

# **Socio-Technical Complex Systems of Systems: Can We Justifiably Trust Their Resilience?**

**Luca Simoncini**

**University of Pisa, Department of Information Engineering, Via G. Caruso 16,  
56122 Pisa, Italy**

e-mail: <[luca.simoncini@iet.unipi.it](mailto:luca.simoncini@iet.unipi.it)>

# Complex Systems of Systems and Resilience

Fukushima is an example of a composition of “mature technology” socio-technical systems (electric power, nuclear reactors, emergency safety systems, human operated control rooms) designed under very consolidated safety standards and operational protocols, with highly trained personnel, that anyway produced a very severe disaster for people and environment.

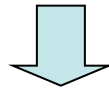
If we extend our attention to present market trends that push forward the deployment and operation of **complex software-based socio-technical systems of systems** that have to be not only dependable but also resilient,

**the following question becomes mandatory**

**Can we justifiably trust the resilience of such systems ?**

## Peculiarities of Socio-Technical Complex Systems of Systems

- These systems have to be dependable in a highly dynamic and changing environment, that is they have to present a high level of resilience;
- These systems are always on line and require pervasive and ubiquitous computing;
- They have to manage sensitive personal, social, corporate, financial and political information;
- These systems include a huge number of humans, as users or operators, who are often untrained and often risk unaware.



These systems have to cope with **new fault types** (escalating and cascading failures in critical utility infrastructures, identity theft, unexpected interactions, common mode failures affecting a very large number of users, etc.), with **changing environments** and possible **uncontrollable human interactions**.

## Open research topics

- Understanding the new risks and threats;
- Understanding the boundary-less nature of systems;
- Dealing with increased scale and complexity and criticality;
- An assessment based on user perception;
- Dealing with changing environments

**but**

it is impossible to anticipate all the possible situations and events that could happen and that could lead to failures with possible catastrophic consequences.

This means that we are going to operate quite critical systems whose design has been made in **ignorance** or **extensive unawareness** of the controlled physical environment, with relevant constraints on their requirements.

## What about physical world and requirements ?

What do we know about physical world  $\implies$  the requirements for a system ?  
This knowledge can be clustered into four groups:

- the **Known Knowns** – what we know that we know
- the **Known Unknowns** – what we know that we do not know
- the **Unknown Knowns** – what we pretend not to know even if we know
- the **Unknown Unknowns** – what we do not even know that we do not know

The KK and KU groups are the easiest since all requirements will be deterministically considered in the design

The specifications for all functions of the system may be derived.

We can also take into consideration (maybe rare) events that we may not be able to deterministically express but that we know that could happen even if we do not know either when they will happen or how they will manifest themselves (some type of security attacks)

**Statistical forecasting and assessment is meaningful (except for ultra-high dependability)**

## What about UK and UU groups?

The UK group is intriguing since it refers to things that we know may (or will) happen but we pretend not to know.

This is quite common in social and political affairs, when “we close our eyes to the evidence” and expect to see what happens.

In our framework, maliciously or accidentally neglected specifications belong to this group, which then lead to incorrect designs, or erroneous operations performed under stress or time pressures.

**The UU group is clearly the most dangerous since there is no way of being able to consider something that we are completely ignorant - or unaware of - in terms of its possibility, manifestation (what, when and how) and consequences**

The type and number (that cannot be known) of possible events belonging to UU group (by experience) grow according to the complexity of the system and its interactions. Their manifestation and consequences cannot be known or forecast. This is a very vague statement that may be mitigated by qualifying these events as “**extremely rare and unlikely**”, however there is a **contradiction** since this qualification applies to events of which we have some knowledge

# Black Swan Events - 1

The theory of Black Swan Events (introduced in 2007 by Nassim N. Taleb) was developed to explain:

- The disproportionate role of high-impact, hard to predict, and rare events that are beyond the realm of normal expectations in history, science, finance and technology
- The non-computability of the probability of the consequential rare events using scientific methods (owing to their very nature of small probabilities);
- The psychological biases that make people individually and collectively blind to uncertainty and unaware of the massive role of the rare event in historical affairs

From Taleb: “What we call here a Black Swan (and capitalize it) is an event with the following three attributes. First, it is an **outlier**, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an **extreme impact**. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it **explainable and predictable**. I stop and summarize the triplet: **rarity, extreme impact, and retrospective (though not prospective) predictability**”

## Black Swan Events - 2

- The event is a surprise (to the observer);
- The event has a major impact;
- After the fact, the event is rationalized by hindsight, as if it *could* have been expected (e.g. as if the relevant data were available but not accounted for)

The main idea for coping with Black Swan Events is **not to attempt to predict them**, but **to build robustness** against negative ones that occur and be able to exploit positive ones by identifying areas of vulnerability in order to **"turn the Black Swans white"**

Black Swan Events are phenomena with specific empirical and statistical properties, which Taleb puts in what he calls "the fourth quadrant".

