Technological vulnerability: parameters and definitions

L J Robertson, PhD student, University of Wollongong. Presenting author Lindsay J Robertson
lindsay@tech-vantage.com

ABSTRACT
In the field of infrastructure security, there is significant definitional diversity of terms such as "vulnerable", "resilient", and even "risk". Without clear definitions any derived metric will be similarly imprecise, and without metrics we can neither assess "vulnerability",nor evaluate options for improvement. While research has made advances in metrics applied to homogeneous systems, adequate modelling of inhomogeneous (more than one service transmitted) and interconnected infrastructures (that supply goods and services to end-users), is generally regarded as being computationally intractable. This paper specifically considers the possibility of characterising end-user "exposure" of a complex technological system, and developing a metric for "exposure" that would allow evaluation of options for improvement in end-user security.

1 Introduction

The Merriam Webster dictionary defines *Vulnerable* as "...*1: capable of being physically or emotionally wounded 2: open to attack or damage: assailable* ..."
It is perhaps a sign of increased dependence upon technology that the term "vulnerability" has migrated from this original context to the realm of complex technological systems. Certainly, "vulnerability" is a term increasingly associated with technological systems for delivering goods and services, and with the closely related topic of critical infrastructure security (see Robertson, (2010) and Gheorghe & Vamanu (2004)). Within both of these contexts, individuals have become progressively more aware of the long and interdependent (technology) supply chains that provide our most basic needs.

Many options exist for decreasing the vulnerability ("hardening") of existing infrastructural services, though in some cases one might suspect that these efforts offer little incremental value. In other cases, technology options for provision of end-user services exist, and may be preferable to risk reduction efforts addressed to existing technologies. There is pressure to identify the most cost-effective approaches, but lack of clarity of definitions hamper efforts to properly prioritise and evaluate options for infrastructural improvement. Definitions that are clear and consistent across a wide range of fields, would allow efforts to secure reliable services to be prioritised better, and would allow overall gains to be more readily demonstrated.

The Merriam Webster dictionary definition of vulnerability has been quoted previously. Birkman (2006) states that "...*the different definitions and approaches show it is not clear just what "vulnerability" stands for as a scientific concept... We are still dealing with a paradox: we aim to measure vulnerability, yet we cannot*

define it precisely... Although there is no universal definition of vulnerability..." Birkman also cites "...*Strategy for Disaster Reduction (UN/ISDR), which defines vulnerability as: The conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards (UN/ISDR, 2004)*...". Einarsson and Rausand (1998, p 535) write "...*[t]he vulnerability concept has yet not been given a generally accepted definition for technological applications...*". Werbeloff and Brown (2011, p 2362), go further by stating that "...*[t]he concept of 'vulnerability' is a dynamic concept and as such is difficult to define*...". Baldick *et al*., (2009, col2, p1), in reflecting on power systems, declare that at the present time, there "...*is not a commonly accepted vulnerability index or assessment method*...". Agarwal and England (2008) agree that even within the (mature) structural engineering discipline, there is "…*no satisfactory measure of robustness: not even a widely agreed definition...*".

This conference topic envisages complex, and inter-related infrastructures;
It may be assumed that the topic of interest is not primarily homogeneous systems (in which a single service is routed through a network, and nodes simply aggregate or distribute that service) but rather inhomogeneous technological systems in which nodes require a variety of inputs to function, and where different parts of the technological system transfer different goods/services. Definitional difficulties cause some specific issues in the field of critical infrastructure and associated technological system.

2 Difficulties associated with terminology and definitions

2.1 Risk and harm

Different definitions of "Harm" will generate different assessments: quite minor "harm" to a sewage system might leave an apartment dweller without usable accommodation. By contrast, quite severe "harm" to a local road system might have limited effect on end-users if power and sewage are available, and supermarkets are close. Rigorous indexation of "harm" to the end-user, would offer a consistent definition of "harm".
In regard to definitions of "risk", ISO 31000 defines "risk" as "...*effect of uncertainty on objectives*..." - such a definition is hardly precise or exclusive!
Posner (2004) has attempted to consider events characterized by large harm and low probability. Others have considered events that are simply low probability ("black swans"). Within less extreme examples, many who practice in the field of risk management have noted that assessments based on a product of harm-probability and harm-magnitude, generates similar metrics for high-impact low probability, and low-impact high probability events.

2.2 Vulnerability

"Vulnerability" can be considered in terms of relationship between operational system load and design maximum system load, however that approach has limited application. This paper proposes that a refinement of the concept of "susceptibility

to failure" offers a more useful definition, and the term "exposure" will be used for this refined definition of "vulnerability".

