2018

# Pathology-Informed Approach in Vulnerability Assessment Methods

Polinpapilinho F. Katina
*Old Dominion University*

Adrian V. Gheorghe
*Old Dominion University*

Charles B. Keating
*Old Dominion University*



## Original Publication Citation

Katina, P. F., Gheorghe, A. V., & Keating, C. B. (2018). *Pathology-informed approach in vulnerability assessment methods*. Probabilistic Safety Assessment and Management PSAM 14, Los Angeles, California. https://www.iapsam.org/psam14/proceedings/paper/paper_62_1.pdf

# Pathology-Informed Approach in Vulnerability Assessment Methods

**Polinpapilinho F. Katina[*a,b,c], Adrian V. Gheorghe[b] and Charles B. Keating[a,b]**
[a] National Centers for System of Systems Engineering, Norfolk, Virginia, USA
[b] Old Dominion University, Norfolk, Virginia, USA
[c] Embry-Riddle Aeronautical University, Worldwide Campus

**Abstract:** A system pathology is a circumstance, condition, or pattern that acts to limit system performance, or lessen system viability, such that the likelihood of a system achieving performance expectation is reduced. The idea of pathology has been described in multiple fields, including computer science, organizational studies, policy analysis, system-of-systems engineering, and systems engineering. However, there is scarcity of literature describing relationship between system pathology and vulnerability assessment. The aim of this study lies at the intersection of system pathology and vulnerability assessment in engineered systems. First, authors provide the state of the art review of literature on system pathology. Second, authors suggest the utility of pathology-informed approach to vulnerability assessment. The aim is to fuse vulnerability assessment methods with pathology-informed concepts for a more robust approach to vulnerability assessment in complex systems. Any investigation into complex systems, with the goal of understanding and improving the system, begins with formulating the problem. This is also the case when one uses the proposed risk-pathology assessment method. The research leverages on recent developments in the Fukushima Daiichi nuclear disaster to offer insights for assessment and design of critical facilities. Finally, the paper concludes with possible multiple research paths.

**Keywords:** Complex System Governance**,** Risk**,** System Pathology**,** System Viability**,** Vulnerability Assessment.

## 1. INTRODUCTION

A system pathology is 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 [1]. While the term 'pathology' has its roots in the field of medicine, with the concern being pathos (Greek: suffering, experiencing, and emotions) and logia (Greek: the study of) in animate organisms, recent research indicates wide acceptable in several disciplines, including computer science, intelligent-based systems, organizational studies, policy analysis, system-of-systems engineering, and systems engineering.

Pathologies have been addressed in multiple fields. In computing systems, pathologies describe issues that degrade performance and are indicative of deviation from the normal expected behavior in hardware transactional memory: FriendlyFire, StarvingWriter, SerializedCommit, FutileStall, StarvingElder, RestartConvoy, and DuelingUpgrades [2]. In intelligence-based systems, pathologies represent organizational structures that might contribute to eroding system effectiveness. Sheptycki's [3] research suggests eleven (11) organizational process pathologies: digital divide, linkage blindness, noise pathology, intelligence overload, non-reporting and non-recording, intelligence gaps, duplication pathology, institutional friction, intelligence hoarding and information silos, defensive data concentration, and occupational subcultures. In management theory and organizational studies, pathology is used to describe organizational issues that might affect performance of formal organizations. Barnard's [4] work on formal organizations describes functional (individual conditions such as privileges, rights, immunities, duties and obligations) and scalar pathological conditions (relationships of superiority in organizational hierarchy and jurisdiction) that affect organizational performance.

[*] Corresponding author: pkatina@odu.edu

In policy analysis, Dery equates pathologies to discrepancies [in social systems] between cherished goals and reality – whose existence and undesirability can be taken for granted [5]. Moreover, the complexities involved in understanding social issues, suggests that the concept of social pathologies varies based on people's worldviews where a problem is not the same to all interested parties [6]. Interestingly, a given problem may not be the same even for all disinterested parties, or even to the same researcher [5].

Additionally, pathologies have roots in the field of cybernetics. The father of management cybernetics, Stafford Beer, drew on biological systems, especially the principles of communication and control, to instruct viability in complex systems. Pathologies, he believed, were at the center of why complex systems, including organizations, fail. Beer also postulated, viable systems of all kind are subject to breakdown. Such breakdowns may be diagnosed, simply in the fact that some inadequacy in the system can be traced to malfunction in one of the five subsystems, where in turn one of the cybernetic features… will be found not to be functioning [7]. He postulated that the etiology of the disorder may be traced, a prognosis may be prepared, and antidotes (even surgery) may be prescribed [7].