The problem concerns the decrease in knowledge when it comes to rare events as these are not visible in past samples and therefore require a strong a priori, or what one can call an extrapolating theory. Accordingly events depend more and more on theories when their probability is small. In the fourth quadrant, knowledge is either uncertain or non existent and consequences are large, requiring more robustness.



## Black Swan Events - 3

Before Taleb, those who dealt with the notion of the improbable, such as Hume, Mill, and Popper focused on the problem of induction in logic, specifically, that of **drawing general conclusions from specific observations**. Taleb's Black Swan Event has a central and unique attribute, *high impact*. His claim is that ***almost all consequential events in history come from the unexpected*** - yet humans later convince themselves that these events are explainable in hindsight (bias)

One problem is the belief that the unstructured randomness found in life resembles the structured randomness found in games. This stems from the assumption that the unexpected may be predicted by extrapolating from variations in statistics based on past observations, especially when these statistics are presumed to represent samples from a bell-shaped curve

More generally, decision theory, which is based on a fixed universe or a model of possible outcomes, ignores and minimizes the effects of events that are "outside the model". **A fixed model considers the "known unknowns", but ignores the "unknown unknowns"**

## Consequences

When complex decisions need to be taken in the fourth quadrant, **neither statistics nor models can be used**, and worse, if they are used following a classical approach, they will deceive us.

Restricting the horizon to the design of socio-technical complex systems of systems in changing environments the application of the Black Swan Events theory implies the **impossibility of providing a meaningful and convincing forecasting and assessment of their resilience based on classical statistical methods.**

Thus the main question must be changed from “**How can resilience be quantitatively assessed?**” to “**How can a socio-technical complex system of systems in changing environments be designed in order to increase the confidence that it may survive and provide an acceptable (maybe reduced) service not only in the presence of changes but also of Black Swan Events (unknown unknowns)?**”

## Primary concerns

- Due to unknown unknowns, **failures will happen** and we **cannot forecast** their evolution (whether or not there will be catastrophes) or probability distribution
- It is **impossible** to have complete and accurate specifications of such systems, therefore **capturing requirements is an evolving process** not only during the design but also during the operational life
- A socio-technical complex system of systems is **not built from scratch**, but is the **composition** of pre-existing systems. It is based on their individual infrastructures, each designed with different paradigms, with different forms of governance, and made to cooperate through **interfaces** (from input signals to communicating humans)
- Humans (designers, maintenance personnel, operators and end-users) are significant components of these systems. It is clear that it is **impossible to force requirements on humans**, especially if the system is used and operated by a large number of persons who are **untrained and/or risk unaware**
- The stored and managed information are **sensitive** from many points of view

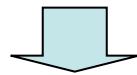
## What can be done ?

We need to approach the design, deployment and operation with tools and methods that stem from engineering (computer, software, ergonomics etc.), decision-making and management, social sciences, culture and education in a holistic way

**Product-centred design**



**Multi-view Resilience-centred design to decision-making (in ignorance)**

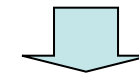


**Cost-performance market limitations**

**Hierarchical top-down relations**



**It works with complete and accurate specifications**



**change the focus and relevance of the design, production and operation activities**

## What can be done ? - Architectural capabilities

The most important requirements in making decisions in ignorance are:

- Detect the incorrectness of the decision as soon as possible. It requires the enhancement of the **controllability** of the design process and of the designed system
- Correct the decisions. It requires the **flexibility** and **adaptability** of the design process and of the designed system

**Controllability**, **flexibility** and **adaptability** are introduced as three capabilities that need to be exploited in socio-technical complex systems of systems

They are architectural capabilities and require a **special focus in the design and operation of the interfaces**. In fact a system may fail because of the interactions between components that operate as designed

**All interfaces are the weak point in all systems of systems**

(signals and commands, human communication during design, operation, maintenance, warning and emergency management,....)