3 "Exposure" of inhomogeneous technology systems

3.1 Inhomogeneous technology system risks

For homogeneous technological systems, graph theory offers some metrics to assess configuration and hence technological "vulnerability" (authors such as Idika & Bhargava (2012) review a number of metrics to describe the degree of interconnectedness of specific homogeneous networks). For inhomogeneous systems, by contrast, current thought is that complete modeling and characterisation is computationally impractical. Since the vast majority of technological systems are inhomogeneous, this is a significant gap.

Any measure of risk can only be associated with a specific technological system (a different technological system would have different values of risk) – yet when risk is quoted, it is rare to actually see inhomogeneous technological systems characterised in a way that quantitatively links it to the associated risks. If it were possible to characterise the configuration and components of inhomogeneous (infrastructural) systems, this would help in assessing their relative weakness level and the relative value (to the end-user) of "hardening" approaches.

3.2 Characterisation of inhomogeneous systems

The previous section has converged on the issue of characterising inhomogeneous infrastructural systems, as a basis for improved assessment of alternative hardening approaches and targeting of efforts. This section proposes a general approach to the characterisation of inhomogeneous critical infrastructural systems, leading to a method of defining relative exposure to risk. The proposed approach assumes that it is possible to represent inhomogeneous infrastructural systems as set of interconnected unit operations, each needing a complete set of inputs in order to generate a design output.

3.3 Inverting the risk issue - hazards and exposures

Risk assessments generally start with hazard identification, and proceed to assess the magnitude of harm, the probability of the hazard occurring, the likelihood that the identified hazard will actually cause the harm and the nature and effectiveness of any mitigation measures. This approach does not generate a good measure of the "vulnerability" of a technological system, nor a metric that can be readily used to evaluate alternative improvement options. It is proposed that a different approach is possible and useful.

A very fundamental, though seldom articulated truth is that a hazard is not a hazard unless it aligns with a system weakness. Therefore, regardless of the statistical probability of any specific hazard occurring (and such probabilities will tend to 1.0 over a long-enough period) occurring, the number of weaknesses will indicate the relative vulnerability/exposure of a specific technological system.

3.4 Quantifying the weaknesses of a technological system

If the (inhomogeneous) technical system is represented in terms of a set of interconnected unit operations, each of which functions when, and only when all inputs are present (and which finally delivers the designated goods/services), then the quantum of input streams crossing the system boundaries has coincidentally defined the points of weakness. This is illustrated in the Figure 1.

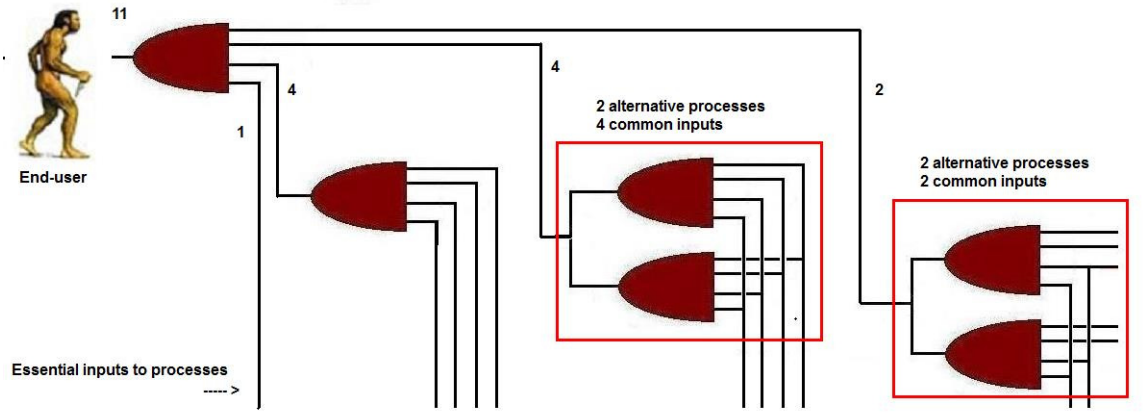

Figure 1 Weaknesses in processes leading to delivery of goods/services

Some clarifications and enhancements of this concept are needed, but an inversion of viewpoint is being proposed: instead of listing/evaluating threats/hazards, it is proposed to examine the number of hazard-targets (weaknesses).

For quantitative assessment, it is proposed to refer to the "exposure" of the technological system – the number of hazard-targets. However simple, a metric that assesses the number of points of weakness of a technological system offers some real utility: it is possible to compare technological systems and determine which has more "exposure", and it is possible to evaluate a proposed change (configuration or components) to an inhomogeneous system and obtain a metric for the decrease in "exposure". Considered in simplistic terms, it is proposed that an inhomogeneous technological system can be represented as a set of AND-gate/unit operations, each assumed to generate an output if, and only if, all inputs are present. For such a representation, each input (crossing the system boundary) represents a stream without which the output will fail – and so the sum of all inputs (to the sum of all unit operations), represents the number of weaknesses of the technological system and offers a measure of that system's "exposure".
In order to be useful, this basic definition needs to be refined and several obvious issues need to be addressed.

