

## Chapter 2

# Governance Vulnerability Facets

**Abstract** In this chapter, several models supporting the notion governance for vulnerability assessment are presented. These include structural vulnerability, operational vulnerability, managerial vulnerability, and relational vulnerability. These notions are presented in view of *Quantitative Vulnerability Assessment* (QVA), which is a method to diagnose vulnerability in complex systems with a focus on strategies that could be undertaken for sustained system development. Theory supporting QVA is presented as well as the general means of transportability of the application are presented.

### 2.1 Strategic Approach for Dealing with Diverse Stakeholders

It is obvious that organizations in the twenty-first century operate under conditions of ambiguity, complexity, emergence, interdependence, and uncertainty (Flood and Carson 1993; Katina et al. 2014; Skyttner 2005). Regardless of your system of interest: health care, energy, transportation, security, etc.: you organizations operate under increasing lack of clarity and situational understanding, it has many richly and dynamically interacting stakeholders, systems, and subsystems with behavior difficult to predict, analysts and stakeholders might lack the ability to deduce behavior, structure, and performance of the constituent elements, and there is a likelihood that your system is influenced and it influenced the state of interconnected systems. Using this backdrop, one can argue that many of our systems, critical to public well-being, operate in the open and have a good chance of failing. The former, which is the subject of this book, for the most part, is referred to as vulnerability. There are several models that address the concept of vulnerability. These models are the subject of the remainder of this chapter along with strategic measures that enable system development and sustainability. Appendix B has been prepared to address ‘governance’ at a more general level.

## 2.2 Angles and Targets of Vulnerability

### 2.2.1 *Structural Vulnerability, System Stability, and Hysteresis*

The ever-increasing complexity associated with technology permeates system structures and patterns. The behavior of high-tech-addictive modern society in conjunction with the collective, contagious anxiety and the unrest brought about by hesitant and confusing reshufflings in the world order and the globalization, places vulnerability of critical infrastructures on top of the agenda of all consequential establishments. Governments, defense industries, private organizations, banking systems, natural catastrophes, technical failures, and accidents as well as terrorists tend to merge into a collage defining the landscape of challenges for the twenty-first century. Our attempt to put some order to this ‘mess’ comes in the form of a model for vulnerability assessment. The goal is to contribute to a management toolset for critical infrastructures management that places emphasis on strategies for sustainable development under present conditions. In particular, this chapter addressed the following topics: (i) quantification of the concept of vulnerability, (ii) making vulnerability an operational concept for sustainable development strategies, and (iii) enabling systems engineering as an approach to vulnerability management. This is done with the aim of arriving at a methodological approach for vulnerability estimating in critical infrastructures different levels (i.e., local and regional) and means to measure potential impact on system sustainable development.

There is a scarcity of practical approaches to quantify vulnerability in critical infrastructures. In the present text, the proposed model, practical and sound, offers: (i) a two-parameter description of vulnerability and the respective equation of state of the system: ‘operable’ and ‘inoperable,’ (ii) a division of the two-parameter phase space of the system into ‘vulnerability basins,’ and (iii) a scale of 0–100 ‘vulnerability’ and the means to measure the respective ‘vulnerability index.’ In essence, the proposed method can offer the ability to diagnose current system vulnerability. The method uses an extensive set of indicators involving internal and external elements with the capability to dynamically monitor the time evolution of the vulnerability as change occurs. Appendix C is reserved for an in-depth discussion on how to arrive at the compact analytic solution for the equation of systems with many component systems. Certainly, this involves hysteresis in which the current state of a system might depend on its history as found in ferromagnetic and ferroelectric materials as evidenced in thermostats and Schmitt triggers to prevent unwanted frequent switching. The aim of the model is to operationalize the concept of vulnerability in the context of multi-dimensional indicators of sustainability.

2.2.1.1    QVA: The Basic Assumptions

*Quantitative Vulnerability Assessment* (QVA) is a result of a warranted equivalence with *Quantitative Risk Assessment* (QRA)—coined within the closing decade of the past century and having made quite a career in the community of risk and safety managers worldwide (Gheorghe and Vamanu 2004a, b; Vamanu et al. 2016). Like its risk-related counterpart, QVA is about expressing its object—vulnerability—in numbers, in a scientifically defensible and practically meaningful way. Unlike QRA, QVA has to face an even more difficult task, for at this time there is no agreed ‘closed formula’ for vulnerability, whereas for risk, one does have a formula: *risk* of a disruptive event equals the *probability* of occurrence of an event times the *measure of event consequences* powered to a subjective *consequence perception exponent*.

At the root of this dis-symmetry is common semantics. Without excessively elaborating, let it be noted that such a popular reference as the Webster’s new explorer encyclopedic dictionary (Merriam-Webster 2006) retains, in the entry for ‘risk,’ the instrumental ingredients of the formula. Table 2.1 attempts to draw out these differences.

In QRA, the task is to take a well-substantiated *noun* to a number. In QVA, the task is to take an *adjective*, reflective of a virtuality (i.e., *open to...*) to a number. To achieve this, four assumptions are made:

**Assumption 1** First, one needs to adapt an operational definition for vulnerability as openness of a system—openness to losing its design functions, and/or structural integrity, and/or identity under the combined interplay of two sets of factors (*U* and *V*), where *U* is risk-featuring factor while *V* is management response-featuring factor. All factors are supposed to be eventually quantifiable by appropriate indicators. *U* factors involve risks that the system is prone to (i.e., the disruptive developments). These include (i) elements *internal* to the system, and/or (ii) reflective to the *processes* that the system hosts, (iii) to the performance of a system of interest. We refer to these as *fast-variable indicators* since they are on the move, constantly. *V* factors involve slow-variable indicators external to the system. These influence system and capability of the system’s management to react/respond to internal developments.

**Assumption 2** The method carries the assumption that the measurable and monitored indicators (i.e., parameters) can be aggregated such that control variables of *U* and *V* can be obtained. This then suggests that *U* and *V* are membership functions of the fuzzy set theory (Christen et al. 1995; Katina and Unal 2015). Accordingly, if

**Table 2.1**    A basic dis-symmetry of risk and vulnerability

Risk (noun)	Vulnerable (adjective)
The <i>chance</i> of injury, damage, or loss; dangerous change; hazard; the <i>degree</i> of probability of loss	Open to being physically or emotionally wounded; open to attack or damage

$X_i, i = 1, 2, \dots, n$  are the normalized indicators contributing in the definition of  $U$ , then one has:

$$U(X_1, X_2, \dots, X_n) = \min\left(1, (X_1^p + X_2^p + \dots + X_n^p)^{\frac{1}{p}}\right) \quad (2.1)$$

where  $X_i$  are obtained from the physical indicators  $Y_i$  as:

$$X_i = A \log_{10}(Y_i) + B, \quad i = 1, 2, \dots, n \quad (2.2)$$

The constants  $A$  and  $B$  are, in turn, derived from the assumed knowledge of two pairs of values for the normalized and physical indicators:  $X_i^{(1)} = 0.2$  and  $X_i^{(2)} = 0.6$ .

$$A \log_{10}(Y_i^{(1)}) + B = X_i^{(1)} \quad (2.3)$$

$$A \log_{10}(Y_i^{(2)}) + B = X_i^{(2)}$$

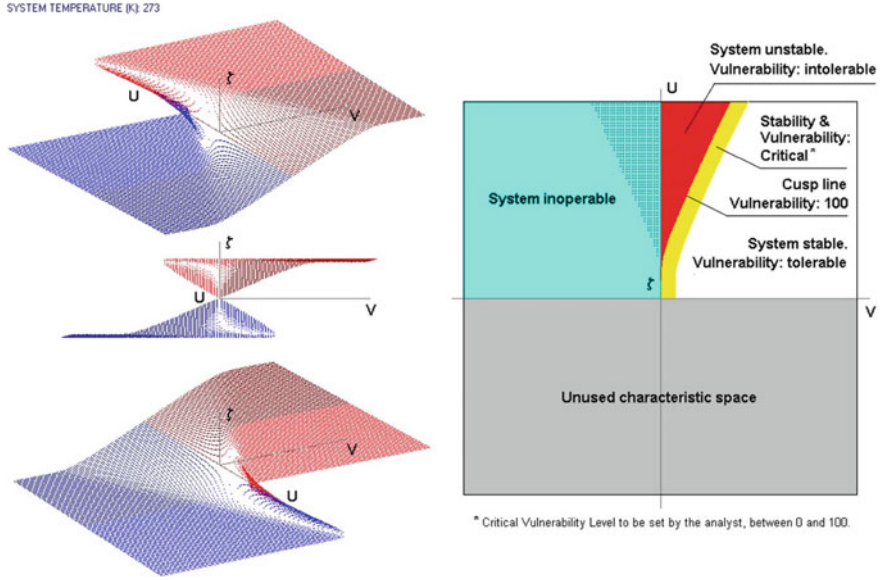
Wherefrom

$$\begin{aligned} A &= (X_i^{(2)} - X_i^{(1)}) / (\log_{10}(Y_i^{(2)}) - \log_{10}(Y_i^{(1)})) \\ B &= (X_i^{(2)} \log_{10}(Y_i^{(1)}) - X_i^{(1)} \log_{10}(Y_i^{(2)})) / (\log_{10}(Y_i^{(1)}) - \log_{10}(Y_i^{(2)})) \end{aligned} \quad (2.4)$$

A similar set of equations would be given for  $V(X_1, X_2, \dots, X_n)$ .

**Assumption 3** Once  $U$  and  $V$  are determined, one then assumes that these make the aggregated control variables of a two-state, multi-component system (see Chap. 7 in Vamanu et al. 2016). By design, the solution adopted for modeling vulnerability comes close to the Bragg–Williams approximation. According to this approach, the membership fractions in a two-state system can be obtained based on probabilities of individual transitions between the two states. The interplay of the actual ‘physical’ and potentially numerous system indicators will result in variations of the aggregated parameters ( $U$  and  $V$ ), which in turn drives the system ‘state’ in and out of a region of instability (Vamanu et al. 2016). In a conventional sense, an *operable* system may thereby appear as: (i) stable and therefore featuring a low vulnerability, (ii) critically unstable (i.e., vulnerable), or (iii) unstable and thereby featuring a high vulnerability. Beyond these, the system may only be found *inoperable*. A schematic of structural vulnerability is presented in Fig. 2.1.

**Assumption 4** As given above, it is not possible to create a *Vulnerability Scale* based on the assessment of the system state in the  $U$  space and  $V$  space. The following is adapted: (i) measuring the *Vulnerability Index* is done using Euclidian distance of the state of  $U$  and  $V$  to the cusp line in the  $U \geq 0, V \geq 0$  region of the  $(U, V)$  plane, and (ii) normalizing the index such that, everywhere on the cusp line,



**Fig. 2.1** Schematics of the QVA machine; left: characteristic of system (i.e., collection of real solutions of the ‘equation of state’ Eqs. 2.6 and 2.16. Adapted from Gheorghe and Vamanu (2004b)

including its  $V \rightarrow 0$  portion, the *Vulnerability Index* must be equal to 100, the assumed maximum.

Subsequently, if  $D$  is the said distance to the cusp line, then the *Vulnerability Index*,  $V_{\text{scale}}$ , on the 0–100 *Vulnerability Scale* is:

$$V_{\text{Scale}} = 100 \left( 1 - \frac{D}{15} \right) \quad (2.5)$$

where the  $(U, V)$  field has been conventionally limited to  $0 \leq U \leq 15$ ,  $0 \leq V \leq 15$ .

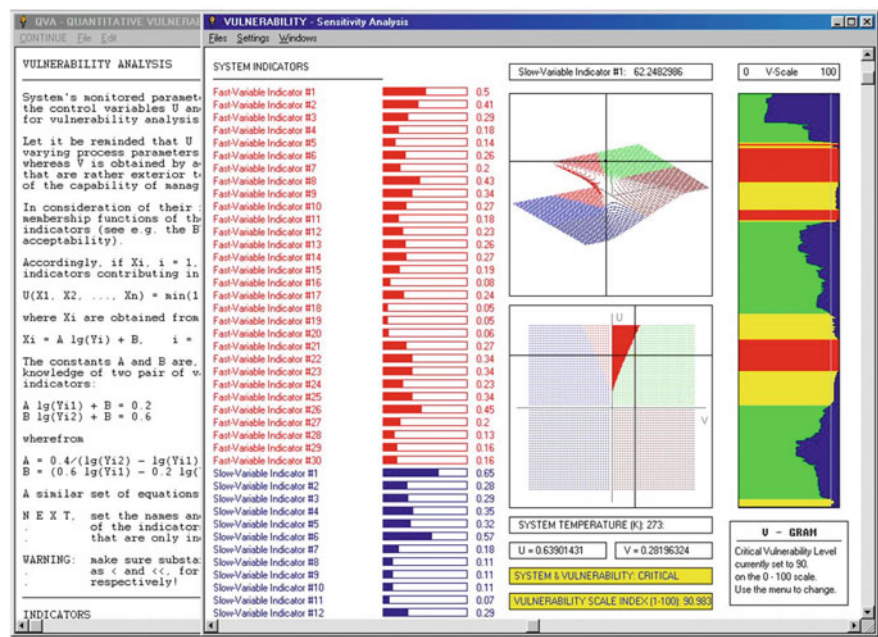
Since no analytic solution for the equation of the cusp line is readily available, distance,  $D$ , is evaluated up to the Bézier interpolation of a sufficient number of  $(U, V)$  knots on the cusp. The knots are determined as median points on the positive  $V$ -axis, for every positive  $U$ , between the last  $V$  that provides three solutions to the system’s equation of state (i.e., equation of ‘characteristic’ in the sense of Thom (1975, 1983), namely:

$$\text{th} \left( \frac{U \cdot \zeta + V}{\theta} \right) = 2\zeta \quad (2.6)$$

and the first  $V$ , larger than the preceding, that provides only one solution. Symbol  $\tanh$  stands for the hyperbolic tangent of the ensuing argument. As argued in the next section, the region of the characteristic's topological foil featuring a single solution to the equation of state is the *region of system stability*, whereas the region featuring three solutions, of which only two can normally be accessed, is the *region of system instability*.

