

## THE INVISIBLE LAYER OF FAILURE — FUNCTION-ORIENTED THINKING IN MINISTERIAL DISASTER-MANAGEMENT OF COMPLEX SYSTEMS

*Tariq Ahmad*

### Introduction

The Fukushima Daiichi Nuclear Power Plant disaster in Ōkuma, Japan, and the 2021 Texas power crisis in the United States are often treated as fundamentally different disasters arising from distinct hazards and operating contexts. Yet both reveal a common underlying problem. On 11 March 2011, Fukushima suffered a catastrophic nuclear accident following the earthquake and *tsunami* that struck eastern Japan. A month earlier, an extreme cold wave in Texas triggered a state-wide power emergency marked by widespread outages, economic disruption and loss of life. Neither event was simply a consequence of hazard intensity or isolated infrastructure failure.

In Fukushima, the reactors shut down largely as designed following the earthquake.<sup>1</sup> The disaster emerged subsequently through loss of electrical power required to sustain reactor cooling and monitoring systems.<sup>2</sup> In Texas, the crisis developed through cascading failures across fuel supply and electricity generation systems during peak winter demand.<sup>3</sup> In both cases, disruption extended beyond damaged components and propagated through larger systems upon which society depended.

These cases highlight an important challenge for disaster risk reduction and management (DRRM) in complex systems. Frequently enough, failures emerge not merely from inadequate planning or oversights in governance, but from planning approaches themselves, which focus primarily on what hazards may do to facilities, while paying comparatively less attention to the functions and dependencies sustaining the wider system. Limited failures, or even underperformance under assumed operating conditions, can generate disproportionate consequences when systems are tightly interconnected. Such systems may comprise infrastructure such as ports, power plants and refineries, organisational entities such as ministries and regulators, and operational networks such as power distribution and civil aviation.

This article argues that disaster planning for such systems — particularly within ministries responsible for critical infrastructure under India's disaster management framework — requires a transition towards a systems-oriented understanding of risk that is centred upon critical functions

---

<sup>1</sup> International Atomic Energy Agency, *The Fukushima Daiichi Accident: Technical Volume 1/5 – Description and Context of the Accident* (Vienna: International Atomic Energy Agency, 2015), <https://www-pub.iaea.org/MTCD/Publications/PDF/AdditionalVolumes/P1710/Pub1710-TV1-Web.pdf>

<sup>2</sup> International Atomic Energy Agency, *The Fukushima Daiichi Accident*, 11.

<sup>3</sup> Joshua W Busby, Kaylee Shoup Baker, Morgan D Bazilian, Ashlynn Q Gilbert, Emily Grubert, Varun Rai, Joshua D Rhodes, Sarang Shidore, Caitlin A Smith, and Michael E Webber, “Cascading Risks: Understanding the 2021 Winter Blackout in Texas”, *Energy Research & Social Science* 77 (2021): 102106, <https://doi.org/10.1016/j.erss.2021.102106>

and interdependencies. It makes the case that ministries responsible for complex infrastructure and service networks should supplement conventional DRRM approaches with methods capable of identifying cascading vulnerabilities and hidden dependencies. Using a set of illustrative examples, the article advances a systems- and function-oriented perspective with particular reference to ministerial disaster management planning under India's National Disaster Management framework,<sup>4</sup> and with special focus on the Ministry of Ports, Shipping and Waterways (MoPSW).<sup>5</sup>

### The Core Problem

To understand the requirement for a shift in approach, the Fukushima and Texas cases merit closer examination.

The Fukushima Daiichi Nuclear Power Plant was designed to withstand severe earthquakes and *tsunamis*, with the reactors shutting down largely as intended following the March 2011 earthquake. The subsequent disaster emerged after the facility experienced a station blackout (SBO),<sup>6</sup> losing electrical power required for cooling and monitoring systems. Although contingency procedures existed for loss of off-site power, these depended upon emergency backup systems which themselves were vulnerable to *tsunami* flooding.<sup>7</sup> The disaster, therefore, revealed not merely a problem of underestimated hazard probability, but the consequences of losing a critical supporting function upon which reactor safety depended.

A similar pattern emerged during the 2021 Texas power crisis. Electricity generation in the state depended substantially upon natural gas supplied through interconnected extraction and processing infrastructure.<sup>8</sup> Extreme cold impaired portions of this supply chain while electricity demand simultaneously increased. Although some infrastructure lacked adequate “winterisation”, one of the principal contributors to the crisis was the progressive degradation of fuel supply rather than immediate destruction or complete infrastructure failure. The resulting disruption propagated through interdependent systems, all supporting electricity generation.