Drawing upon systems science [8] and extrapolations from system-of-systems research [1], research proposes over 80 system theory-based pathologies [9,10,11]. Another study conducted at MIT describes system pathologies as errors of execution in systems engineering processes [12].

In summary, there is a variety of perspectives, categories, classifications, and characteristics of system pathology. A common theme is such research is: A system pathology is an aberration from normal 'healthy' conditions. A pathology inherently bad for any given system, even more so for complex and critical infrastructure systems, since pathologies can negatively influence the expected performance of such systems. In present state of our knowledge, there remains a scarcity of literature examining the relationship between the concept system pathology and the topics of vulnerability assessment.

The aim of the present study lies at the intersection of system pathology and vulnerability assessment in engineered systems. To fulfil this aim, authors provide the state of the art review of literature on system pathology --- including theory, definitions and applications. Second, authors suggest the utility of pathology-informed approach to vulnerability assessment. The aim is to fuse vulnerability assessment methods with pathology-informed concepts for a more robust approach to vulnerability assessment in engineering systems. Any investigation into complex systems, with the goal of understanding and improving the system, begins with formulating the problem. This is also the case when one uses the proposed pathology-vulnerability assessment method. The proposed method places emphasis on problem formulation since it considered the most critical stage [5] and is probably the single most important routine, since it determines in large part…the subsequent course of action [13]. The research leverages on recent developments in the Fukushima Daiichi nuclear disaster to offer insights for assessment and design of critical facilities. Finally, the paper concludes with possible multiple research paths --- involving possible areas of application of the developed method, development of methods and tools, and enhancing the suggested method through consideration of relevant topics such as resilience.

## 2. SYSTEM PATHOLOGY PREVELENCE

As indicated above, there are varying perspective of system pathology. In this section, we offer purposely selected categories, classifications, and characteristics of pathologies. First, Table 1 provides nine interrelated metasystem functions essential for governance of all complex systems and acting to enable system viability [14]. These functions provide a 'backdrop' against which the selected system pathologies are derived [15]. Following the development of the Complex System Governance (CSG) formulation, the subsequent research [16] has resulted in development of a three-stage methodology (i.e., initialization, readiness level assessment, and governance development) for implementation to provide structured identification, assessment, and development of CSG. This development methodology relies on effective formulation of the problem domain at the 'front end' of the effort. As part of this formulation, the identification, assessment, and strategizing with respect to pathologies is fundamental.

**Table 1: Elements of CSG Reference Model**

| Metasystem function | Primary role of the function |
|---|---|
| Metasystem five (M5): Policy and identity | To provide direction, oversight, accountability, and evolution of the System. Focus includes policy, mission, vision, strategic direction, performance, and accountability for the system such that: (1) the system maintains viability, (2) identity is preserved, and (3) the system is effectively projected both internally and externally. |
| Metasystem Five Star (M5*): System context | To monitor the system context (i.e., the circumstances, factors, conditions, or patterns that enable and constrain the system). |
| Metasystem Five Prime (M5'): Strategic system monitoring | To monitor measures for strategic system performance and identify variance requiring metasystem level response. Particular emphasis is on variability that may impact future system viability. Maintains system context. |
| Metasystem Four (M4): System development | To provide for the analysis and interpretation of the implications and potential impacts of trends, patterns, and precipitating events in the environment. Develops future scenarios, design alternatives, and future focused planning to position the System for future viability. |
| Metasystem Four Star (M4*): Learning and transformation | To provide for identification and analysis of metasystem design errors (second order learning) and suggest design modifications and transformation planning for the System. |
| Metasystem Four Prime (M4'): Environmental scanning | To provide the design and execution of scanning for the system environment. Focus is on patterns, trends, threats, events, and opportunities for the system |
| Metasystem Three (M3): System operations | To maintain operational performance control through the implementation of policy, resource allocation, and design for accountability. |
| Metasystem Three Star (M3*): Operational performance | To monitor measures for operational performance and identify variance in system performance requiring system level response. Particular emphasis is on variability and performance trends that may impact system viability. |
| Metasystem Two (M2): Information and communications | To enable system stability by designing and implementing architecture for information flow, coordination, transduction and communications within and between the metasystem, the environment, and the systems being governed. |