The rough equivalence of (i) *system Instability...Highest/Intolerable Vulnerability* and (ii) *system Stability ... Lower/Tolerable Vulnerability* is assumed. In the sense of the definition, within the region of instability, the *Vulnerability Index* is supposed to be uniformly 100, while it would gradually decrease away from the edge of the instability region. In a basic ‘simple’ computer-assisted QVA exercise, and for the sake of an example, Fig. 2.2 depicts a system described by 30  $U$ -type generic indicators and 20  $V$ -type indicators.

The geometric (Euclidian) distance of the state point in the  $(U, V)$  plane to the cusp line is taken as a measure of the vulnerability. The measure is normalized such that vulnerability is 100 everywhere on the cusp line and its analytic continuation as  $V$  is equal to 0.



**Fig. 2.2** An example of a computerized QVA exercise involving 30  $U$ -type and 20  $V$ -type indicators.  $V$ -Gram represents a histogram of vulnerability over time on the scale of 0–100. It can be placed on record and then called back for analysis, adapted from Gheorghe and Vamanu (2014)

### 2.2.1.2 QVA Modeling: Vulnerability and Stability in Multi-component Systems

Let us assume a system consisting of a large number,  $M$ , of elemental constituents or *members*. Elemental is taken in context as in ‘atomic’ sense such that a member should be seen as complex and fully connected to its environment, and yet indivisible as in a ‘black box.’ System members interact with each other with, in principle, a varying intensity. To describe the interaction, a *coupling constant*, or *intrinsic parameter*,  $U$ , is assumed to be either known or inferable. However, it is also recognized that members state can also be influenced by factors exterior to the system, as issue being accountable via an *influence field* or *extrinsic parameter*,  $V$ .

A member of the system may assume only two distinct *states*, state 1 and state 2. The generic ‘states’ may be seen as opposite in respect of a given criterion of judgment as in normal–abnormal, up–down, and pro–con, although this is not *always* the case. The only condition of essence is that states 1 and 2 are distinguishable from each other. At any given time,  $t$ , let  $M_1$  members be in state 1 and  $M_2$  members be in state 2. Since only two states are possible, one has:

$$M_1 + M_2 = M \quad (2.7)$$

The overall state of the system may then be described via the pair of numbers  $(M_1, M_2)$ , while the system dynamics, or ‘motion’ in its state space, will follow from variations in  $M_1$  and  $M_2$  that should be consistent with Eq. (2.7). The smallest transitions in the state of the system would obviously involve alterations by one unit in the numbers of members:

$$(M_1 - 1, M_2 + 1) \xleftarrow{w_{12}} (M_1, M_2) \xrightarrow{w_{21}} (M_1 + 1, M_2 - 1) \quad (2.8)$$

Assume that the respective transitions are governed by the probabilities  $W_{12}$  and  $W_{21}$ , respectively, as indicated in the relationship (Eq. 2.8). Admission of the process (Eq. 2.8) leads also to the recognition of a *function of distribution* of the system’s states,  $f(M_1, M_2)$ , that would obey the master Eq. (2.9):

$$\begin{aligned} \partial f(M_1, M_2, t) / \partial t = & w_{21}(M_1 - 1, M_2 + 1) \cdot f(M_1 - 1, M_2 + 1) \\ & + w_{12}(M_1 + 1, M_2 - 1) \cdot f(M_1 + 1, M_2 - 1) \\ & - (w_{21}(M_1, M_2) + w_{12}(M_1, M_2)) \cdot f(M_1, M_2) \end{aligned} \quad (2.9)$$

The state  $(M_1, M_2)$  of the system can alternatively be described by the *membership fraction*

$$\zeta = (M_1 - M_2) / (2M), \quad (2.10)$$

defined such that if all system members are in state 1, then  $\zeta = 1/2$ , whereas if all members are in state 2, then  $\zeta = -1/2$ .

Upon that, one notes that the master Eq. (2.9) involves the following states:

$$\begin{array}{ll} (M_1, M_2) & \zeta \\ (M_1 - 1, M_2 + 1) & \zeta - 1/M \\ (M_1 + 1, M_2 - 1) & \zeta + 1/M \end{array}$$

so that Eq. (3.3) may be rewritten as:

$$\begin{aligned} \partial f(\zeta)/\partial t = & w_{21}(\zeta - 1/M)f(\zeta - 1/M) + w_{12}(\zeta + 1/M)f(\zeta + 1/M) \\ & - (w_{21}(\zeta) + w_{12}(\zeta))f(\zeta) \end{aligned} \quad (2.11)$$

The initial assumption that the number,  $M$ , of system members is large allows one a series expansion of all quantities in the second member of Eq. (2.11). Restricting the expansion to the second order in  $(1/M)$ , one obtains:

$$\partial f/\partial t + \partial J/\partial \zeta = 0. \quad (2.12)$$

Equation (2.12) is a continuity (i.e., conservation) equation for the state distribution function  $f$ , involving the ‘current’

$$J = (1/M)(w_{21} - w_{12}) \cdot f - (1/(2M_2))\partial((w_{21} + w_{12}) \cdot f)/\partial \zeta \quad (2.13)$$

Looking for the stationary states of the system, one assumes now:

$$\partial f/\partial t = 0, \quad (2.14)$$

which leaves one with the equation

$$\partial J/\partial \zeta = 0. \quad (2.15)$$

having as solution

$$J = \text{constant and, in particular, } J = 0 \quad (2.16)$$

Using the expression (2.13) of the current  $J$ , Eq. (2.16) can immediately be integrated to give:

$$f(\zeta) = \text{const} \cdot \frac{\exp \left[ 2M_1 \int_{-1/2}^{\zeta} \frac{w_{21}(\xi) - w_{12}(\xi)}{w_{21}(\xi) + w_{12}(\xi)} d\xi \right]}{w_{21}(\zeta) + w_{12}(\zeta)} \quad (2.17)$$

The constant in Eq. (2.17) can be determined setting the  $f(\zeta)$  to be normalized to 1:



$$\int_{-1/2}^{1/2} f(\zeta) d\zeta = 1 \quad (2.18)$$

To normalize, that is, to fully determine the distribution function  $f(\zeta)$ , one needs to make an assumption on the analytical form of the transition probabilities,  $w_{12}$  and  $w_{21}$ . The following expressions would correspond to the notion that the transitions are a cooperative phenomenon:

$$\begin{aligned} w_{12}(\zeta) &= wM_1 \cdot \exp(-U \cdot \zeta + V/\theta) \\ w_{21}(\zeta) &= wM_2 \cdot \exp(U \cdot \zeta + V/\theta) \end{aligned} \quad (2.19)$$

where  $U$  is the coupling constant (intrinsic parameter) and  $V$  is the influence field (extrinsic parameter) that were previously introduced, while  $\theta$  is a generalized ‘temperature’ of the system.

One makes now the natural assumption that the values of the membership fraction  $\zeta$  that make the distribution function  $f(\zeta)$  reach its extremes would make the space of possible states (the ‘characteristic’) of the system. Taking the expressions (2.19) of the transition probabilities into Eq. (2.17), and requesting that the condition

$$\partial f(\zeta)/\partial \zeta = 0 \quad (2.20)$$

be fulfilled, one has:

$$\text{cth}((U \cdot \zeta + V)/\theta) = (1/2 - 1/(U/\theta - 2M))/\zeta, \quad (2.21)$$

where  $\text{cth}$  denotes the hyperbolic cotangent function,  $\text{cth}(x) = (\exp(x) + \exp(-x))/(\exp(x) - \exp(-x))$ . Using again the fact that the number of members,  $M$ , in the system is large, the second term in the parenthesis in the right-hand side of Eq. (2.21) is ignored, so that, finally, the space of system states

$(U, V, \zeta)$  is given by the equation:

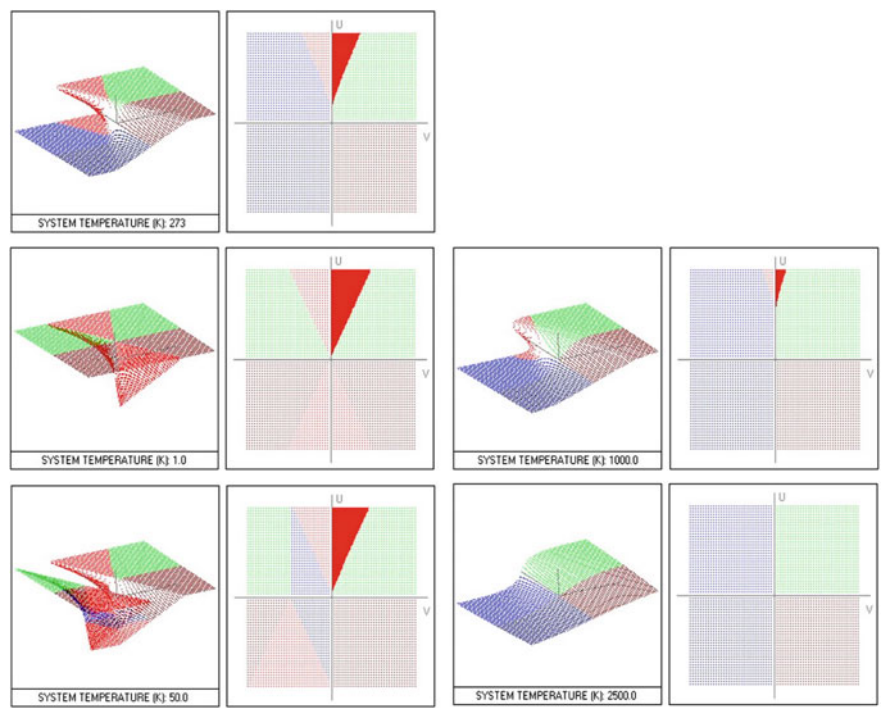
$$\text{th}((U \cdot \zeta + V)/\theta) = 2\zeta \quad (2.22)$$

where  $\text{th}$  denotes the hyperbolic tangent function,  $\text{th}(x) = (\exp(x) - \exp(-x))/(\exp(x) + \exp(-x))$ . Depending on the degree of interaction between system constituents (members), reflected in the coupling constant  $U$ , and on the external influence on all system members—reflected in the field  $V$ , and also taking into consideration the temperature,  $\theta$ , of the system, Eq. (2.22) may display the following number of real solutions  $\zeta$  that may be related to the overall system condition shown in Table 2.2.

Figure 2.3 renders the situation. The boxes in the left-hand side present the cuspidal foil  $\zeta_{\text{sys}} = \zeta(U, V)$ , also known as system’s ‘characteristic,’ seen in perspective. The  $(U, V)$  plane on the right-hand side is color-coded to emphasize the different basins of the system’s ‘phase space.’

**Table 2.2** Overall system conditions associated with real solutions

Number of real solutions	System conditions
1	Stable. Smooth transitions in population membership, between state 1 and state 2 <b>Low and/or acceptable vulnerability</b>
3; of which 2 are identical	Critical. Sharp transitions in membership between states 1 and 2 are possible. Either state 1 or state 2 may suddenly become improbable <b>System is critically vulnerable</b>
3; all different from each other	Unstable. Sharp transitions in membership between states 1 and 2 are possible. Frequency of occurrence of states 1 and 2 are comparable. Though Eq. (22) has three real roots, the intermediate root is generally taken as having no physical meaning and is therefore discarded <b>System is dangerously/unacceptably vulnerable</b>



**Fig. 2.3** Generic system ‘characteristics’ at different temperatures, figures adapted from Gheorghe and Vamanu (2004b)

As it turns out, the aspect of the foil expressing the topology of the system's space of states would vary with the generalized 'temperature'  $\theta$ . The concrete details would, of course, depend on the scaling adopted for the 'energy'-wise parameters involved. Indeed, drawing further upon the physical analogy behind the model one would have  $\theta = k_B T$ , with  $k_B$  a 'Boltzmann' constant relating to the energy per degree of freedom of a system member and  $T$  being the 'absolute temperature.' Likewise, with the Ising model of ferromagnetics in mind, the coupling constant  $U$  would be reminiscent of the pair exchange energy, while  $V$  would bring to mind an external magnetic field casting its influence on all the 'spins' that make up the system. For practical purposes, the exercise attempted has adopted a 'Boltzmann' constant equal to  $1/273$ , while preserving the absolute 'temperature' scale, where the 0 centigrade would correspond to  $T = 273.15$ . That would take parameters  $U$  and  $V$  in the convenient range of 1–15.

On this parameter scaling, at a 'normal' temperature of 273 K, and higher up, the system 'characteristic' would show one instability region in the positive  $U$  range, whereas at lower temperatures, a second instability region would progressively manifest itself in the negative  $U$  and  $V$  range, until, very close to 0 K. The two instability regions would almost connect with each other at  $U = 0$  and  $V = 0$ . At this stage into the exercise, it is perhaps too early to speculate on the significance of such occurrences. More careful thinking should go, for example, into establishing whether negative  $Us$  (i.e., anti-ferromagnetic states) should at all be accepted, which would indicate a spontaneous antagonism of individual system members. At any rate, the current QVA model, relying on the definitions (Eqs. 2.1 through 2.4) for the indicators, would make use of only the  $U \geq 0$ ,  $V \geq 0$  quadrant of the  $(U, V)$  plane.