**Less fully automated procedures**  **Main human responsibility + automated early warning detection**

## What can be done ? - Technical level

- From B. Randell (2005): “However, for structuring to have some direct relevance to questions of operational dependability, and in particular fault tolerance, it must be what might be described as strong – **strong** structuring actually controls interactions within and between systems, and limits error propagation in both time and space, i.e. constitutes *real* not just perceived or imagined boundaries.”
- From C. Jones (2007): a systematic way to derive specifications and leads to recording assumptions concerning the controlled world to specify and design complex systems of systems
- From M. Thomas (2003): poses the question, with respect to software dependability, as to what is **known** and what is **not done** in industry due to educational and cultural limitations and difficulties deriving from cost-performance pressures.
- Recent EU Projects and NoE:
  - Crutial (2006-2008) - networked ICT systems for the management of the electric power grid
  - ReSIST NoE (2006-2009) - Resilience for Survivability in IST
  - Hidenets (2006-2009) - end-to-end resilience solutions for distributed applications
  - CONNECT (2009-1012) - [How to make networked systems eternally connected](#)

## What can be done ? - Enterprise and Managerial protocols

- Changing the focus from product-centred to resilience-centred design and operations requires a strong shift in the managerial skills and attitude
- Each decision-maker (at design and operational level) should have a complete view of the mechanisms and types of interactions between the cooperating systems
- Special training is needed aimed at a deep revision of the current cultural protocols in the managerial, technical and responsibility chains
- An independent authority, not tied to the protocols to be changed, is needed
- A new resilience-centred organization should execute technical and managerial processes as if they were a single process
- In case of “unknown unknowns”, a multi-view (controllability) and shared analysis of the manifestations (flexibility) should be undertaken rapidly in order to introduce possible countermeasures (adaptability) with no centralized and delegated responsibility

## What can be done ? - Educational issue

What about the educational and cultural attitude of the multitude of untrained and risk unaware users who operate and interact with the system?

- Open door to the system with easy access for malicious activities (attacks to privacy, identity theft, malicious matching and profiling, to sabotage and terrorist attacks even those designed simply to cause widespread panic)
- Unpredictability of events generated by untrained users
- Evident social impact
- No way of solve this problem by only spreading education and culture on risks and consequences
- Toughest to address since it requires the spread of resilience-centred attitudes to a large patchy set of interacting entities, many of which have limited knowledge of their actions



## What can be done ? - Conclusions

- Research on dependability attributes and means precondition for the ability to develop and operate resilient systems
- Composing dependable systems does not imply the dependability of the composed system and least of all its resilience, due to dinamicity, the changing environment and the presence of “unknown unknowns” and thus to the impossibility of providing statistical measures
- Using the best known heuristics to design and operate socio-technical complex systems of systems in changing environments
- Put the maximal attention to the design and operation of interfaces
- Attention to small events and warnings that may indicate a deviation from expected behaviour, in order to try to build some qualitative metric for resilience

### Anyway

Socio-technical complex systems of systems in changing environments will fail sooner or later, with very difficult forecast of the consequences of such failures

Introduction of socio-technical complex systems of systems and extension of civil and social rights for citizens against an excessive possibly dangerous pervasiveness or high impact consequences

## Suggested readings

- Simoncini, L.: Socio-technical Systems of Systems: Can We Justifiably Trust Their Resilience. In: Dependable and Historic Computing: Essays dedicated to Brian Randell on the Occasion of His 75th Birthday, Jones, C.B. and Loyd, J.L. (eds.), Lecture Notes in Computer Science, 6875, pp 486-497, Springer-Verlag (2011)
- Littlewood, B.: Limits to Evaluation of Software Dependability. In: Software Reliability and Metrics, 7th Annual CSR Conf., Garmisch-Partenkirchen, pp. 87-110, Elsevier (1991)
- Laprie, J.C.: From Dependability to Resilience. Technical report LAAS n. 08001 (2008)
- Taleb, N.N.: The Black Swan: The Impact of the Highly Improbable. Random House and Penguin. ISBN 978-1-4000-6351-2. New York (2007). The book was completed in 2010 with the second edition including a long essay "On Robustness and Fragility"
- Taleb, N.N.: The Role and Nature of High Impact Events (Black Swans): Technical Commentary and Empirical Data. (2008) <http://www.fooledbyrandomness.com/EDGE/index.html>
- Jackson, S.: Architecting Resilient Systems. John Wiley & Sons, Hoboken, NJ (2010)
- Randell, B.: Dependability, Structure and Infrastructure. In: Cyberspace Security and Defence: Research Issues. Kowalik, J.S., Gorski, J. and Sachenko, A. (eds.), pp. 143--160, NATO Science Series II, ISBN 1-4020-3380-X, Springer (2005)
- Jones, C.B., Hayes, I.J., Jackson, M.A.: Deriving Specifications for Systems that are Connected to the Physical World. In: Formal Methods and Hybrid Real-Time Systems: Essays in Honour of Dines Bjørner and Zhou Chaochen on the Occasion of Their 70th Birthdays. Jones, C.B., Liu, Z. and Woodcock, J. (eds.), Lecture Notes in Computer Science, 4700, pp 364-390, Springer-Verlag (2007)