These functions are derived and grounded in Management Cybernetics, where a pathology describes deficiencies in functions necessary for viability (i.e., continued existence) of an organization (system). Using systems principles of communication and control, Stafford Beer [17,18,19] supplemented by evolving research in viability (e.g., see Keating and Morin [20]), envisioned the necessary and sufficient subsystems of Production (1), Coordination (2), Operations (3), Monitoring (3*), Development (4), Learning and Transformation (4*), and System Identity (5) as essential functions that must be performed by any system. Beer [7] postulated that "malfunction in one of the five subsystems, where in turn one of the cybernetic features …will be found not to be functioning" [7, p. 17] constitutes a pathology. An elaboration on this research by Ríos [21] provides a broad categorization of organizational pathologies including structural, functional and informational. The concept of pathology from the cybernetic sense has also been extended to 'system of systems' and defined as "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" [1, p. 253]. Over 40 'system of system' pathologies were proposed from the work of Keating and Katina [1]. This set of pathologies is directly related to subsystem functions necessary for organizational viability.

Most recently, Katina's [10] research produced over 80 pathologies that might exist for a complex system. This set of pathologies emerged from an examination of concepts from systems theory as they relate to problem formulation. Using a thesis that failure to adhere to systems theory decreases the likelihood of achieving expected system performance outcomes, Katina [9,10,11,22] used the Grounded Theory Method and QSR International's NVivo®10 software package to analyze systems theory text 'data' for 'significant word or phrase' and then thinking critically about the meaning as it relates to

phenomena at hand. A detailed account of these systems theory-based pathologies is found elsewhere [10,22]. However, "the importance lies in the detailed research-based development of the extended set of pathologies that might plague a complex system (organization)" [22, p. 1291].

**Table 2: System Pathologies Corresponding to CSG Functions**

| Metasystem function | Corresponding set of pathologies |
|---|---|
| Metasystem five (M5): Policy and identity | M5.1. Identity of system is ambiguous and does not effectively generate consistency system decision, action, and interpretation. |
| | M5.2. System vision, purpose, mission, or values remain unarticulated, or articulated but not embedded in the execution of the system. |
| | M5.3. Balance between short term operational focus and long term strategic focus is unexplored. |
| | M5.4. Strategic focus lacks sufficient clarity to direct consistent system development. |
| | M5.5. System identity is not routinely assessed, maintained, or questioned for continuing ability to guide consistency in system decision and action. |
| | M5.6. External system projection is not effectively performed. |
| Metasystem Five Star (M5*): System context | M5*.1. Incompatible metasystem context constraining system performance. |
| | M5*.2. Lack of articulation and representation of metasystem context. |
| | M5*.3. Lack of consideration of context in metasystem decisions and actions. |
| Metasystem Five Prime (M5'): Strategic system monitoring | M5'.1. Lack of strategic system monitoring. |
| | M5'.2. Inadequate processing of strategic monitoring results. |
| | M5'.3. Lack of strategic system performance indicators. |
| Metasystem Four (M4): System development | M4.1. Lack of forums to foster system development and transformation. |
| | M4.2. Inadequate interpretation and processing of results of environmental scanning – non-existent, sporadic, limited. |
| | M4.3. Ineffective processing and dissemination of environmental scanning results. |
| | M4.4. Long-range strategic development is sacrificed for management of day-to-day operations – limited time devoted to strategic analysis. |
| | M4.5. Strategic planning/thinking focuses on operational level planning and improvement. |
| Metasystem Four Star (M4*): Learning and transformation | M4*.1. Limited learning achieved related to environmental shifts. |
| | M4*.2. Integrated strategic transformation not conducted, limited, or ineffective. |
| | M4*.3. Lack of design for system learning – informal, non-existent, or ineffective. |
| | M4*.4. Absence of system representative models – present and future. |
| Metasystem Four Prime (M4'): Environmental scanning | M4'.1. Lack of effective scanning mechanisms. |
| | M4'.2. Inappropriate targeting/undirected environmental scanning. |
| | M4'.3. Scanning frequency not appropriate for rate of environmental shifts. |
| | M4'.4. System lacks enough control over variety generated by the environment. |
| | M4'.5. Lack of current model of system environment. |
| Metasystem Three (M3): System operations | M3.1. Imbalance between autonomy of productive elements and integration of whole system. |
| | M3.2. Shifts in resources without corresponding shifts in accountability/shifts in accountability without corresponding shifts in resources. |
| | M3.3. Mismatch between resource and productivity expectations. |
| | M3.4. Lack of clarity for responsibility, expectations, and accountability for performance. |
| | M3.5. Operational planning frequently pre-empted by emergent crises. |
| | M3.6. Inappropriate balance between short term operational versus long term strategic focus. |
| | M3.7. Lack of clarity of operational direction for productive entities (i.e., subsystems). |
| | M3.8. Difficulty in managing integration of system productive entities (i.e., subsystems). |
| | M3.9. Slow to anticipate, identify, and respond to environmental shifts. |
| | M3*.1. Limited accessibility to data necessary to monitor performance. |