In this section, thus far, QVA is presented as an approach for cooperative behavior in multi-component systems. It is addressed along the line '*to whom it may concern*,' primarily targeting readers with a background in Physics that feel like getting more enlightened about and confident in QVA. If one is interested in the physical analogy of the model as well as logical and calculational flow, along with model assumptions, equations, and the respective notations and remarks on potential system collapse, interdependence, and temperature effects, then the authors suggest acquaintances with 'Appendix D' in Vamanu et al. (2016).

### ***Limitations of QVA***

The apparent association of the method proposed by catastrophe theory (CT) (Thom 1975, 1983; Zeeman 1977) may give rise to some discomfort in some segments of the critical readers, given the never-exhausted controversy around the meaning and the value associated with CT. A comprehensive coverage of the issues associated with CT is found in Thom (1983). Aware of those issues, present authors find it appropriate to note that given the way the QVA model was proposed, key objections fall off target. Table 2.3 is drawn to address these objections.

Notice that the last criticism, or rather an objection, steams from susceptibility of the QVA to experimental control—a previous objection, which paves the way to counter the fourth possible objection. Lingering one moment longer in the realm of

**Table 2.3** A summary of CT criticisms and comparative QVA strengths

CT Objections	QVA-related responses
‘CT may be reproached for being an abstract schema independent of physical reality’ (a paraphrase from Thom 1983)	Using as conceptual background for the QVA model, the archetype of order–disorder phenomena and phase transitions in multi-component (many-body) systems, and tracking the theoretical apparatus back to some concrete solutions such as the Bragg–Williams approximation to the Ising model—which, in turn, covers great many cases of ‘physical reality’—would largely free the proposed QVA approach from the objection
‘CT is in itself purely qualitative and it simultaneously ignores considerations of scale and the quantitative laws of classical Physics’ (a paraphrase from Thom 1983)	The QVA model, method, algorithm, and computer code as described are patent proof to the contrary: The statistical mechanics-inspired tools have provided for an effective quantitative approach to vulnerability, including a <i>Vulnerability Index</i> and <i>Scale</i> . If the scaling conventions may indeed be said as being user-defined, and thereby arbitrary, the topology of the phase space behind these is, on the other hand, univocal and indisputable—within the given model terms
‘CT is not susceptible to experimental control’ (a paraphrase from Thom 1983)	QVA <i>is</i> , undoubtedly, susceptible to experimental control and was created precisely with purpose in mind. The computer codes that were designed to implement the method are only the soft expression of a machine that may eventually take the hard form of a ‘black box.’ The code is designed to take in input by the dozens, of the physical indicators of a given system and delivering output multimedia including video and sound, which serves as an ‘alarm’ warning on system evolving vulnerability status
‘(There is) ... the thorny problem of uniqueness of models in CT: if one has two models, $M$ , $M'$ , in competition (on the same system), can one always find a model $M''$ that covers both?’ (a paraphrase from Thom 1983)	With QVA, the uniqueness issue is solved by (i) fairly admitting that models are <i>not</i> unique, a model $M$ for a system $S$ being fully determined by its collection of $U$ - and $V$ -type indicators, in both numbers and nature, and (ii) emphasizing that the <i>appropriateness</i> of a model—the only criterion of interest in accepting it for practical purposes—has to be settled by <i>experimentation</i>

Thom's (1983) comments, let us note that, the way it is proposed, the QVA may well make proof of some convenient 'ontological range', which Thom (1983) describes as 'the manner in which the phenomena [can] take place and in which it describes their underlying mechanisms' (Thom 1983, p. 111). The 'phenomenon' in the case of QVA is the *coherent convergence of dozens of internal, fast-varying, and external, slow-varying, system features, expressed in as many physically different indicators, into an identifiable and quantifiable vulnerability state*.

At this point, we suggest an 'Assumption Zero' of this research: *any critical infrastructure can be accommodated within the concept of a multi-component, multi-indicator system the parts of which would show some kind of collective behavior by virtue of their interacting, as well as some susceptibility to external factors acting upon the system components*.

While the current proposal should be seen as only a test of feasibility, further developments may consolidate a fully operational QVA methodology. In an attempt to make present concepts more 'fun,' researchers developed a 'mix game' approach to concepts outlined in this section—see Appendix D.

### 2.2.2 Operational Vulnerability and System Dynamics in Phase Portraits

In a study commissioned by the Swiss Federal Department of Defense, Civil Protection and Sports, and Directorate for Security Policy, by a research team of the Swiss Federal Institute of Technology (Gheorghe 2004), it was shown that the dynamics of a three-body component business system could be modeled using ordinary differential equations for a generalized measure of component 'productions' of  $X$ ,  $Y$ , and  $Z$  such that:

$$\begin{aligned} dX/dt &= a1 + a2X + a3X^2 + a4XY + a5XZ + a6Y + a7Y^2 + a8YZ + a9Z + a10Z^2 \\ dX/dt &= a11 + a12X + a13X^2 + a14XY + a15XZ + a16Y + a17Y^2 + a18YZ + a19Z + a20X^2 \\ dX/dt &= a21 + a22X + a23X^2 + a24XY + a25XZ + a26Y + a27Y^2 + a28YZ + a29Z + a30Z^2 \end{aligned} \quad (2.23)$$

In this equation, coupling coefficients  $ai$  may be nil. It is equally evident that the Euler solving of the system patterns above can also have the topologies of (1) unbounded states and (2) bounded states. The classification for bounded states can include fixed point, limit cycle, and strange attractor.

In turn, qualitative differences between attractor configurations can be captured by two indicators: the Lyapunov exponent,  $L$ , and the fractal (in effect, correlation) dimension,  $F$ .  $L$  is the largest of two quantities that are defined based on comparing successive Euler iterations of the solutions of system (Eq. 2.23):

$$\begin{aligned}
X_{n+1} &= X_n + hF(X_n, Y_n, Z_n) \\
Y_{n+1} &= Y_n + hG(X_n, Y_n, Z_n) \\
Z_{n+1} &= Z_n + hH(X_n, Y_n, Z_n)
\end{aligned} \tag{2.24}$$

and which account for the propensity of the solutions to either coalesce over a bounded topological variety or diverge to infinity.  $L$  is, therefore, relating to system's *stability*.  $F$ , on the other hand, relates to the degree the phase space is occupied by point states of the system: The larger the degree of occupancy, the larger the  $F$ . It is conjectured that  $F$  relates to two apparently conflicting qualities of the system: the *predictability* and the *maneuverability*. There is a built-in assumption that a system whose phase space pattern occupies more of the space foil-like or bulk configurations of higher  $F$  is likely to offer more space of maneuver for the coupling coefficients that describe the exchanges between system components, and yet, on the other hand, it is more difficult to point at a space region where the system state may find itself, at any time.

On the contrary, a string-like (lower  $F$ ) configuration in the phase space makes the inference of the system whereabouts easier—a higher predictability—whereas the maneuverability is, comparatively, lower.

### 2.2.2.1 The Rules

Speculating over the features above may result in the following classification of situations that can be monitored as it evolves in time because of fluctuations or otherwise intentional (programmed) evolutions in the coupling (exchange) coefficients  $ai$  that can be used in a dashboard for monitoring business systems:

```

-----
'Stability
if diagnose = "Fixed Point" then
    Current Stability State = "CALM"
    if Previous Stability State = "CALM" then Stability Trend = "CONSTANT"
    if Previous Stability State = "NORMAL" then Stability Trend = "IMPROVING"
    if Previous Stability State = "ACCEPTABLE" then Stability Trend = "IMPROVING"
    if Previous Stability State = "UNACCEPTABLE" then Stability Trend = "IMPROVING"
end if
if diagnose = "Limit Cycle" then
    Current Stability State = "NORMAL"
    if Previous Stability State = "CALM" then Stability Trend = "DETERIORATING"
    if Previous Stability State = "NORMAL" then Stability Trend = "CONSTANT"
    if Previous Stability State = "ACCEPTABLE" then Stability Trend = "IMPROVING"
    if Previous Stability State = "UNACCEPTABLE" then Stability Trend = "IMPROVING"
end if
if diagnose = "Strange Attractor" then
    Current Stability State = "ACCEPTABLE"
    if Previous Stability State = "CALM" then Stability Trend = "DETERIORATING"
    if Previous Stability State = "NORMAL" then Stability Trend = "DETERIORATING"
    if Previous Stability State = "ACCEPTABLE" then Stability Trend = "CONSTANT"
    if Previous Stability State = "UNACCEPTABLE" then Stability Trend = "IMPROVING"
end if
if diagnose = "Unbounded" then
    Current Stability State = "UNACCEPTABLE"
    if Previous Stability State = "CALM" then Stability Trend = "DETERIORATING"
    if Previous Stability State = "NORMAL" then Stability Trend = "DETERIORATING"
    if Previous Stability State = "ACCEPTABLE" then Stability Trend = "DETERIORATING"
    if Previous Stability State = "UNACCEPTABLE" then Stability Trend = "CONSTANT"
end if

'Predictability
if diagnose = "Unbounded" then Current Predictability State = "UNACCEPTABLE"
if diagnose = "Fixed Point" then Current Predictability State = "CALM"
if diagnose = "Limit Cycle" then Current Predictability State = "NORMAL"
if diagnose = "Strange Attractor" then
    if F<=D/4 then
        Current Predictability State = "CALM"
        if Previous Predictability State = "CALM" then Predictability Trend = "CONSTANT"
        if Previous Predictability State = "NORMAL" then Predictability Trend = "IMPROVING"
        if Previous Predictability State = "ACCEPTABLE" then Predictability Trend = "IMPROVING"
        if Previous Predictability State = "UNACCEPTABLE" then Predictability Trend = "IMPROVING"
    end if
    if F>D/4 and F<=D/2 then
        Current Predictability State = "NORMAL"
        if Previous Predictability State = "CALM" then Predictability Trend = "DETERIORATING"
        if Previous Predictability State = "NORMAL" then Predictability Trend = "CONSTANT"
        if Previous Predictability State = "ACCEPTABLE" then Predictability Trend = "IMPROVING"
        if Previous Predictability State = "UNACCEPTABLE" then Predictability Trend = "IMPROVING"
    end if
    if F>D/2 and F<=3*D/4 then
        Current Predictability State = "ACCEPTABLE"
        if Previous Predictability State = "CALM" then Predictability Trend = "DETERIORATING"
        if Previous Predictability State = "NORMAL" then Predictability Trend = "DETERIORATING"
        if Previous Predictability State = "ACCEPTABLE" then Predictability Trend = "CONSTANT"
        if Previous Predictability State = "UNACCEPTABLE" then Predictability Trend = "IMPROVING"
    end if
    if F>3*D/4 then
        Current Predictability State = "UNACCEPTABLE"
        if Previous Predictability State = "CALM" then Predictability Trend = "DETERIORATING"
        if Previous Predictability State = "NORMAL" then Predictability Trend = "DETERIORATING"
        if Previous Predictability State = "ACCEPTABLE" then Predictability Trend = "DETERIORATING"
        if Previous Predictability State = "UNACCEPTABLE" then Predictability Trend = "CONSTANT"
    end if
end if

'Maneuverability
if diagnose = "Unbounded" then
    Current Maneuverability State = "UNACCEPTABLE"
    if Previous Maneuverability State = "CALM" then Maneuverability Trend = "DETERIORATING"
    if Previous Maneuverability State = "NORMAL" then Maneuverability Trend = "DETERIORATING"
    if Previous Maneuverability State = "ACCEPTABLE" then Maneuverability Trend = "DETERIORATING"
    if Previous Maneuverability State = "UNACCEPTABLE" then Maneuverability Trend = "CONSTANT"
end if
if diagnose = "Fixed Point" then
    Current Maneuverability State = "UNACCEPTABLE"
    if Previous Maneuverability State = "CALM" then Maneuverability Trend = "DETERIORATING"
    if Previous Maneuverability State = "NORMAL" then Maneuverability Trend = "DETERIORATING"
    if Previous Maneuverability State = "ACCEPTABLE" then Maneuverability Trend = "DETERIORATING"
    if Previous Maneuverability State = "UNACCEPTABLE" then Maneuverability Trend = "CONSTANT"
end if

