# Resilience Assessment: Accidental and Malicious Threats

Mohamed Kaâniche
CNRS; LAAS; Université de Toulouse – 7, Avenue du colonel Roche, F-31077 Toulouse, France
Université de Toulouse; UPS; INSA; INP; LAAS; F-31077 Toulouse, France
*mohamed.kaaniche@laas.fr*

**A large body of research has been dedicated to the analysis, assessment and protection of cyber-physical systems and critical infrastructures against potential threats that might affect the dependability, the security or the resilience of the services delivered to the users. Traditionally, accidental and malicious threats have been taken into account separately. In this talk we will address the challenges raised by the resilience assessment and analysis of such systems considering accidental and malicious threats in an integrated way and we will present some examples of research studies carried out in this context.**

*Critical infrastructures, resilience, assessment, accidental threats, malicious threats*

## 1. SUMMARY

In the past decade, several concerns have been raised about the vulnerability of critical infrastructures and cyber-physical systems and their efficient protection in the presence of accidental and malicious threats (Rahman et al. 2009).

Historically, most of the efforts were dedicated to the protection of critical infrastructures against accidental faults and natural disasters with a specific focus on safety. The situation changed significantly after the September 11, 2001 tragic events that led to increased international concerns about the security and robustness of critical infrastructures in response to evolving malicious threats

The vulnerability of critical infrastructures has increased as a result of the wider use of open networks and information infrastructures, and the proliferation of vulnerable operating systems and control devices. Recent events targeting critical infrastructures show that the threat is real. A widely reported example is the Stuxnet sophisticated malware discovered in July 2010 that targeted specific industrial computer control equipment and software, used for instance in nuclear power plants in Iran [(Langner 2011).

A large body of research has been dedicated to the analysis, assessment and protection of cyber-physical systems and critical infrastructures against potential threats that might affect the dependability, the security or the resilience of the services delivered to the users. The resilience term is used differently, by different communities. It is defined in (Laprie 2011) as the persistence of service delivery that can justifiably be trusted, when facing changes.

Traditionally, accidental and malicious threats have been taken into account separately. In this talk we will address the challenges raised by the resilience assessment and analysis of such systems considering accidental and malicious threats in an integrated way and we will present some examples of research studies carried out in this context.

In particular this objective has been addressed in the context of the CRUTIAL project (http://crutial.rse-web.it/) considering the example of power grid critical infrastructures and the associated information infrastructures dedicated to their management and control.

CRUTIAL focussed on the failures resulting from interdependencies between these infrastructures. The characterization of such failures and the modelling of their impact on relevant properties of power systems have been investigated by means of models at different abstraction levels: i) from a very abstract view expressing the essence of the typical phenomena due to the presence of interdependencies, ii) to an intermediate detail level representing in a rather abstract way the structure of the infrastructures, in some scenarios of interest, iii) to a quite detailed level where the infrastructures components and their interactions are investigated at a finer grain, considering elementary events

occurring at the components level and analysing their impact at the system level.

Accordingly, the proposed resilience assessment framework (Kaâniche et al. 2009) is based on a hierarchical modelling approach that accommodates the composition of different types of models and formalisms, including generalized stochastic Petri nets, fault trees, Stochastic Well formed Nets, and Stochastic Activity Networks. Additionally, a new formalism called "Dependent Automata" has been developed to provide a rigorous definition of interdependencies related failures. Also, unified models for describing cascading and escalating failures considering accidental and malicious threats in an integrated way have been defined (Laprie et al. 2007)

Besides these models, the CRUTIAL project resilience assessment activities included architecture validation activities as well as testbed based experiments to analyse the impact of different attack scenarios on control applications.

We will outline some of the results obtained in the context of this project and discuss some open research problems.

## 3. REFERENCES


Kaâniche, et al. (2009) CRUTIAL Project Deliverable D16 - Final version of the modelling framework. http://crutial.rse-web.it/Dissemination/DELIVERABLES-OF-THE-PROJECT.asp

Laprie, Jean-Claude, Kanoun, Karama, Mohamed Kaâniche, (2007) Modelling interdependencies between Electricity and Information Infrastructures. The 26th International Conference on Computer Safety, Reliability, and Security (SAFECOMP-2007), Nuremberg, Germany, LNCS 4680, Springer, pp. 54-67.

Laprie, Jean-Claude "From Dependability to Resilience", IEEE International Conference on Dependable Systems and Networks (DSN-2008), Supplemental volume, Anchorage, Alaska, USA, pp. G8-G9, 2008.

Langner, R. "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy*, vol. 9, no. 3, 2011, pp. 49–51.

Rahman, H.A., Beznosov, K., Marti, J.R., "Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports", Int. Journal on Critical Infrastructures, vol.5, n°3, 2009


**BIO**

Mohamed Kaâniche has been at LAAS-CNRS, Toulouse, France, since 1988 where he currently holds a position of "Directeur de Recherche", heading the Dependable Computing and Fault Tolerance Group. From March 1997 to February 1998, he was a Visiting Research Assistant Professor at the University of Illinois at Urbana-Champaign, IL, USA.

His research addresses the dependability and security assessment of hardware and software fault tolerant computer systems and critical infrastructures, using analytical modelling and experimental measurement techniques.

He has been involved in several national and European research projects and acted as a consultant for companies in France and as an expert for the European Commission. He has served on program and organization committees of international dependability related conferences. He was Program Chair of PRDC-2004, EDCC-5, DSN-PDS 2010, LADC-2011 and SAFECOMP- 2013. He is General co-Chair of DSN-2016 that will be held in Toulouse, France in June 2016.