| | |
|---|---|
| Metasystem Three Star (M3*): Operational performance | M3*.2. System-level operational performance indicators are absent, limited, or ineffective. |
| | M3*.3. Absence of monitoring for system and subsystem level performance. |
| | M3*.4. Lack of analysis for performance variability or emergent deviations from expected performance levels - the meaning of deviations. |
| | M3*.5. Performance auditing is non-existent, limited in nature, or restricted mainly to troubleshooting emergent issues. |
| | M3*.6. Periodic examination of system performance largely unorganized and informal in nature. |
| | M3*.7. Limited system learning based on performance assessments. |
| Metasystem Two (M2): Information and communications | M2.1. Unresolved coordination issues within the system. |
| | M2.2. Excess redundancies in system resulting in inconsistency and inefficient utilization of resources - including information. |
| | M2.3. System integration issues stemming from excessive entity isolation or fragmentation. |
| | M2.4. System conflict stemming from unilateral decisions and actions. |
| | M2.5. Excessive level of emergent crises - associated with information transmission, communication, and coordination within the system. |
| | M2.6. Weak or ineffective communications systems among system entities (i.e., subsystems). |
| | M2.7. Lack of standardized methods (i.e., procedures, tools, and techniques) for routine system level activities. |
| | M2.8. Overutilization of standardized methods (i.e., procedures, tools, and techniques) where they should be customized. |
| | M2.9. Overly ad-hoc system coordination versus purposeful design. |
| | M2.10. Difficulty in accomplishing cross-system functions requiring integration or standardization. |
| | M2.11. Introduction of uncoordinated system changes resulting in excessive oscillation. |

The above articulated pathologies are aberrations from normal 'healthy' conditions. This postulation, then suggest that there is utility identification of system pathology with a goal of developing countermeasures to address identified pathologies. However, and within the spirit of present research, there is a need to develop an explicit linkage between system pathology and vulnerability assessment. This linkage is the topic of discussion in the following section.

## 3. VULNERABILITY AND ITS ASSESSMENT

### 3.1. System Vulnerability

The term 'vulnerability' has many definitions [23]. These definitions are accepted to various degrees with no definition unanimously being accepted [24]. In fact, 'vulnerability' was long considered as being closely similar to risk, if only with a broader interpretation. However, some authors make a clear distinction between vulnerability and risk. For example, Turner et al. [25] depict vulnerability as a degree to which a system, subsystem, or system component is likely to experience harm due to exposure to a hazard, either a perturbation or a stress/stressor. However, Einarsson and Rausand [26] as well as Holmgren et al. [27], vulnerability is defined as the properties of a system that may weaken or limit its ability to survive and perform its mission in presence of threats that originate both within and outside the system boundaries. Song's [28] research establishes a critical difference between vulnerability and the degree of vulnerability: vulnerability is the susceptibility and resilience (or survivability of the community system) and its environment to hazards. In this case, susceptible comprises two aspects: exposure and sensitivity while survivability mainly comprises elements of robustness, reliability, redundancy, and adaptation [28]. The 'degree of vulnerability' is a numerical index of the vulnerability based on different criteria, usually in the range 0 to 100 percent [28].

Aven's definition appears to be consistent with other research, when invoking "manifestation of the inherent states of the system that can be subjected to a natural hazard or be exploited to adversely affect that system" [29, p. 515]. In distinguishing between vulnerability and risk, [28] directs attention to the differences in the manner of analysis associated with the two concepts. In risk assessment, one might select a particular stress (or threat, hazard) of concern, and seek to identify consequences for a variety of system properties. In contrast, in vulnerability assessment, one selects a particular system (or component) and examine how it can be affected by a variety of stressors. In the present case, stressors can include system pathologies. Obviously, such an analysis will involve identification of means to reduce vulnerability [30].