```

```

if diagnose = "Limit Cycle" then
    Current Maneuverability State = "ACCEPTABLE"
    if Previous Maneuverability State = "CALM" then Maneuverability Trend = "DETERIORATING"
    if Previous Maneuverability State = "NORMAL" then Maneuverability Trend = "DETERIORATING"
    if Previous Maneuverability State = "ACCEPTABLE" then Maneuverability Trend = "CONSTANT"
    if Previous Maneuverability State = "UNACCEPTABLE" then Maneuverability Trend = "IMPROVING"
end if
if diagnose = "Strange Attractor" then
    if F<=D/8 then
        Current Maneuverability State = "ACCEPTABLE"
        if Previous Maneuverability State = "CALM" then Maneuverability Trend = "DETERIORATING"
        if Previous Maneuverability State = "NORMAL" then Maneuverability Trend = "DETERIORATING"
        if Previous Maneuverability State = "ACCEPTABLE" then Maneuverability Trend = "CONSTANT"
        if Previous Maneuverability State = "UNACCEPTABLE" then Maneuverability Trend = "IMPROVING"
    end if
    if F>D/8 and F<=D/4 then
        Current Maneuverability State = "NORMAL"
        if Previous Maneuverability State = "CALM" then Maneuverability Trend = "DETERIORATING"
        if Previous Maneuverability State = "NORMAL" then Maneuverability Trend = "CONSTANT"
        if Previous Maneuverability State = "ACCEPTABLE" then Maneuverability Trend = "IMPROVING"
        if Previous Maneuverability State = "UNACCEPTABLE" then Maneuverability Trend = "IMPROVING"
    end if
    if F>D/4 then
        Current Maneuverability State = "CALM"
        if Previous Maneuverability State = "CALM" then Maneuverability Trend = "CONSTANT"
        if Previous Maneuverability State = "NORMAL" then Maneuverability Trend = "IMPROVING"
        if Previous Maneuverability State = "ACCEPTABLE" then Maneuverability Trend = "IMPROVING"
        if Previous Maneuverability State = "UNACCEPTABLE" then Maneuverability Trend = "IMPROVING"
    end if
end if

'System Condition

if Current Stability State = "UNACCEPTABLE" then Current System Condition = "UNACCEPTABLE"

if Current Stability State = "ACCEPTABLE" then
    if ((Current Predictability State = "UNACCEPTABLE") or (Current Maneuverability State =
"UNACCEPTABLE")) then
        Current System Condition = "UNACCEPTABLE"
    end if
    if ((Current Predictability State = "ACCEPTABLE") or (Current Maneuverability State =
"ACCEPTABLE"))
and ((Current Predictability State<>"UNACCEPTABLE") and (Current Maneuverability
State<>"UNACCEPTABLE"))) then
        Current System Condition = "ACCEPTABLE"
    end if
    if ((Current Predictability State = "NORMAL") and (Current Maneuverability State = "NORMAL")) then
        Current System Condition = "NORMAL"
    end if
    if ((Current Predictability State = "NORMAL") and (Current Maneuverability State = "CALM")) then
        Current System Condition = "NORMAL"
    end if
    if ((Current Predictability State = "CALM") and (Current Maneuverability State = "NORMAL")) then
        Current System Condition = "CALM"
    end if
    if ((Current Predictability State = "CALM") and (Current Maneuverability State = "CALM")) then
        Current System Condition = "CALM"
    end if
end if

if Current Stability State = "NORMAL" then
    if ((Current Predictability State = "UNACCEPTABLE") or (Current Maneuverability State =
"UNACCEPTABLE")) then
        Current System Condition = "ACCEPTABLE"
    end if
    if ((Current Predictability State = "ACCEPTABLE") or (Current Maneuverability State =
"ACCEPTABLE"))
and ((Current Predictability State<>"UNACCEPTABLE") and (Current Maneuverability
State<>"UNACCEPTABLE"))) then
        Current System Condition = "NORMAL"
    end if
    if ((Current Predictability State = "NORMAL") and (Current Maneuverability State = "NORMAL")) then
        Current System Condition = "CALM"
    end if
    if ((Current Predictability State = "NORMAL") and (Current Maneuverability State = "CALM")) then
        Current System Condition = "CALM"
    end if

```



```

end if

if ((Current Predictability State = "CALM") and (Current Maneuverability State = "NORMAL")) then
    Current System Condition = "CALM"
end if

if ((Current Predictability State = "CALM") and (Current Maneuverability State = "CALM")) then
    Current System Condition = "CALM"
end if

end if

if Current Stability State = "CALM" then
    if ((Current Predictability State = "UNACCEPTABLE") or (Current Maneuverability State =
"UNACCEPTABLE")) then
        Current System Condition = "NORMAL"
    end if

    if ((Current Predictability State = "ACCEPTABLE") or (Current Maneuverability State =
"ACCEPTABLE"))
and ((Current Predictability State<>"UNACCEPTABLE") and (Current Maneuverability
State<>"UNACCEPTABLE")) then
        Current System Condition = "CALM"
    end if

    if ((Current Predictability State = "NORMAL") and (Current Maneuverability State = "NORMAL")) then
        Current System Condition = "CALM"
    end if

    if ((Current Predictability State = "NORMAL") and (Current Maneuverability State = "CALM")) then
        Current System Condition = "CALM"
    end if

    if ((Current Predictability State = "CALM") and (Current Maneuverability State = "NORMAL")) then
        Current System Condition = "CALM"
    end if

    if ((Current Predictability State = "CALM") and (Current Maneuverability State = "CALM")) then
        Current System Condition = "CALM"
    end if
end if

if Previous System Condition = "CALM" then
    if Current System Condition = Previous System Condition then System Condition Trend =
"CONSTANT"
    if Current System Condition<>Previous System Condition then System Condition Trend =
"DETERIORATING"
end if

if Previous System Condition = "NORMAL" then
    if Current System Condition = Previous System Condition then System Condition Trend =
"CONSTANT"
    if Current System Condition = "CALM" then System Condition Trend = "IMPROVING"
    if Current System Condition = "ACCEPTABLE" then System Condition Trend = "DETERIORATING"
    if Current System Condition = "UNACCEPTABLE" then System Condition Trend = "DETERIORATING"
end if

if Previous System Condition = "ACCEPTABLE" then
    if Current System Condition = Previous System Condition then System Condition Trend =
"CONSTANT"
    if Current System Condition = "CALM" then System Condition Trend = "IMPROVING"
    if Current System Condition = "NORMAL" then System Condition Trend = "IMPROVING"
    if Current System Condition = "UNACCEPTABLE" then System Condition Trend = "DETERIORATING"
end if

if Previous System Condition = "UNACCEPTABLE" then
    if Current System Condition = Previous System Condition then System Condition Trend =
"CONSTANT"
    if Current System Condition<>Previous System Condition then System Condition Trend =
"IMPROVING"
end if

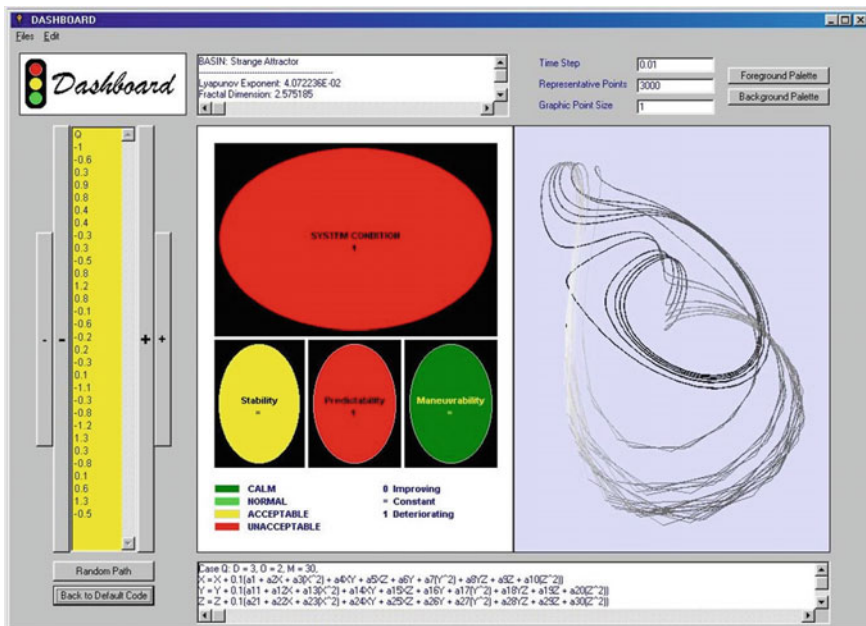
```

-----

The overall system condition would result to ‘calm,’ ‘normal,’ ‘acceptable,’ or ‘unacceptable,’ depending on the interplay of the factors described. A trend can also be identified, in consideration of the precedence in system’s conditions: ‘constant,’ ‘improving,’ or ‘deteriorating.’ The code offers one possible interface; we shall refer to the ‘dashboard’ to demonstrate the concept. Figure 2.4 depicts a standard view of the ‘dashboard’ with the left-hand side offering daily monitor of business system components. The right-hand side of the dashboard is for those who might be interested in the patterns behind the performance of the business system. Additional views are presented in Figs. 2.5, 2.6, and 2.7.

Several ‘illustrational’ scenarios were developed using this model. In these scenarios, different system conditions were developed and data used for random (uncorrelated) variation of the system model control parameters in the coupling (exchange) coefficients. Figures 2.8, 2.9, and 2.10 are the products of mockup runs. Figure 2.8 depicts a case for *increased predictability* by the narrowing of the occupied phase space—a consequence of uncorrelated variations in the system model’s control parameters. Notice that the resulting overall system condition is ‘normal.’

A case for increased *maneuverability* by the widening of the occupied phase space—a consequence of uncorrelated variations in the system model’s control parameters—is depicted in Fig. 2.9. Notice that the resulting overall system condition is ‘acceptable.’ Figure 2.10 depicts a case for an unacceptable *diminishing of*



**Fig. 2.4** A standard ‘Dashboard’ view indicating system conditions, adapted from Gheorghe and Vamanu (2006)

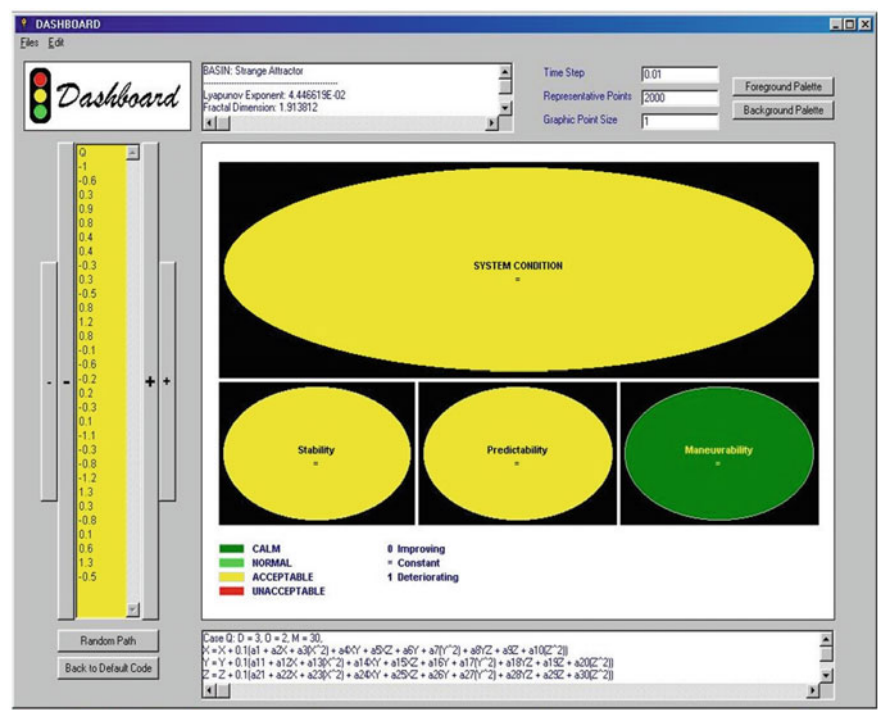


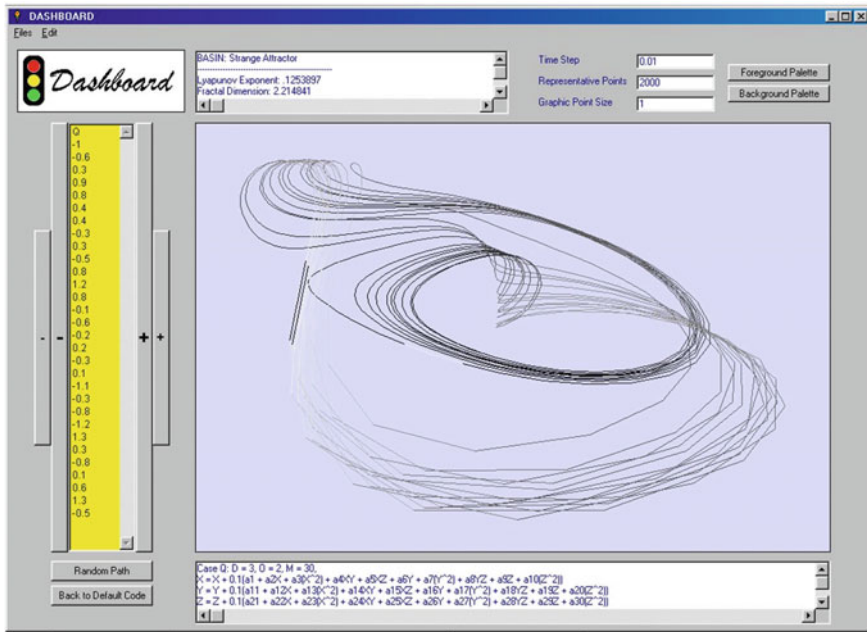
Fig. 2.5 ‘Dashboard’ indicating an ‘acceptable’ system condition, adapted from Gheorghe and Vamanu (2006)

the predictability by the excessive spread-out of the system state trajectory flow over the phase space—a consequence of uncorrelated variations in the system model’s control parameters. Notice that this results in an overall system condition of ‘unacceptable.’

It is only fair at this stage to recognize that the scaling of ‘system condition’ is subject to a considerable arbitrariness. The scaling of practical values must depend, extensively, on stakeholder perspective on the matter. The analyst can influence the auditing and numerical experiments; however, the stakeholders of the system should be the primary influencers. Furthermore, there might be a need to implement more refined notions and indicators of the chaos theory.

The concept of a ‘dashboard’ and the language used in this section are borrowed from the Basel Committee’s debate on business operational risks and vulnerability (Doerig 2000; Romeike and Maitz 2001). In particular, Doerig (2000, p. 74) suggests that the dashboard approach ‘is intended to provide senior management with a simple overview of operational risk levels and directional trends at the highest reporting aggregation level per business unit.’