Both these cases reveal two important characteristics of disaster in complex systems. First, failures may originate at locations physically or organisationally distant from the apparent site of disaster, propagating through interconnected dependencies. Second, disruption frequently concerns not the principal infrastructure itself, but the supporting functions and operating assumptions upon which it relies.

The same problem is visible from an organisational perspective. The attacks of 11 September 2001 demonstrated how emergency arrangements may fail even where formal command and coordination mechanisms exist,<sup>9</sup> while the COVID-19 pandemic exposed how routine assumptions underlying disaster response — including physical co-location of personnel and continuity of operations<sup>10</sup> — can become unexpectedly vulnerable. In India, the concurrence of

---

<sup>4</sup> National Disaster Management Authority, *National Disaster Management Plan 2019* (New Delhi: National Disaster Management Authority, 2019), <https://ndma.gov.in/sites/default/files/PDF/ndmp-2019.pdf>

<sup>5</sup> National Institute of Disaster Management, “Projects”, accessed 31 May 2026, <https://nidm.gov.in/projects.asp>

<sup>6</sup> International Atomic Energy Agency, *The Fukushima Daiichi Accident*, 14.

<sup>7</sup> International Atomic Energy Agency, *The Fukushima Daiichi Accident*, 15.

<sup>8</sup> Busby et al., “Cascading Risks: Understanding the 2021 Winter Blackout in Texas”

<sup>9</sup> National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: U.S. Government Printing Office, 2004), <https://govinfo.library.unt.edu/911/report/index.htm>

<sup>10</sup> Alexander J Towbin, Jennifer Regan, David Hulefeld, Eric Schwieterman, Laurie A Perry, Sarah O'Brien, Akhil Dhamija, Timothy OConnor, and Jay A Moskovitz, “Disaster Planning During SARS-CoV-2/COVID: One

the pandemic and Cyclone *Amphan*<sup>11</sup> further illustrated how overlapping hazards and operational constraints may stress emergency systems<sup>12</sup> even without producing systemic collapse.

These examples suggest that the challenge lies not merely in isolated planning failures, but in the very logic through which disaster risks are often framed. Conventional disaster planning frequently begins by asking:

*What will a hazard do to a facility, organisation or process?*

Yet complex systems often fail through a different pathway:

*How does a hazard affect the critical functions and dependencies required for that facility, organisation or process to operate?*

This distinction reflects a function-oriented understanding of disaster risk.

Importantly, this concern is not entirely absent from existing practice. Business continuity planning, dependency mapping and critical function analysis frequently recognise the importance of sustaining essential functions and managing interdependencies. However, such perspectives remain unevenly integrated within large-scale disaster management planning, particularly at organisational and ministerial scales where infrastructure, responsibilities and operational dependencies span multiple domains.

This creates a practical challenge. Ministries overseeing complex infrastructure rarely possess a single office capable of maintaining complete understanding of all vulnerabilities, dependencies and cascading pathways. India's Ministry of Ports, Shipping and Waterways (MoPSW), for example, oversees infrastructure, regulatory functions and operational networks connected to logistics, energy supply and international maritime systems whose consequences are seldom localised. Such complexity cannot be ignored, yet neither can it be analysed as a single undifferentiated whole.

A method is, therefore, required to simplify complexity without overlooking it. Large organisations already provide an important clue. Ministries and institutions are composed of semi-autonomous units — departments, divisions and agencies — performing distinct functions while interacting through identifiable interfaces. Understanding disaster risk in complex systems consequently becomes a problem of organising these interdependent relationships into analytically manageable components. This forms the basis of a “System of Systems” (SoS) approach.

### **“System of Systems” (SoS) Approach – Principles**

The challenge identified earlier is not merely one of recognising that complex systems possess multiple vulnerabilities, but of understanding how such complexity can be analysed without becoming unmanageable. Ministries and organisations overseeing critical systems cannot realistically trace every dependency, operational process, and hazard pathway, simultaneously. A

---

Radiology Informatics Team's Story”, *Journal of Digital Imaging* 34, No. 2 (2021): 290–296,  
<https://doi.org/10.1007/s10278-021-00420-x>

<sup>11</sup> Shubham Kumar, Preet Lal, and Amit Kumar, “Influence of Super Cyclone ‘Amphan’ in the Indian Subcontinent amid COVID-19 Pandemic”, *Remote Sensing in Earth Systems Sciences* 4, No. 1–2 (2021): 96–103,  
<https://doi.org/10.1007/s41976-021-00048-z>

<sup>12</sup> Cross Synergy Publications, “A Case Study on Disaster Management”, September 2022,  
<https://crosssynergypublications.rpsg.in/the-whitepaper/a-case-study-on-disaster-management>

method is, therefore, required to simplify complexity without ignoring it. The SoS approach<sup>13</sup> addresses this challenge by organising complexity into analytically manageable components.