In summary, regardless of diverging perspectives definitions of vulnerability, there is consensus on the need to consider vulnerability during system assessment. If one adopts vulnerability as "inherent characteristics of a system that create the potential for harm but are independent of the risk of occurrence of any particular hazard" [28, p. 19], then there emerges a need for consideration of the inherent nature of the system and stressors that could affect the system. It is at this consideration that system pathologies might be used to enhance vulnerability assessment methods.

### 3.2. System Vulnerability Assessment Methods

There is no shortage of methods and tools to assist in vulnerability assessment [31]. Vulnerability assessment methods include and not limited to, Econometric Methods which include *Vulnerability as Expected Poverty* (VEP), *Vulnerability as Expected Utility* (VEU), and *Vulnerability as Uninsured Exposure to Risk* (VER), *Household Economy Approach* (HEA), *Household Livelihood Security Analysis* (HLSA), *Household Vulnerability Index* (HVI), *Individual Household Model* (IHM), *Participatory Vulnerability Analysis* (PVA) and *Participatory Capacity and Vulnerability Analysis* (PVCA), *Participatory Wealth/Well-being Ranking* (PWR), Poverty Measures: *Poverty Assessment Tool*s (PAT) and the *Progress out of Poverty Index* (PPI), and *Southern Africa Vulnerability Initiative* (SAVI) Framework, just to name a few. Beyond the need to know the advantages and disadvantages of each method, the selection and usage of a vulnerability assessment method must depend on the context of the problem of interest and capability of the method.

One of the widely used methods is Hierarchical Holographic Vulnerability Assessment (HHVA). HHM has its roots in Hierarchical Holographic Modeling (HHM), which is used in stepwise approach within the framework of parsing the vulnerability concept, hazards and accident scenarios identification, and vulnerability management [32]. The proposed framework can serve as generic vulnerability assessment.

The goal and the overview of HHVA can be summarized as: (a) a way to better understand the system, its elements, and their interdependencies, (b) holistically identify hazards (threats) the system could expose to, (c) systematically point out and assess vulnerabilities, (d) develop policy options against these vulnerabilities, and (d) filter, ranking and recommend policy options. HHVA has nine phases and these are articulated elsewhere [23,28].

The first, and arguably the most important, step is the identify all possible hazards (threats) that the system is exposed to. In this stage of analysis, system pathology play an important role. At this level of the analysis, it can be easier to focus on the technical aspects of the systems. However, anyone of the suggested pathologies (Table 2) could be at the heart of vulnerabilities of the system of interest. An assessment system pathology could highlight soft issues affecting system technical performance.
At this stage in assessment, a method, M-Path, for assessing pathology could be used in conjunction with HHMA. Specifically, phase-one of M-Path [33] involves the identification and discovery of the degree to which the systems theory-based pathologies exist in a given situation/system. This phase involves elicitation of information regarding degree of existence and impact of each pathology.

### 3.3. Pathology-Informed Vulnerability Assessment: The Case for Fukushima Daiichi Nuclear Disaster

Fukushima accident, also called Fukushima nuclear accident or Fukushima Daiichi nuclear accident, accident in 2011 at the Fukushima Daiichi ("Number One") plant in northern Japan, the second worst nuclear accident in the history of nuclear power generation. The site is on Japan's Pacific coast, in northeastern Fukushima prefecture about 100 km (60 miles) south of Sendai. The facility, operated by the Tokyo Electric and Power Company (TEPCO), was made up of six boiling-water reactors constructed between 1971 and 1979. At the time of the accident, only reactors 1–3 were operational, and reactor 4 served as temporary storage for spent fuel rods. Figure 1 depicts the exclusion zone of Fukushima Daiichi nuclear power plant.