The debate over the ‘dashboard’ approach to risk management has established several competing methods with varying degrees of complexity, sophistication, and feasibility operational risk evaluation in the banking sector. These methods include



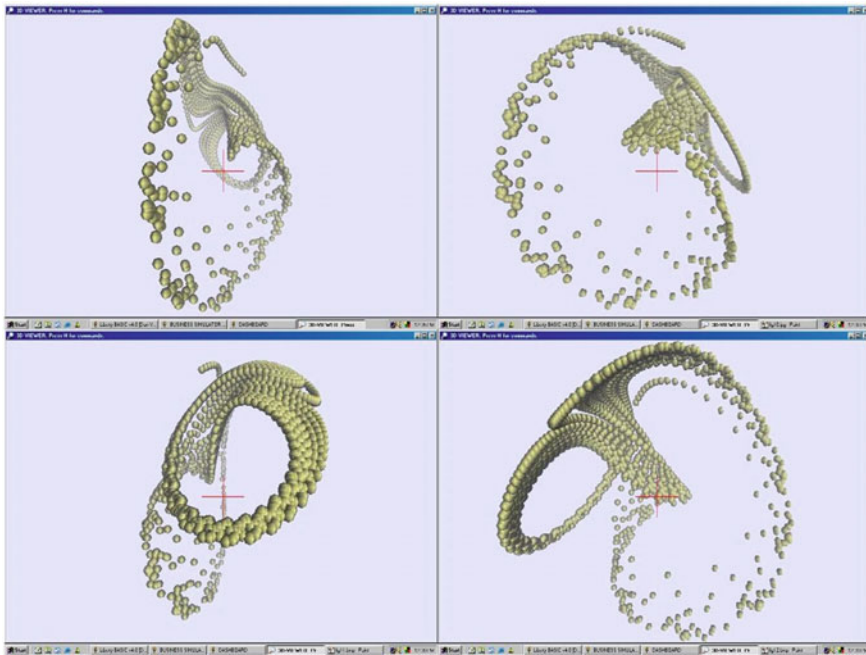
**Fig. 2.6** Element of the ‘Dashboard’ indicating patterns of the business system, adapted from Gheorghe and Vamanu (2006)

‘Basic Indicator Approach,’ ‘Standardised Approach,’ ‘Internal Measurement Approach,’ and ‘Loss Distribution Approach’ (Doerig 2000; Romeike and Maitz 2001). Certainly, there is still room for complementary approaches offering insights into assessment, new and emerging risks and vulnerabilities.

Subsequently, we suggest that approach suggested in this section’s series of demonstrations could be used to investigate the ‘motions’ or exchanges in business structures and components to unveil intelligible structure(s) in the motion itself.

### 2.2.3 Managerial Vulnerability and Consensual Analytical Hierarchies

There are several methods associated with describing vulnerability (Nilsson et al. 2001) including *Index Method* as suggested in Vamanu et al. (2016). However, such methods do not appear to offer a complete picture of on local authority’s actual risk level or ability to manage the risks—the municipal vulnerability/robustness. In this section, an attempt is made, therefore, to design a method that could be used to comprehensively do vulnerability analysis at a municipal level and yet easily updated to account for changes that might occur. To this end, we suggest the following advantages for this method:

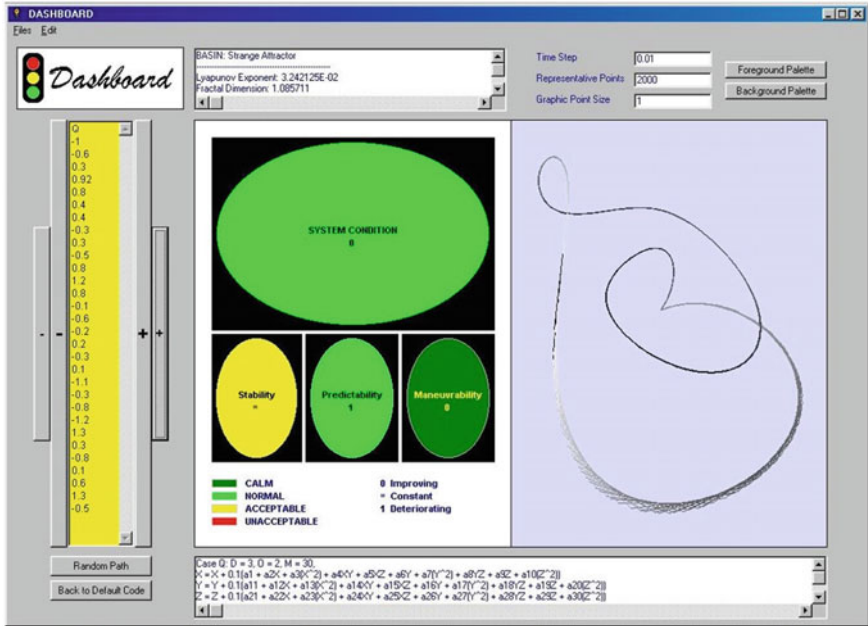


**Fig. 2.7** Depicting system's phase space pattern as seen in 3D fashion, from four viewing angles, adapted from Gheorghe and Vamanu (2006)

- It gives a chance for assessing the individual local authority's ability to manage the current risks.
- The vulnerability/robustness can be assessed as a result of generally defined acceptance criteria. These are determined as an upper and lower limit. The result of this is vulnerability is divided up into three areas: one area where vulnerability is unacceptable, another where vulnerability can be tolerated, if all the financially possible efforts have been fulfilled, and a third where vulnerability is generally acceptable. Figure 2.11 depicts these areas.
- The provided vulnerability model could also be used as a basis for distributing financial means to the local municipal authorities.

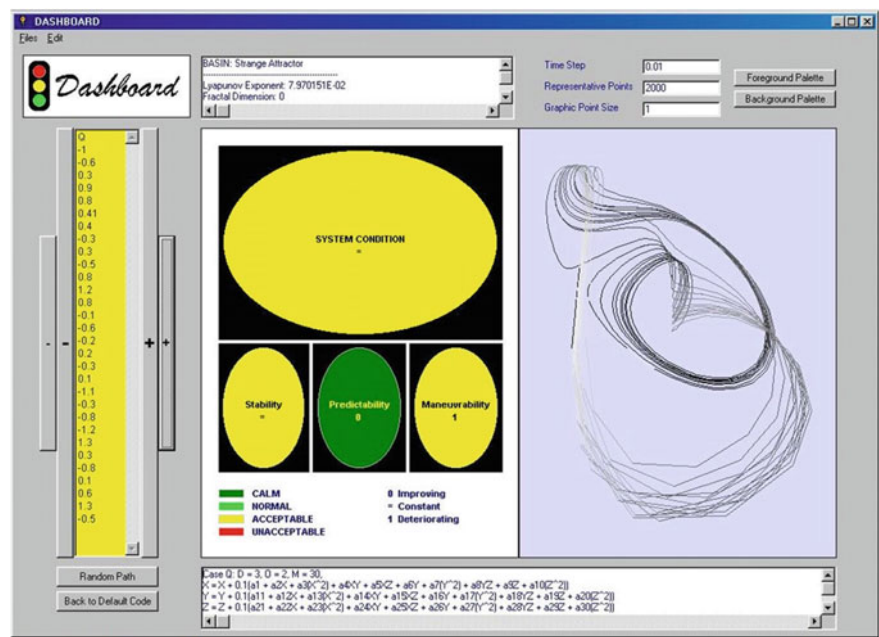
We now describe the main parts of the model. There are five main parts to this model:

- (I) The definition of current hazards and damage types. This model uses five different damage types: loss of life, damage to person, absence owing to illness, damage to the ecological system, and damage to property. Notice that these damage types are offered here randomly. Interestingly, several other damage types can be used including those associated with psychological trauma—a type of damage to the mind that occurs because of a severely distressing event. It should be evident that further work is required in this area to choose as damage types as well as possible consequences.



**Fig. 2.8** A ‘normal’ system condition despite ‘deteriorating’ phase space, adapted from Gheorghe and Vamanu (2006)

- (II) Damage and probability are divided up into four classes with the Swiss system as role model with index values of 1, 2, 4, and 4 with 1 corresponding to least harmful and 4 being the most dangerous.
- (III) A systematic risk inventory is carried out for all examined municipal hazards, natural and malicious, which are given an index value, on a scale of 1–4, for each type of damage types as well as probability.
- (IV) For all hazards, the existing damage indexes are multiplied by the probability index. The product of the damage index and probability index is summed up over relevant damage types (least 1, maximum 5). The sum is named  $Z_i$ . The maximum value of  $Z_i$  for specific hazard can be, for example, 80. This value can be obtained from a damage class 4, a probability class 4, and 5 damage types. The individual values for  $Z_i$  give the municipal danger profile; the sum of  $Z_i$ , gives a measurement of the collective risks and corresponds to the local authority’s risk value.
- (V) An inventory is made of the resources for risk management. For each defined hazard (danger), the capability to manage the risk is described using two coefficients:  $\alpha_i$  and  $\beta_i$  where index  $i$  describes the actual hazard. The value of  $\alpha_i$  and  $\beta_i$  can for each of them amount to 1, but the total value can never be more than 1 (perfectly managed hazard).



**Fig. 2.9** An ‘acceptable’ system condition despite ‘deteriorating’ maneuverability phase space, adapted from Gheorghe and Vamanu (2006)

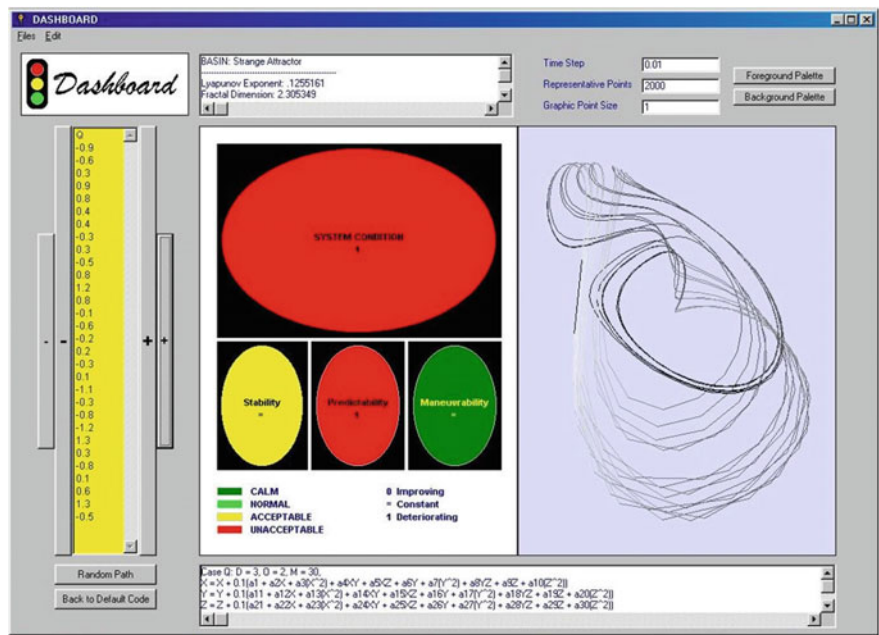
**2.2.3.1 Deriving  $\alpha_i$**

$\alpha_i$  describes the general hazard-independent ability to eliminate risks, counteract losses, intrusion, and damage as well as limit damage consequences. The checklists suggested in Lagbo-Bergqvist and Lexén (2000) could be used as a guide for setting value of  $\alpha_i$ . In practice, the task is to set a value for the municipality for each of the five parameters: loss of life, damage to person, absence owing to illness, damage to ecological system, and damage to property (see Tables 2.4, 2.5, and 2.6), summing it up and finally normalizing. A structured method is used throughout this process based on multiple-criteria decision analysis (MCDA) method to derive  $\alpha_i$  values.

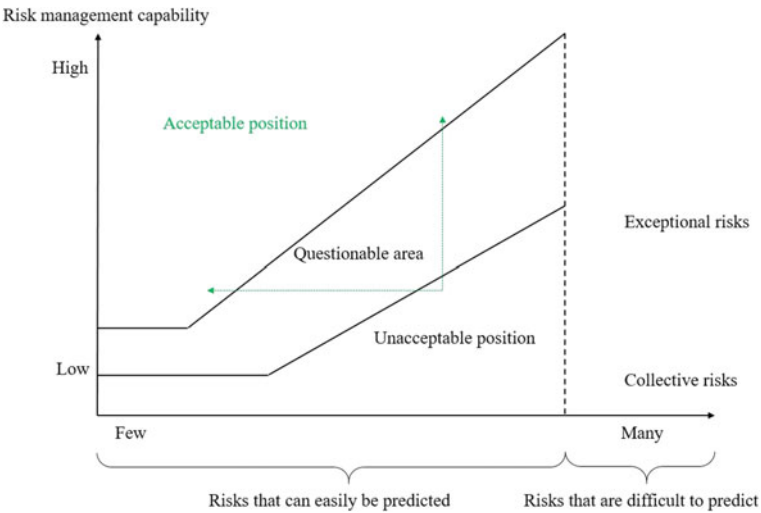
**2.2.3.2 Deriving  $\beta_i$**

$\beta_i$  offers the states for specified hazard  $i$ , such as a factory plant, natural disaster (e.g., flooding), or level of the resources (actions) directly linked to this hazard. In this case, a hazard is taken as a ‘danger.’ Once again, this assessment can be made with the help of existing checklists for technical, administrative safety control, competing gaming, and techniques in modeling and simulation, among others. Each one of these actions must be specific of the hazard and, thus, not included in the calculation of the corresponding  $\alpha_i$  value.





