity are naturally present. **Diversity** can, and should be taken advantage of in order to prevent vulnerabilities to become single points of failure.

Those four technologies for resilience are of course related to the means for dependability, as shown on Figure 2.

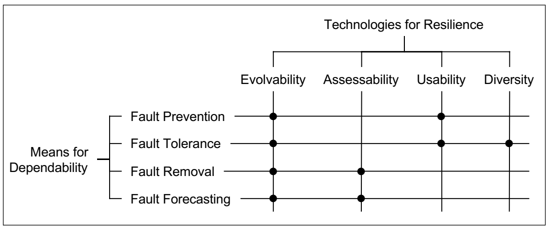


Figure 12- Relationship between the technologies for resilience and the means for dependability

Acknowledgments

The work reported here has been performed in the framework of the European Network of Excellence ReSIST (Resilience for Survivability in Information Society Technologies). The work has benefited from discussions with several ReSIST members. Comments by Karama Kanoun and Brian Randell on former versions of the text are especially acknowledged.

References

[Alsberg & Day 1976] P.A. Alsberg, J.D. Day, "A principle for resilient sharing of distributed resources", *Proc. 2nd Int. Conf. on Software Engineering*, San Francisco, Oct. 1976, pp. 562-570.

[Anderson 1985] T. Anderson (Ed.), *Resilient Computing Systems*, Collins, 1985.

[Avizienis et al. 2004] A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing*, Vol.1, No.1, Jan-March 2004, pp. 11-33.

[Claudel 1936] P. Claudel, "The American elasticity", in *Works in Prose*, La Pleiade, Gallimard, Paris, 1965, pp. 1204-1208; in French.

[Engle et al. 1996] P.L. Engle, S. Csatle, P. Menon, "Child development: vulnerability znd resilience", *Social Science and Medicine*, vol. 43, no. 5, 1996, pp. 621-635.

[Gray 1986] J.N. Gray, "Why do computers stop and what can be done about it?", *Proc. 5th Symp. on Reliability in Distributed Software and Database Systems,* Los Angeles, Jan. 1986, pp. 3-12.

[Hamel & Välikangas 2003] G. Hamel, L. Välikangas, "The quest for resilience", *Harvard Business Review*, Sept. 2003.

[Holling 1973] C.S. Holling, "Resilence and stability of ecological systems", *Annual Review of Ecology and Systematics*, vol. 4, 1973, pp. 1-23.

[Hollnagel et al. 2006] E. Hollnagel, D. Woods, N. Leveson (Eds.), *Resilience Engineering – Concepts and Precepts*, Ashgate, 2006.

[Kanoun et al. 1991] K. Kanoun, J. Arlat, L. Burrill, Y. Crouzet, S. Graf, E. Martins, A. MacInnes, D. Powell, J.L. Richier, J. Voiron, "Validation", ch. 15 of *Delta-4: a generic architecture for dependable distributed computing*, D. Powell (Ed.), Reearch Reports Esprit, Springer-Verlag, 1991, pp. 395-406.