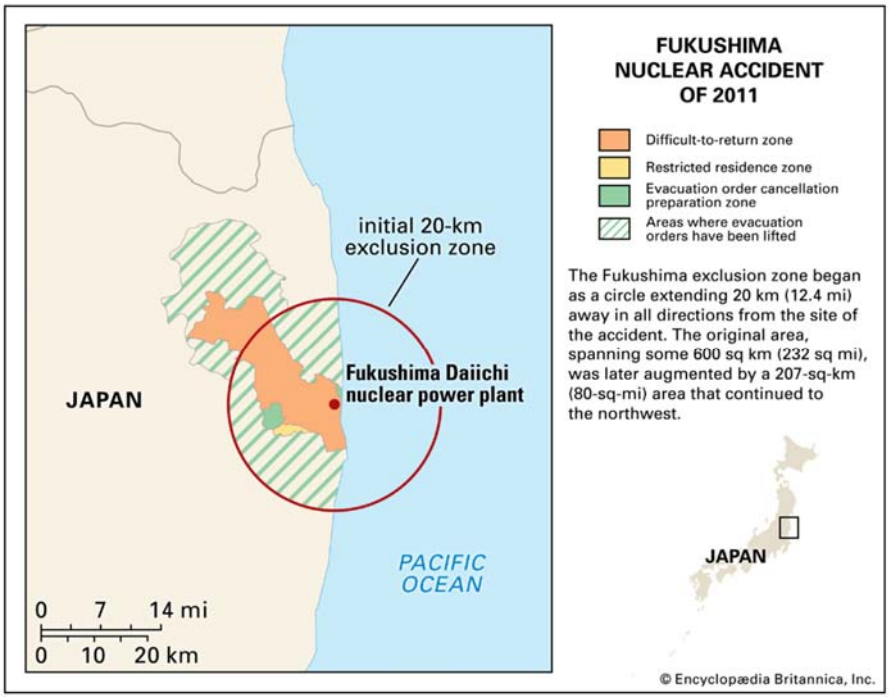


**Figure 1: Fukushima Exclusion Zone**[†]

A mapping of pathology-informed vulnerability assessment can be used to provide an interesting perspective. Granted, this mapping is after the fact. Nonetheless, the pathologies associated with different functions provide a glimpse into potential failure modes that could affect design of such systems that is beyond the technical specifications. This is supported by official findings conducted to investing the Fukushima accident (e.g., see Fukushima Nuclear Accident Analysis Report [34]). Prior safety concerns suggest there was a culture of ignoring safety concerns involving layout of emergency cooling system (e.g., the original plans separated the piping systems for two reactors in the isolation condenser from each other. However, the application for approval of the construction plan showed the two piping systems connected outside the reactor. The changes were never noted; a clear violation of regulations), lack of consideration for flooding (e.g., there is evident suggesting that one of two backup generators of Reactor 1 failed, after flooding in the reactor's basement in October 1991 as well as a lack of consideration of employee concerns), lack of consideration of several studies warning of effects of possible Tsunami, and well as a lack of consideration of earthquake vulnerability (e.g., at a 2008 meeting of the G8's Nuclear Safety and Security Group in Tokyo, experts warned that a strong earthquake with a magnitude above 7.0 could pose a 'serious problem' for Japan's nuclear power stations).

These issues are pathological in nature and review assessment at a different local level. A pathology-informed vulnerability assessment suggests examining pathologies at policy and identity, system context, strategic monitoring, system development, learning and transformation, environmental

[†] Obtained from https://www.britannica.com/media/full/1768504/232271

scanning, system operations, operational performance, and communication (and information) as potential issues that could affect system performance.

Interestingly, such an assessment might uncover different types of vulnerability, all with potential different effects on the system. Six categories vulnerabilities for large-scale complex man-made system are suggested in Table 3.

**Table 3: Selected Vulnerability Assessment Methods**

| Vulnerability Category | A Brief Description |
|---|---|
| Structure stability induced vulnerability | Structure indicates various components that constitute the system, including subsystems, components, and their configurations. Structure stability induced vulnerability means diversified physical, cyber, organizational failures or unfavorable changes in structure components induce structure unstable, increasing the chances that a will not keep the assigned function and operation pattern and thus possible leading to unwanted situations. |
| Complexity induced vulnerability | Taking complexity as multi-components within or between the large-scaled systems with intricate interdependencies, complexity induced vulnerability is taken to describe a situation in which high interdependency and interconnection could create right conditions for a small defect or accident initiated at one point to high chances to propagate throughout the system and escalate into unwanted situations. |
| Operation induced vulnerability | Operations of a system include: 1) the cooperation (i.e., resource and function dynamic assignment and nonlinear interactions), with other interdependent systems or within interconnected multi-components in the system and 2) various maintenance, procedure(process) and emergence action factors within the system. Miss-cooperation can affect the resilience of the system, through nonlinear interactions a determined small change can lead to unexpected emergence, making system at critical situation. And many major accidents occur either during maintenance and procedure operation or because of inadequate or faulty executed maintenance and procedure control. |
| Geography induced vulnerability | Geography is a determinant of climate and primary disadvantage environment controls on a system; it is a determinant as to which natural factors pose hazards to a system. Geography induced vulnerability is also an important path leading to unwanted situations. |
| Organization induced vulnerability | Organization factors comprise decision-making structure, policy and regulation establishment, emergency communication and response etc. Fallible decision or outdated policy and regulation can threat the survivability of a system, inadequate organization can cause system breakdown. |
| Management induced vulnerability | Management mainly implies the security, personnel, operational and financial management. Absence of detection and control for the security issues increases the system susceptibility. Inadequate personnel education and appointment can lead 'sharp end' of the system functions. Unreasonable resource allocation reduces the system resilience to the related hazards. |