**Fig. 2.10** An ‘unacceptable’ system condition with ‘deteriorating’ predictability phase space, adapted from Gheorghe and Vamanu (2006)



**Fig. 2.11** Illustration of vulnerability of municipality as well overall risks and risk management ability



**Table 2.4** A classification of accidents affecting the population

Class	Lives	Personal injuries	Personal injury days
1	1–3	1–5	1–999
2	4–10	6–20	1000–49,000
3	11–50	21–100	50,000–499,000
4	>50	>100	>500,000

**Table 2.5** A classification of damages to the ecological system

Class	Ecological system (km <sup>2</sup> )
1	0–0.1
2	0.1–1
3	1–10
4	>10

**Table 2.6** A classification of damages to property

Class	Consequence (Mkr)
1	<1
2	<50
3	<500
4	>500

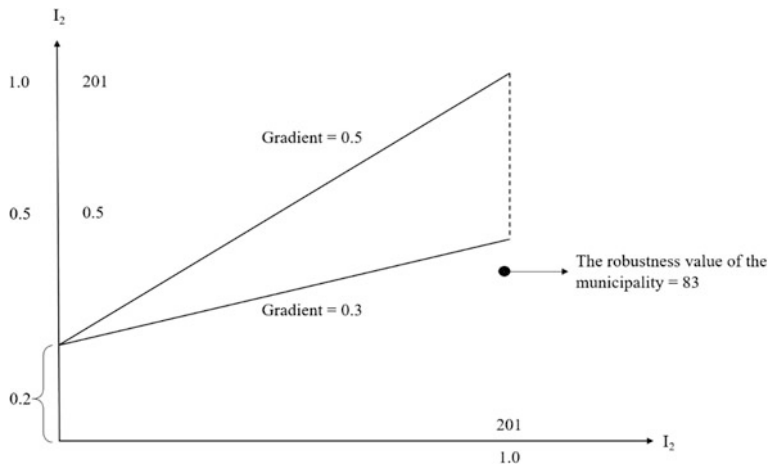
When determining values of  $\alpha_i$  and  $\beta_i$ , such things as existing safety cultures must be evaluated and quantified (e.g., see Warren 2015). A safety control must be carried out partly in the administrative situation and partly from a systematic point of view. Within both areas, methods have been developed for safety control. For example, safety, health, and the environment (SHE) model offers a checklist consisting of 145 points assessed and placed on a scale from 0 to 10 approach (Kemikontoret 1996). Another is Katina's 'pathological' issues, a total of 83, that could hinder organizational performance (Katina 2015a, b). Such models can function as a basis for assessing  $\alpha_i$  and  $\beta_i$ , but presumably continued development work is required to select suitable points that are most practical for use on a regular basis.

VI. Presentation of the result. In this phase, the results are presented based on the including criteria for acceptable vulnerability.

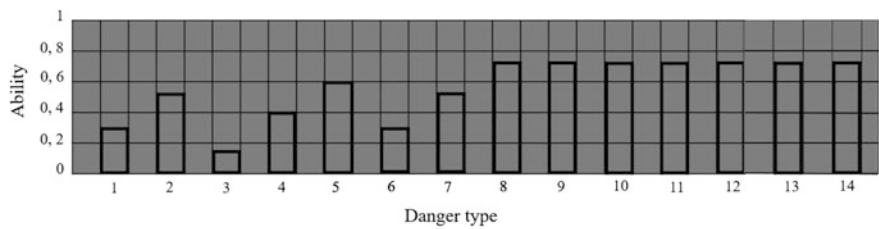
An example of the application of the presented model is discussed in the following section, discussing a fictitious municipality's vulnerability inventory. The municipality has 14 hazards of importance. The result is 14  $Z_i$  values ( $0.0 < Z_i < 80$ ) and 14 values of  $\alpha_i$  and  $\beta_i$  (for the sake of simplicity,  $\alpha_i$  and  $\beta_i$  would not amount to more than 0, 5; that is  $0.0 \leq \alpha_i, \beta_i \leq 0.5$ ).

First, we can conclude the following:

- If we draw profiles with the 14 values for  $Z$ ,  $\alpha_i$ , and  $\beta_i$ , respectively, we obtain the municipality's risk profile stating if and where efforts should be taken (see Fig. 2.13).



**Fig. 2.12** Value of the individual municipality vulnerability management in relation to acceptance criteria



**Fig. 2.13** An indication of how far the general and object-specific risk management resources stretch to deal with different risks

- If we sum up the 14  $Z$  values, we get the collective risk value of the municipality (see Table 2.9).

Three indexes are defined with the following values for the investigated local authority:

- $I_1$  = Maximum possible danger level ( $Z_{\max}$ ) =  $14 \times 80 = 1120$
- $I_2$  = Current risk level  $\sum_1^{14} Z_i = 201$
- $I_3$  = Current vulnerability management capability level  $\sum_1^{14} (\alpha_i + \beta_i) Z_i = 83$

The quotient  $I_2/I_1$  gives the relative threat level with the given hazards that have been discovered in the inventory. Of greater interest is the quotient  $I_3/I_2$  that is a direct measurement of how well the local authority manages its vulnerability situation. The nearer to the value of 1, the more robust and resilient a municipality is considered. The value of 1 equals to completely robustness. Acceptance criteria can be directly used against this quotient as a municipality independent means of

measurement, and the quotient  $I_3/I_2$  thus becomes an important measurement of the local authority's vulnerability in relation to other local authorities and relative to a given nationwide value.

An alternative way of using the calculated indexes is illustrated in Fig. 2.12 which also illustrates a method of defining a more general applicable acceptance criterion. Horizontal and vertical axes are graded from 0 to 1.0 where 1.0 is equal to the value of the index  $I_2$  (=201). A *lower acceptance curve*, could, for example, be stated with the starting point 0.2 on the y-axis and with a slope = 0.3. An *upper acceptance curve* could be given with the same starting point but with the slope = 0.5. If the local authority's  $I_3$  value (the level of the current capability to manage its vulnerability) comes under the lower limit curve, the result would not be acceptable. If  $I_3$  comes over the upper limit curve, the state of the system would certainly be acceptable. An  $I_3$  value between the curves indicates that an improvement, built on an analysis of cost *efficiency*, must be carried out.

The following notes apply:

- **Note 1:** The starting point on the y-axis of 0.2 is motivated by the fact that there is always a certain level of risk management, irrespective of the size and number of hazards.
- **Note 2:** By considering an individual local authority and using the relative values of  $I_2$  and  $I_3$ , we will always be on the line  $I_2 = 1$ .

In the present approach, it is quite fine to do away with the relative values by only using the absolute values. In this case, the numbers provided by local authorities can be used. Also, one should differentiate the diagrams based on the classification stipulated by the Swedish Association of Local Authorities (Kemikontoret 1996); otherwise, the solution of the figure could return as 'not acceptable.' The method could be sorted in under all application classes 1, 2, 3, and 4, of the Swiss system, concerning their areas of use.

### 2.2.3.3 Model Application: Calculating Vulnerability Management Capability Index

The following is an example indicating how an index for vulnerability management capability is calculated for a fictive local authority.

#### *Step 1: Definition of hazard and damage types*

In this case, the hazard types of concern involve:

- Threats against municipal services
- Natural catastrophes
- §43 factory buildings
- Hazards associated with information technology safety are excluded.

The following damage types are considered:

- Population—divided into three separate damage types (see Table 2.4)
- Ecological systems (see Table 2.5)
- Property (see Table 2.6).

*Step 2: Classification of damage types and probability*

Undoubtedly, population can be affected in terms of death and personal injury. Time can also be an important factor when dealing with injury, especially the size of an injury. The effects can be, for example, measured in terms of number of days a person is affected (i.e., personal injury days). Table 2.4 is an attempt to classify accidents into different classes. It should be noted that exactly how such a classification should be made is not clear at this stage. However, authors can speculate that such classification could vary from system to system and from nation to nation. In effect, the context of operation could affect this classification.

An important step, when defining a risk, is to determine the likelihood (i.e., probability) of occurrence of the risk event. In this case, Table 2.7 demonstrates a classification of the probability associated with the damage types.

*Step 3: Inventory of hazards*

From this classification, we gain the following values associated with the municipality in question:

(A) *Provision systems (water, electricity, sewage)*

A vulnerability analysis of the municipal service systems means that indexes for the different damage types and probability are given values (Table 2.8) as stated below:

The three Z values for risk are:  $Z_1 = 20$ ,  $Z_2 = 28$ , and  $Z_3 = 30$ . The total of 78 is placed in relation to theoretically possible maximum value of 240.

(B) *Natural disasters (severe)*

We consider a municipality with several severe natural risk events, including blizzards, flooding, landslides, and forest fires.

For blizzards

Personal days (off work) index = 3, property damage index = 2, probability class index = 3,  $Z_i$  value =  $(3 + 2) \times 3 = 15$

For flooding

Personal days (off work) index = 3, ecological system index = 3, property damage index = 4, probability class; index = 4,  $Z_i$  value =  $(3 + 3 + 4) \times 4 = 40$

**Table 2.7** Probability classes for the above damage type

Class	Probability $P$ /year
1	$P < 10^{-3}$ /year
2	$10^{-3}$ /year $< P < 10^{-2}$ /year
3	$10^{-2}$ /year $< P < 10^{-1}$ /year
4	$P > 10^{-1}$ /year

**Table 2.8** Index and probability for different municipal service systems

Damage type	Municipal services systems		
	Water	Electricity	Sewage
Lives	0	0	0
Injured	3	4	4
Personal injury days	1	3	3
Property	1	0	3
Environment	5	7	10
Probability class	4	0.4	0.3
Total	20	28	30

**Table 2.9** Calculation of municipal vulnerability management capability (robustness)

Hazard types	Risk value, $Z$	$\alpha$	$\beta$	$\sum (\alpha + \beta)$	Vulnerability management capability (robustness) = $\sum (\alpha + \beta) \times \text{risk value}$
Water	20	0.1	0.2	0.3	6
Electricity	28	0.2	0.3	0.5	14
Sewage	38	0.1	0.1	0.2	6
Snow	15	0.1	0.3	0.4	6
Flooding	40	0.1	0.5	0.6	24
Landslide	18	0.1	0.2	0.3	5
Forestry	14	0.2	0.3	0.5	7

*§43-object*

$N_1$	4	0.1	0.3	0.4	=15 for all the objects in total
$N_2$	3	0.1	0.3	0.4	
$N_3$	8	0.1	0.3	0.4	
$N_4$	2	0.1	0.3	0.4	
$N_5$	5	0.1	0.3	0.4	
$N_6$	7	0.1	0.3	0.4	
$N_7$	7	0.1	0.3	0.4	
	$\sum = 201$				$\sum = 83$

#### For landslides

Index for personal days (off work) index = 2, ecological system index = 2, property damage index = 2, probability index = 3,  $Z_i$  value  $(2 + 2+2) \times 3 = 18$

#### For forest fires

Index for personal days (off work) index = 1, ecological system index = 3, property damage index = 3, probability index = 2,  $Z_i$  value  $= (1 + 3 + 3) \times 2 = 14$

#### (C) *Industry (including public buildings) and other 43 industrial buildings*

We assume that there are seven industrial buildings and that each building has a probability index of 1 meaning that severe accident happens no more than once in every 1000 years in each of the industrial buildings.

Further, we assume an aggregate scale index 0, 4, 3, 8, 2, 5, 7, 7 for the seven industrial buildings. The total  $Z$  value will be 36. Thus, the value of 36 is to be compared to a theoretical maximum value of 560.

*Step 4: Inventory of resources for risk management*

It is possible to divide up risk management resources, in a local municipal authority, into two parts: First are those that can be considered general in a local authority,  $\alpha_i$ , and second are those that are linked to the individual object or phenomenon,  $\beta_i$ , including the 43 industrial buildings. How though do we determine  $\alpha_i$ , and  $\beta_i$ ? First, we assume that the maximum number of resources needed to deal with the risk level amounts to value of 1. After that, for the sake of simplicity, we divide the resources at random into two similar parts, giving an interval within which it is possible, for a local authority, to find general and object-specific resources.

Therefore, we can assume that:

- For general risk management capability,  $0.0 < \alpha_i < 0.5$ , and
- For object-linked or the phenomenon linked to the risk management capability,  $0.0 < \beta_i < 0.5$

In Table 2.9, the assumed values of  $\alpha_i$  and  $\beta_i$  are used. By adding these to each other, we gain the total number of resources (maximum 1) that exist in a local authority. If this percentage value is multiplied by the risk value for the different threat types, a new value is gained which states the level of robustness regarding the risk level.

For each hazard (danger type), the value of the vulnerability management capability (robustness) can be placed against a corresponding risk value. This is done to show the capability of the municipality stack-up against a given risk in a specific area. An example of this ‘stackness’ is provided in Fig. 2.13. For example, one can conclude that municipal ability to deal with danger type 5 is only at 0.6.

In Table 2.8, we obtain vulnerability management capability value of 83 by adding items on the most right-hand column. It is now possible to summarize the result of the calculations already done as three individual indexes:

- The maximum possible danger or threat level; total maximum sum of the earlier part steps in *Step 2* = 1080 =  $I_1$
- The current risk level = 201 =  $I_2$
- The current vulnerability management capability level = 83 =  $I_3$

The different indices can be presented in two ways:

1. Relative diagram to determine acceptance. It must be drawn for each municipality individually.
2. Absolute values  $I_2$ ,  $I_3$ , and  $I_3/I_2$  which can apply for a whole nation.