The fundamental principle of SoS is that a system — whether physical, organisational or conceptual — may be understood through the functions it performs, the dependencies it relies upon, and the interfaces through which it interacts with other systems. A system may itself comprise multiple sub-systems interacting internally in complex ways. Beyond the system boundary, however, these internal interactions may often be reduced to a smaller set of functional relationships and dependencies.

This principle reflects how large organisations already operate. Institutions are rarely monolithic. Rather, they comprise semi-autonomous units functioning at different levels of hierarchy and responsibility. The SoS approach formalises this structure for disaster analysis by recursively organising systems into sub-systems connected through defined interfaces.

Its principal analytical advantage lies in the “black box” principle. Disaster planning does not require complete understanding of every connected system’s internal workings. Instead, the primary concern becomes whether a system can reliably perform the functions upon which others depend. Internal complexity may therefore be treated as a “black box”, allowing attention to focus on functions, dependencies and interfaces.

This distinction is particularly important for disaster risk reduction and management (DRRM), where cascading failures frequently emerge not through collapse of isolated systems but through disruption at points of interaction. By identifying such interfaces explicitly, the SoS approach simplifies analysis while revealing vulnerabilities that may otherwise remain hidden.

**Figure 1** illustrates this principle through an organisational schema centred on a port system such as Deendayal Port and its associated connections. The red dashed boundary represents the jurisdictional domain of the MoPSW, and the figure should be interpreted not merely as an organogram but as a representation of interacting systems and interfaces.

---

<sup>13</sup> Nirupama N, “Systems Approach to Management of Disasters: Methods and Applications”, *Disaster Prevention and Management: An International Journal* 20, No. 4 (2011): 450–451, <https://doi.org/10.1108/09653561111161770>

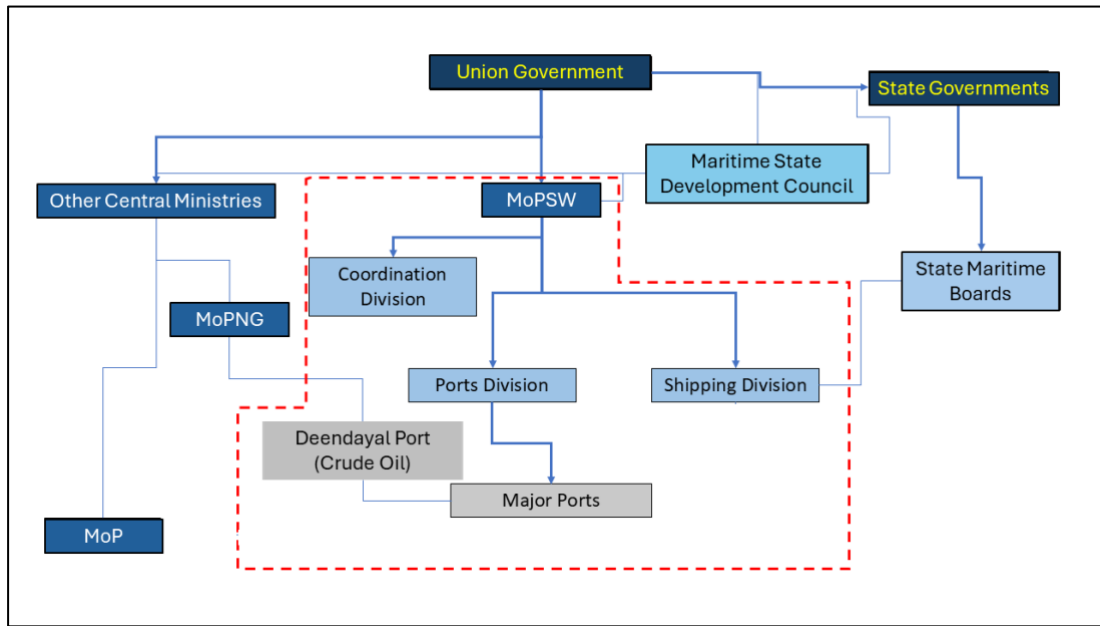


Fig 1: A macro level organisational schema of the functioning of a major port under the MoPSW governance framework.

Source: Adapted by the Author from the MoPSW

Within this boundary, multiple entities and processes operate with their own internal complexity. External systems need not, however, fully understand these internal arrangements. For example, the Ministry of Petroleum and Natural Gas (MoPNG) may treat delivery of hydrocarbons up to designated port interfaces as falling within MoPSW's functional domain, while MoPSW may regard onward transmission and downstream processing as belonging to MoPNG. The internal functioning of either ministry may therefore remain analytically "black-boxed" to the other, provided the required functions are reliably performed.