3.5 Refining the concept of "exposure"

The proposed "AND gate" concept is simply a notional/logical and-gate, producing an output when all inputs exist. Inputs will include process streams, but in addition, one input to the "gate" is ALWAYS the functional unit operation itself (in an "operational" timeframe).

It is likely that there will be cases where an output stream could be alternatively sourced from more than one process. If all of the alternative processes that can generate a specified output are considered within a "bubble", it can be appreciated that the output stream is only jeopardised when inputs streams that are common to all the (alternative) processes are jeopardised. The "exposure" of the alternatively-sourced output is therefore related to the number of common inputs to all of the alternative processes.

In a real inhomogeneous system, there will be hazards that have a higher statistical probability of occurring within a given timeframe, and there will also be hazards with a lower probability. Nevertheless, it can be observed that over a sufficiently long time period, all probabilities approach 1.0, and so a characterisation of the number of weak points remains a valid and useful metric.

In a real inhomogeneous system, many intermediate streams have some buffering capability. Such capability reduces the impact of very short-duration outages, and in a dynamic simulation of a specific system the interactions of demand variation and buffering capacities is of the essence. Nevertheless, few situations exist where long term buffering is possible, and for very many situations (e.g. electric power required to operate a motor) buffering is not available at all.

A metric for “exposure” would be impractical if the approach generated an unbounded scope. Initial work indicates that end points (where multiple alternatives exist, with no common inputs) are practical.

4 Conclusion

4.1 Significance of technology configuration

This paper has commenced with a very high level review of definitions: it has proposed the consistent indexation of “harm” to end users, and has noted the need to develop a refined definition of the concept of “vulnerability” for inhomogeneous technological systems.

4.2 Technology system exposure

The paper has proposed an approach for characterising a complex technological system; this approach generates a metric that represents the total “exposure” (to hazards) of the technological system. This provides a quantifiable refinement of the general concept of “vulnerability”, and unlike “risk” approaches, it not only recognises the significance of the underlying technological system but generates a metric closely linked to the actual weaknesses of a technological system.

4.3 Application

As professionals considering the next generation of infrastructures, we note that

- Our infrastructural systems have tended to grow progressively larger and more complex, and to present more and more points of weakness.

- It is important to avoid expending much effort on “hardening” one system while failing to recognise that another system is inherently more vulnerable.
- It is important to avoid prioritising effort on one approach to “hardening”, without realizing that other approaches might generate a better outcome.

.

This paper proposes a simple method that characterises a technological system by assessing the technological weaknesses, offers a useful approach to both prioritisation of “hardening” efforts, and to reducing end-user exposure to failure.

References

Agarwal, J; England, J (2008) "Recent developments in robustness and relation with risk" Proceedings of the Institution of Civil Engineers: Structures and Buildings 191(4) p183-188.

AS/NZS ISO 31000:2009. Risk Management - Principles and guidelines.

AS/NZS ISO 31000:2009. ISO GUIDE 73:2009 Risk management: Vocabulary.

Baldick, R. C., B; Dobson, I; Dong, Z; Gou, B; Hawkins, D; Huang, Z; Zhang, X (2009). Vulnerability assessment for cascading failures in electric power systems, 2009 IEEE/PES Power Systems Conference and Exposition, PSCE 2009.

Birkman J (2006), Ed. "Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions." Publisher United Nations university. Place of Publication Tokyo ISBN-10 9280811355 ISBN-13 9789280811353.

Einarsson, S; Rausand, M (1998). An approach to vulnerability analysis of complex industrial systems, Risk Analysis. 18 (5), pp. 535-546.

Gheorghe A V & Vamanu D V (2004) Towards QVA - Quantitative vulnerability assessment: A generic practical model, Journal of Risk Research. 7: 613-628.

Idika N & Bhargava B (2012) Extending attack graph-based security metrics and aggregating their application. IEEE Transactions on Dependable and Secure Computing. art. no. 5611550, pp. 75-85.

Posner, R. A. (2004). Catastrophe: Risk and Response Oxford University Press, 2004).

Robertson L J (2010) "From societal fragility to sustainable robustness: Some tentative technology trajectories" Technology in Society 32 (40-41) p342-351.

Werbeloff, L; Brown, R(2011). Working towards sustainable urban water management: The vulnerability blind spot, Water Science and Technology. 64: 2362-2369.