The acceptance criteria, in accordance with point 1 above, are illustrated in the diagram above. The lower acceptance line starts in  $(0.2 \times 201) = 40.2$  and ends

$40 + (0.3 \times 201) = 100.5$  and the upper acceptance line ends in  $40 + (0.5 \times 201) = 140.5$ . The variables consist of starting point and gradient on the lower and upper line. The starting point is determined by defining a baseline for basic services (e.g., all local authorities must have a security coordinator). The exact gradient lines for municipal authorities are determined through several large-scale calibrating studies.

This section offers an approach to assessing local authority's ability to manage risk events using a measure of vulnerability capability that involves lower and upper acceptance curves. The presented model defines hazards and damage types, probabilities associated with such hazards, and the available resources that can be used to deal with such threats. Authors submit that the model offers utility at a local level as well as the national level and can be used in connection with different risks and well as known checklists.

### 2.2.4 *Relational Vulnerability and System Penetrability*

The topic of assessing the vulnerability in critical infrastructures is becoming extremely important, under the stringent needs for protecting them against malicious, technical, and natural disasters. A few attempts have been made to give an adequate working framework to the concept of vulnerability. However, these efforts do not fully reflect the stringent needs to quantify the vulnerability and then offer systematic steps for (1) an agreed upon criteria for vulnerability acceptance—the framing of this issue should get you to realize that is no such a thing as systems free of vulnerability—and (2) vulnerability economics, implying the fact that vulnerability of systems could decrease by allocating resources at different stages of system evolution. What is suggested in this section is considering vulnerability assessment of critical infrastructures by addressing the aspect of their *complexity*. In defining and measuring complexity of such systems, the concept of graphs is needed and used. In this case, the vulnerability, referring to nature of the system itself, is seen as the capacity of a system made of people, hardware, software, organizational, and management procedures being *penetrated*. The degree of vulnerability is then supported by the capability of the system performing its designed functions.

This section addresses a special line of thought, setting the task of *taking a straightforward approach to complexity as a source of vulnerability*. The practical goal is to attach a relevant metric to the internal connectivity of multi-component systems so that this is turned to account from a quantitative vulnerability assessment (QVA) oriented standpoint.

#### 2.2.4.1 **Models of Relational Vulnerability**

Since the promotion of the concept—complexity-induced vulnerability—requires a versatile *modus operandi*, able to accommodate a variety of user-defined, convincing applications, a generic model was sought. The reference in hand were the

graphs, as a comprehensive expression of multi-component systems and their internal connectivity—*ergo*, ‘complexity,’ in the parochial sense adopted. There are several assumptions associated with models in question starting with assumption zero:

*Assumption 0: The operational representation of a multi-component system is a graph.*

Here is the spelt-out equivalence. The members (i.e., constituents, parts) of the system are the graph’s **knots**. The interactions of the members are represented by directed knot **links**, and the graph is customized to a system by attaching to knots a set of **features**, appropriately quantified and normalized on a vulnerability-relevant scale. **Knots** are, generically, the irreducible components or ‘atoms’ of a system and are the subjects of the analysis. Depending on the nature of the targeted system, ‘knots’ may be employees, departments, subsidiaries, contractors, parts in an engineered machinery, circuitry, plant, member-states of an alliance, etc., *or collections of these*, showing a sufficient degree of coherence to play a coordinated part in the overall system’s internal interaction game.

**Links** connect knots such that exchange/trade information, energy, and/or substance are possible. In effect, links define a system by way of its exchange boundaries. Links enter the model by *Connection Lists* attached to each knot in the graph of the system in question. Normally, exchanges between knots proceed under an authority rule, or otherwise said—in hierarchic fashions. That is why links are *directed*, so that, in the sense of the model, knot A may have knot B on its connection list, while knot B may not necessarily have knot A on its connection list. Links are of critical importance in evaluating, among others, the security efficiency, efficacy, and sustainability of the system.

**Features** are meant to characterize the knots. Depending on what the ‘knot’ is (i.e., employees, departments, subsidiaries, contractors, parts in an engineered machinery, etc.), ‘features’ should be selected providing maximum relevance concerning the objective of the analysis (e.g., security, efficiency, efficacy, etc.). In the current model, ‘features’ enter the quantitative vulnerability assessment through *values* and *weights*. The feature ‘values’ are attached to the system ‘knots’ and provided as a decimal number in the range 1 through 9. It is assumed to be in direct proportion to the degree of *vulnerability relevance* that the feature may attain for different knots. In a way of a random example, in an embassy, within feature ‘position,’ a desk clerk might be given a value of 3 compared to a value of 9 that could be given to a cipher officer. Contrastingly, feature ‘weights’ compares features in terms of their *relative* vulnerability relevance such that feature ‘*Clearance*’ is more vulnerability relevant than feature ‘*Qualification*.’ Weights are entered by the user as arbitrary numbers and are eventually normalized by the code over a span of 0.0 to 1.0. In this case, the ‘weights’ are meant to discriminate among ‘features’ placing these in perspective as far as *importance* and play their part in quantitative evaluations involving the ‘knots’ and their ‘features.’ The model and its algorithms have been implemented in a software tool, DOMINO, as part of a decision support system. Four screenshots of DOMINO are presented in Fig. 2.14 for a system with 100 knots and features.



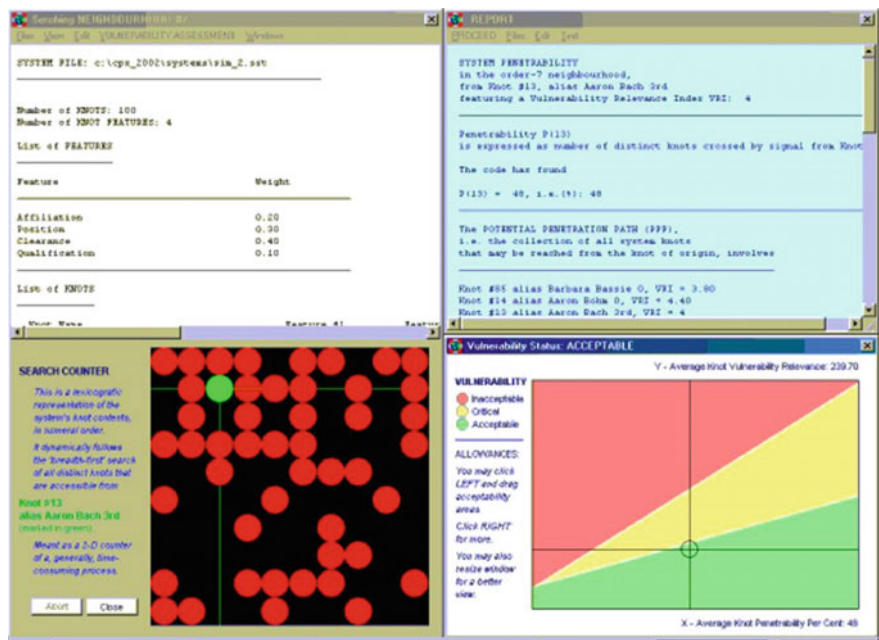


Fig. 2.14 DOMINO—DSS features for complexity vulnerability assessment, adapted from Gheorghe and Vamanu (2004a)

2.2.4.2 Connectivity as Penetrability

There are, basically, two possible interpretations of the meaning of internal connectivity. These meanings are not contradictory, rather complementary and in fact intertwined. One is a *benign*, while the other is *cautious* interpretation. As per the benign interpretation, the more extensive and multi-lateral the exchanges among system parts or constituents, the better. In this instance, the system is considered ‘functional,’ ‘lively,’ ‘active,’ and ‘dynamic’—terms often associated with the promise of high productivity, efficacy, alert response to inputs, and high profits. Complementarity to this view is the perspective of looking for lack of connectivity which would reveal chances of inherent defects in the systems (e.g., a short circuit in the control room of a nuclear power plant), an accidental instruction (i.e., a static discharge in a highly relevant computer circuitry), or a foul play (i.e., a fatal virus dropped in a company database), and which could be initiated at one specific knot in the system and having a higher chances to propagating throughout the system, thus having the potential to impair larger system segments. In this interpretation, a higher connectivity rhymes with a higher vulnerability. All epistemological (e.g., see Fernandez 2009; Flood and Carson 1993) and ethical debate left aside, this research exercise will try and reconcile the two stands, which would generate the operational assumptions as indicated in Table 2.10.

**Table 2.10** Operational assumptions for connectivity as penetrability

Assumptions	Description	Implications
Assumption 1	A higher internal connectivity in a system is a desirable quality only to the extent that the cumulated vulnerability relevance of the connected knots is tolerable	This allegation expresses the fact that not all ‘knots’ (i.e., system constituents have the same vulnerability relevance. The involvement in exchanges—of information, energy, substance of <i>some</i> —could be more meaningful and attention-catching, than others. When assumption I is considered, it produces the following consolidating findings
Assumption 2	The higher the vulnerability relevance of the knots involved in the exchange path of any knot of origin, including the relevance of the knot of origin itself, the higher the vulnerability induced in the overall system by the respective knot of origin	
Assumption 3	The higher the cumulated vulnerability relevance of the system’s knots, the higher the system vulnerability itself	

Upon a consideration of these assumptions, one might be attempted to characterize a system vulnerability in terms of its ‘complexity.’ To this end, we suggest two distinct, if not completely independent, parameters: (a) system’s penetrability and (b) connectivity’s vulnerability relevance. System’s penetrability is a quality that may have metrics such as the number (e.g., average number) of knots that can be accessed starting from a (any) given knot in the system. Connectivity’s vulnerability relevance depends on penetrability as defined above along with vulnerability relevance grades as assigned to knot features. In an  $X$ – $Y$  plane underlined by these parameters, one may conduct a meaningful appraisal of ‘*vulnerability tolerance*,’ as a means of understanding and recognizing that vulnerability of a part of life, be it functional or structural, and that it can be inherent, has unavoidable drawbacks, or otherwise limitation, of all *negentropic* systems.

#### 2.2.4.3 Quantifying Vulnerability Relevance of Penetrability

With this said, one must recall that the objective function of the investigation may easily be written. Let’s consider:

$N_k$  be the number of knots,  $K_i$ ,  $i = 1, 2, \dots, N_k$ , in the graph  $\mathbf{G}$  representing a multi-component system,

$N_f$  be the number of vulnerability-relevant knot features  $F_j, j = 1, 2, \dots, N_f$ ,  
 $W(F_j)$  be the weights of the features  $F_j, j = 1, 2, \dots, N_f$ , where

$$0 \leq W(F_j) \leq 1 \quad (2.25)$$

$G(F_j, K_i)$  be the value (grade) of the feature  $F_j$  of knot  $K_i$ , where

$$1 \leq G(F_j, K_i) \leq 9 \quad (2.26)$$

Then, one has:

The individual vulnerability relevance,  $V_k(K_i)$ , of knot  $K_i$ :

$$V_k(K_i) = \sum_{j=1}^{N_f} W(F_j) \cdot G(F_j, K_i) \quad (2.27)$$

- (a) The search-path (breadth-first) vulnerability relevance,  $V_p(K_i)$ , of knot  $K_i$  and all the knots that can be accessed either directly or via other knots, into the system (index 'p' for 'path'):

$$V_p(K_i) = V_k(K_i) + \sum_{m=1}^{N_j} 'V_k(K_m) \quad (2.28)$$

with  $V_k(\cdot)$  given by Eq. (2.27). The sign ' in Eq. (2.28) emphasizes the limitation of the sum to only those knots that can be, directly or indirectly, accessed starting from knot  $K_i$ .

- (b) The maximum possible vulnerability relevance of a system's knot:

$$V_{\max} = \max(V_k(K_i)) \cdot N_k = 9 \times SW(F_j) \cdot N_k = 9 \times 1 \times N_k \quad (2.29)$$

obtained in consideration of expressions (2.25), (2.26), and Eqs. (2.27), (2.28).

- (c) The average vulnerability relevance per knot of system:

$$V_{\text{avg}} = \left( \sum_{i=1}^{N_i} V_p(K_i) \right) / N_K \quad (2.30)$$

with  $V_p(\cdot)$  given by Eq. (2.28).

One may also define:

(d) The penetrability of the system from knot  $K_i$ :

$$P(K_i) = \text{number of distinct knots that can be accessed from } K_i, \quad (2.31)$$

both directly and via other knots, plus 1—the knot of origin

(e) The *Maximum System Penetrability*, obviously given by

$$P_{\max} = N_k \quad (2.32)$$

f. The *Average System Penetrability*, per knot, given by:

$$P_{\text{avg}} = \left( \sum_{i=1}^{N_i} p(K_i) \right) / N_K \quad (2.33)$$

At this point, it is possible to visualize the issue in hand, complexity-induced vulnerability as depicted in Fig. 2.15.