## 4. CONCLUSION

A system pathology is 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 [1]. While the term 'pathology' has its roots in the field of medicine, with the concern to logia (the study of) and pathos (suffering, experiencing, and emotions) in animate organisms, recent research indicates wide acceptable in several disciplines, including computer science, intelligent-based systems, organizational studies, policy analysis, system-of-systems engineering, and systems engineering.

In this study, we extend pathology to vulnerability assessment by incorporating system pathologies in assessment of issues that affect system performance. This approach calls for adoption of system pathology and their assessment in system vulnerability approaches. The M-Path Method and HHMA are presented as complementary, guiding in the identification of pathologies, beyond technical failures that can affect system performance.

The deployment of M-Path Method in different venues can also serve a dual-role beyond identification and development of responsive strategic actions to deal with pathologies. First, the more the method is utilized in field applications, the more refined the method becomes. In essence, certain elements of the method might need to be modified based on feedback from field applications. This might be for local application or perhaps to the more general structure and deployment of the methodology. Second, over time patterns of pathologies might emerge. It is possible that certain kinds of pathologies might be associated with certain organizations or circumstances. However, the further development of the method is predicated on field applications to provide continuing development. Subsequently, this might offer insights into the nature of effective and ineffective strategies in response to pathologies in organizations.

**Acknowledgements**

Authors acknowledgements support from the National Centers for System of Systems Engineering.

**References**

[1] C. B. Keating and P. F. Katina, "*Prevalence of pathologies in systems of systems*," International Journal of System of Systems Engineering, vol. 3, no. 3/4, pp. 243–267 (2012).

[2] J. Bobba et al., "*Performance pathologies in hardware transactional memory*," in Proceedings of the 34th annual international symposium on Computer architecture, San Diego: CA, pp. 81–91. (2007).

[3] J. Sheptycki, "*Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing*," European Journal of Criminology, vol. 1, no. 3, pp. 307–332 (2004).

[4] C. I. Barnard, "*Functions and pathology of status systems in formal organizations*," in Industry and Society, W. F. Whyte, Ed. New York, NY: McGraw-Hill, pp. 46–83, (1946).

[5] D. Dery, "Problem definition in policy analysis," University Press of Kansas, 1984, Lawrence, KS.

[6] H. S. Becker, Ed., "Social problems: A modern approach," Wiley, 1966, New York, NY.

[7] S. Beer, "*The viable system model: Its provenance, development, methodology and pathology*," The Journal of the Operational Research Society, vol. 35, no. 1, pp. 7–25 (1984).

[8] K. M. Adams, P. T. Hester, J. M. Bradley, T. J. Meyers, and C. B. Keating, "*Systems theory as the foundation for understanding systems*," Systems Engineering, vol. 17, no. 1, pp. 112–123 (2014).

[9] P. F. Katina, "*Emerging systems theory–based pathologies for governance of complex systems*," International Journal of System of Systems Engineering, vol. 6, no. 1/2, pp. 144–159 (2015).

[10] P. F. Katina, "*Systems theory-based construct for identifying metasystem pathologies for complex system governance*," Ph.D., Old Dominion University, United States – Virginia (2015).

[11] P. F. Katina, "*Systems theory as a foundation for discovery of pathologies for complex system problem formulation*," in Applications of Systems Thinking and Soft Operations Research in Managing Complexity, A. J. Masys, Ed. Geneva, Switzerland: Springer International Publishing, 2016, pp. 227–267.