#### 2.2.4.4 Tolerability of Vulnerability

Since, as indicated, the only meaningful issue in QVA, quantitative vulnerability assessment, is ‘*How tolerable the vulnerability of this system is,*’ a discussion may be conducted:

(a) In the  $X$ – $Y$  plane featuring

$$\begin{aligned} X &= P(K_i) / P_{\max}, \\ Y &= V_p(K_i) / V_{\max}, \end{aligned} \quad (2.34)$$

with the quantities involved given by Eqs. (2.28), (2.29) and (2.31), (2.32), respectively, and

(b) In the  $X$ – $Y$  plane featuring

$$\begin{aligned} X &= P_{\text{avg}} / P_{\max}, \\ Y &= V_{\text{avg}} / V_{\max}, \end{aligned} \quad (2.35)$$

with the quantities involved given by Eqs. (2.30), (2.33) and (2.31), (2.32), respectively. While the approach (2.35) would indeed qualify a system’s connectivity (i.e., ‘complexity’), overall vulnerability relevance, the approach (2.34) has

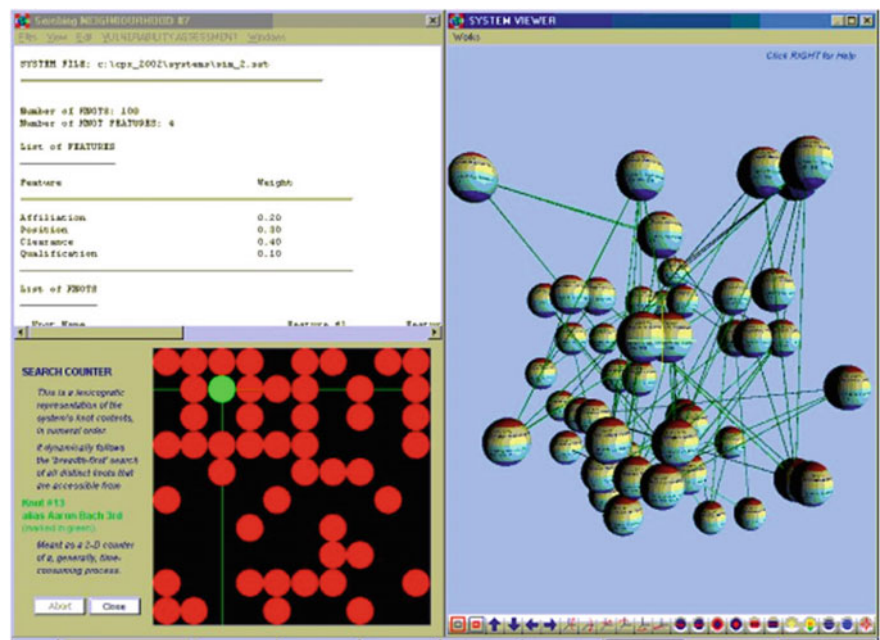


Fig. 2.15 Visualizing complexity-induced vulnerability by DOMINO software, adapted from Gheorghe and Vamanu (2004a)

also merits in signaling extremes, or ‘vulnerability spikes,’ originating in knots that would deserve special attentions. The  $X$ – $Y$  space, as defined above, is divided, generally, into three basins: (a) **acceptable vulnerability** basin, indicated by the green area; (b) **critical vulnerability** basin, indicated by the yellow area; and (c) **unacceptable vulnerability** basin, indicated by the red area.

The  $X$  and  $Y$  parameters are not to be taken as completely independent of each other, the configuration of the basins remains debatable, and, on this account, the code makes provisions enabling the user to interactively redefine the basins. The default configuration proposed by the code associated with this model *assumes an acceptable vulnerability at 0-penetrability*. Such a scheme may be termed as ‘over-confident.’ It reflects a ‘non-guilty-until-otherwise-proved’ presumption, or attitude, in the sense that each and every constituent of a system carries, by design, a ‘vulnerability relevance.’ However, there is an irrefutable reality that one cannot build a healthy system, company, circuit, alliance, etc., resting on the assumption that it is *bound* to be unsafe or malicious. The opposite attitude, assuming an unacceptable vulnerability, even at 0-penetrability, could be termed ‘paranoiac’ with, however, no derisive connotation. In-between, a ‘cautious’ or ‘conservative’ attitude may also be identified, assuming complete uncertainty on vulnerability at 0-penetrability, that is,  $Y = 0$  for  $X = 0$ .

User may position him/herself in respect of the above, by the mouse-driven action of shifting the basin divides. In DOMINO, both the initial left-hand-side gap

and the aperture of the ‘critical vulnerability’ area can be fine-tuned based on response to user’s beliefs. This type of analysis, however, introduces a requisite element of subjectivity (i.e., stakeholder perception of vulnerability) since it is possible to have a system in the basin of ‘acceptable’ vulnerability that might be in a ‘critical’ or even ‘unacceptable’ basin. Figure 2.16 depicts full information structure from DOMINO involving the three basins of vulnerability along with relevance to vulnerability assessment for each knot in a structure of interest.

2.2.4.5 Supplementary Model Resources

The evaluation of system vulnerability based on system’s internal connectivity, introduced in this chapter, relies heavily on statistical connotations. However, recall that the newcomers of SCI, UCI, and BCI, as well as the likes, might not have standing and readily available statistical data rooted in historical accounts. Certainly, this might be true when attempting to address emerging areas of research such as cybersecurity in cyber-physical systems, blockchain technology, algo- and robot techniques. This suggests a need for application of approaches that are non-statistical in nature: *scenario-based investigations*. A scenario-based investigation could provide insights; for example, at any moment in time, a system monitor may be interested in whether knot B could be reached by signals emitted at

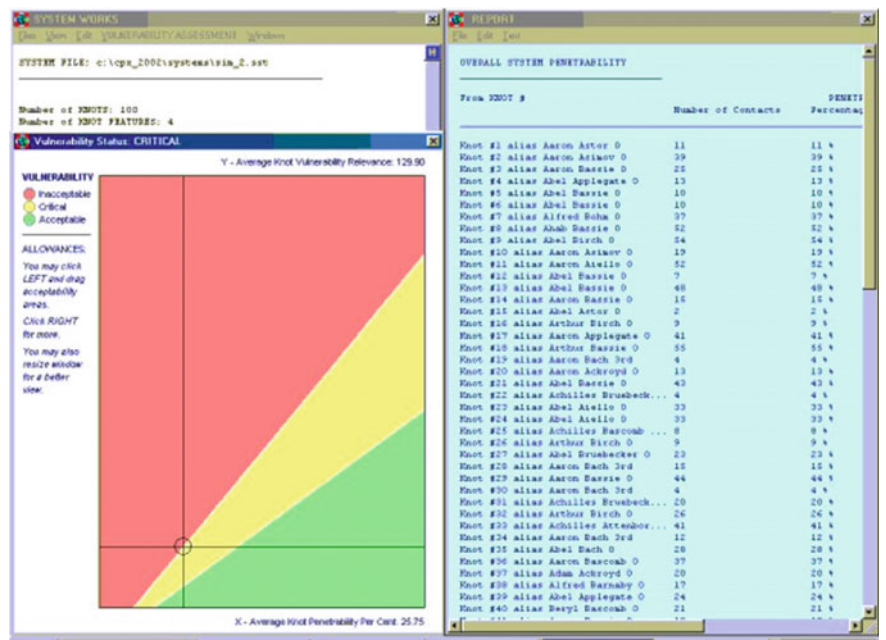


Fig. 2.16 An example of the three vulnerability basins along with knots along with system architecture, adapted from Gheorghe and Vamanu (2004a)

knot A. The *route* through which such a contact proceeds may also be relevant, as well as the *cumulated 'vulnerability relevance'* of all knots involved in the process.

*Normative, or ceiling, values* for the vulnerability relevance burden of every individual knot, of knot pairs, or groups of knots, may equally be contemplated within a vulnerability-conscious system management. Although the current model places emphasis on the *distinct* number of knots that can be reached from a given knot of origin, the *frequency* of the intermediate knots being visited by the signal started at origin, until it reaches the destination knot, may present importance, in a vulnerability, or foul play scenario, inquiry. DOMINO enables one to study such investigations. Future research expects to include other features that might be of interest to system monitors. A proposed and interesting area of research is system theory-based pathologies (Katina 2015a, b, 2016a, b; Keating and Katina 2012; Troncale 2013). A pathology is defined as a circumstance, condition, factor, or pattern that acts to limit system performance, or lessen system viability, such that the likelihood of a system achieving performance expectation is reduced (Keating and Katina 2012). Simply stated, these are *organizational diseases*. The current state of research has yielded over 80 systems theory-based pathologies classified in terms of dynamics of a system, system goals/missions, information flow, processes, regulation, resources, systemic structures, and understanding (Katina 2015b). Obviously, there remain questions of relating pathologies to vulnerability, levels of pathologies, how pathologies can affect a system (e.g., penetrability), and the economics of pathologies. Appendix E provides an in-depth classification of systems theory-based pathologies.

## 2.3 Remarks

In this chapter, a new metric for system vulnerability by considering their complexity, as a new and comprehensive measure, is introduced. The applicability of this model is rather generic, and it needs to be adapted to various applications in case. The model has been complemented by the design and implementation of a decision support system, named DOMINO, which exhibits various features related to the process of measuring and assessing the vulnerability of sociotechnical systems.

## References

- Christen, P., Bohnenblust, H., Seitz, S. (1995). How to compare harm to the population with damage of the environment? A quantitative multi-attribute approach for risk analysis based on fuzzy set theory. In J. J. Mewis, H. J. Pasman, E. E. De Rademaeker (Eds.), *Proceedings of the 8th international symposium* (pp. 691–704). Antwerp: Elsevier Science BV.
- Doerig, H.-U. (2000). *Operational risks in financial services: An old challenge in a new environment*. London: Institut international d'études bancaires.
- Fernandez, G. W. (2009). *Epistemological beliefs and teacher efficacy* (Ph.D.). University of Virginia, United States, Virginia.

- Flood, R. L., Carson, E. R. (1993). *Dealing with complexity: An introduction to the theory and application of systems science*. New York: Plenum Press.
- Gheorghe, A. V. (2004). *The hidden faults: Towards a standing method to assess Switzerland's vulnerabilities*. Zurich, Switzerland: Laboratory of Safety Analysis, ETH Zurich.
- Gheorghe, A. V., Vamanu, D. V. (2004a). Complexity induced vulnerability. *International Journal of Critical Infrastructures*, 1(1), 76–84.
- Gheorghe, A. V., Vamanu, D. V. (2004b). Towards QVA—Quantitative Vulnerability Assessment: A generic practical model. *Journal of Risk Research*, 7(6), 613–628.
- Gheorghe, A. V., Vamanu, D. V. (2006). Risks in business design for critical infrastructures: the “DASHBOARD” concept. *International Journal of Critical Infrastructures*, 2(1), 70–82.
- Katina, P. F. (2015a). Emerging systems theory-based pathologies for governance of complex systems. *International Journal of System of Systems Engineering*, 6(1/2), 144–159.
- Katina, P. F. (2015b). *Systems theory-based construct for identifying metasystem pathologies for complex system governance* (Ph.D.). Old Dominion University, United States, Virginia.
- Katina, P. F. (2016a). Metasystem pathologies (M-Path) method: Phases and procedures. *Journal of Management Development*, 35(10), 1287–1301. doi:[10.1108/JMD-02-2016-0024](https://doi.org/10.1108/JMD-02-2016-0024).
- Katina, P. F. (2016b). Systems theory as a foundation for discovery of pathologies for complex system problem formulation. In A. J. Masys (Ed.), *Applications of Systems Thinking and Soft Operations Research in Managing Complexity* (pp. 227–267). Geneva, Switzerland: Springer International Publishing.
- Katina, P. F., Pinto, C. A., Bradley, J. M., Hester, P. T. (2014). Interdependency-induced risk with applications to healthcare. *International Journal of Critical Infrastructure Protection*, 7(1), 12–26.
- Katina, P. F., Unal, R. (2015). Application of fuzzy sets in decision analysis for prioritising critical energy infrastructures. *International Journal of Decision Sciences, Risk and Management*, 6(1), 1–15.
- Keating, C. B., Katina, P. F. (2012). Prevalence of pathologies in systems of systems. *International Journal of System of Systems Engineering*, 3(3/4), 243–267. doi:[10.1504/IJSSE.2012.052688](https://doi.org/10.1504/IJSSE.2012.052688).
- Kemikontoret, (1996). *Administrativ SHM—revision*. Stockholm: Association of Swedish Chemical Industries.
- Lagbo-Bergqvist, E., Lexén, R. (2000). *Vägen till bättre styrning av säkerhetsarbetet i kommuner och landsting*. Stockholm: Svenska kommunförbundet Landstingsförbundet.
- Merriam-Webster. (2006). *Webster's new explorer encyclopedic dictionary*. Springfield, MA: Federal Street Press.
- Nilsson, J., Magnusson, S., Hallin, P., Lenntorp, B. (2001). *Models for vulnerability auditing and distribution of governmental economical means at the local authority level*. Lund, Sweden: LUCRAM: Lund University Centre for Risk Analysis and Management.
- Romeike, F., Maitz, J. (2001). *Operational risk*. London: CSC Financial Services EMEA.
- Skyttner, L. (2005). *General systems theory: Problems, perspectives, practice* (2nd ed.). Singapore: World Scientific Publishing Co., Pte. Ltd.
- Thom, R. (1975). *Structural stability and morphogenesis*. Reading, MA: Westview Press.
- Thom, R. (1983). *Mathematical models of morphogenesis*. (W. M. Brooks, D. Rand, Trans.). New York: Halsted Press.
- Troncale, L. (2013). Systems processes and pathologies: Creating an integrated framework for systems science. *INCOSE International Symposium*, 23(1), 1330–1353.



- Vamanu, B. I., Gheorghe, A. V., Katina, P. F. (2016). *Critical infrastructures: Risk and vulnerability assessment in transportation of dangerous goods—transportation by road and rail* (Vol. 31). Cham, Switzerland: Springer International Publishing.
- Warren, J. H. (2015). *Safety culture monitoring: A management approach for assessing nuclear safety culture health performance utilizing multiple-criteria decision analysis* (Ph.D.). Old Dominion University, United States, Virginia.
- Zeeman, E. C. (1977). *Catastrophe theory: Selected papers*. London: Addison-Wesley.

Critical Infrastructures, Key Resources, Key Assets  
Risk, Vulnerability, Resilience, Fragility, and Perception  
Governance

Gheorghe, A.; Vamanu, D.V.; Katina, P.; Pulfer, R.  
2018, XXVII, 442 p. 202 illus., 192 illus. in color.,  
Hardcover

ISBN: 978-3-319-69223-4