[12] H. L. Davidz, "*Systems engineering pathology: Leveraging science to characterize dysfunction*," in Disciplinary Convergence in Systems Engineering Research, Cham, Switzerland: Springer, 2018, pp. 683–696.

[13] H. Mintzberg, D. Raisinghani, and A. Théorêt, "*The structure of the 'unstructured' decision processes*," Administrative Science Quarterly, vol. 21, no. 2, pp. 246–275 (1976).

[14] C. B. Keating, "*Governance implications for meeting challenges in the system of systems engineering field*," in 2014 9th International Conference on System of Systems Engineering (SOSE), Adelaide, Australia, 2014, pp. 154–159.

[15] P. F. Katina and C. B. Keating, "*Metasystem Pathologies: Towards discovering of impediments to system performance*," in Proceedings of the 2016 Industrial and Systems Engineering Research Conference, Anaheim, CA, 2016.

[16] C. B. Keating and P. F. Katina, "*Complex system governance development: A first generation methodology*," International Journal of System of Systems Engineering, vol. 7, no. 1/2/3, pp. 43–74, (2016).
[17] S. Beer, "*The heart of the enterprise*," John Wiley & Sons, 1979, New York, NY
[18] S. Beer, "*The brain of the firm: The managerial cybernetics of organization*," Wiley, 1981, Chichester, UK.
[19] S. Beer, "*Diagnosing the system for organizations*," Oxford University Press, 1985, Oxford, UK.
[20] C. B. Keating and M. Morin, "*An approach for systems analysis of patient care operations,*" J Nurs Adm, vol. 31, no. 7–8, pp. 355–363 (2001).
[21] J. P. Ríos, "Design and diagnosis for sustainable organizations: The viable system method," Springer Berlin Heidelberg, 2012, New York, NY.
[22] P. F. Katina, "*Metasystem pathologies (M-Path) method: Phases and procedures*," Journal of Mgmt Development, vol. 35, no. 10, pp. 1287–1301, (2016).
[23] A. V. Gheorghe, D. V. Vamanu, P. F. Katina, and R. Pulfer, "*Critical Infrastructures, Key Resources, and Key Assets*," Springer International Publishing, 2018, Cham, Switzerland.
[24] B. I. Vamanu, A. V. Gheorghe, and P. F. Katina, "Critical infrastructures: Risk and vulnerability assessment in transportation of dangerous goods - Transportation by road and rail," Springer International Publishing, 2016, Cham, Switzerland.
[25] B. L. Turner et al., "*A framework for vulnerability analysis in sustainability science*," PNAS, vol. 100, no. 14, pp. 8074–8079, Jul. 2003.
[26] S. Einarsson and M. Rausand, "*An approach to vulnerability analysis of complex industrial systems*," Risk Analysis, vol. 18, no. 5, pp. 535–546, (1998).
[27] A. Holmgren, S. Molin, and T. Thedéen, "*Vulnerability of complex Infrastructure; power system and supporting digital communication system*," presented at the 5th International Conference on Technology, Policy, and Innovation, Utrecht, the Netherlands, 2001.
[28] C. Song, "A methodological framework for vulnerability assessment for critical infrastructure systems, hierarchical holographic vulnerability assessment (HHVA)," Thesis, ETH Zürich, Zürich, 2005.
[29] T. Aven, "*On some recent definitions and analysis frameworks for risk, vulnerability, and resilience*," Risk Analysis, vol. 31, no. 4, pp. 515–522, (2011).
[30] B. E. Tokgoz and A. V. Gheorghe, "*Resilience quantification and its application to a residential building subject to hurricane winds*," Int J Disaster Risk Sci, vol. 4, no. 3, pp. 105–114, (2013).
[31] W. Moret, "*Vulnerability assessment methods*," The United States Agency for International Development, Washington D.C., AID-OAA-LA-13-00001, 2014.
[32] Y. Y. Haimes, "*Hierarchical holographic modeling*," IEEE Transactions on Systems, Man, and Cybernetics, vol. 11, no. 9, pp. 606–617, (1981).
[33] P. Katina, "*Problem formulation research: From systems theory to discovery of system pathology*," Modern Management Forum, vol. 1, no. 2, pp. 1–11, (2017).
[34] Tokyo Electric Power Company, Inc., "*Fukushima Nuclear Accident Analysis Report*," Fukushima Nuclear Accident Investigation Committee, Tokyo, 2012.