**Figure 2** represents this relationship in simplified functional form. MoPSW's concern becomes the delivery of crude oil and natural gas to designated transfer points, while MoPNG's concern becomes reception and downstream processing. This simplification reflects the principal analytical value of SoS — complex institutional arrangements become understandable through a limited set of functional relationships.

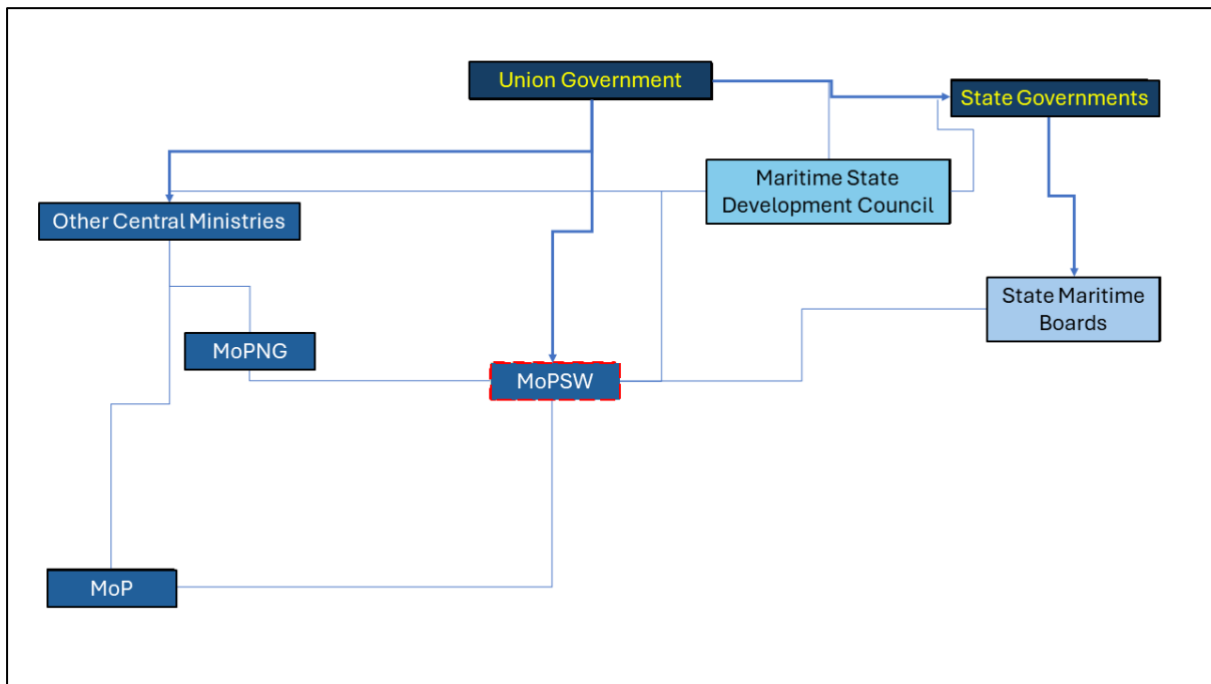


Fig 2: Representation of the schema in the Fig 1 with MoPSW collapsed to a single node.

Source: Adapted by the Author from the MoPSW

The simplified schema also exposes an important DRRM insight. Frequently, vulnerabilities arise not within isolated systems alone, but at the interfaces connecting them. Pipelines, transfer terminals, or storage facilities situated within port jurisdiction, may each represent shared dependencies, whose disruption affects multiple ministries simultaneously. Such vulnerabilities often remain obscured when planning is conducted solely within administrative or facility boundaries.

From a DRRM perspective, the operational questions consequently become more precise. For the MoPSW, the concern becomes whether vulnerabilities affect the ministry's ability to receive, berth, unload and transmit hydrocarbons. For the MoPNG, the concern becomes whether vulnerabilities affect reception, storage, and downstream processing to entities under ministries such as the power plants under the Ministry of Power (MoP). While these relationships may initially appear self-evident, their explicit acknowledgement provides the analytical basis for identifying shared vulnerabilities and clarifying disaster management responsibilities.

The same principle applies within ministries themselves. **Figure 3** illustrates an interface relationship between the Shipping Division and the Ports Division, both of which are within the MoPSW. The Ports Division oversees port infrastructure and associated administrative functions, while the Shipping Division, through the Directorate General of Shipping, administers navigation, harbour entry and regulatory compliance.

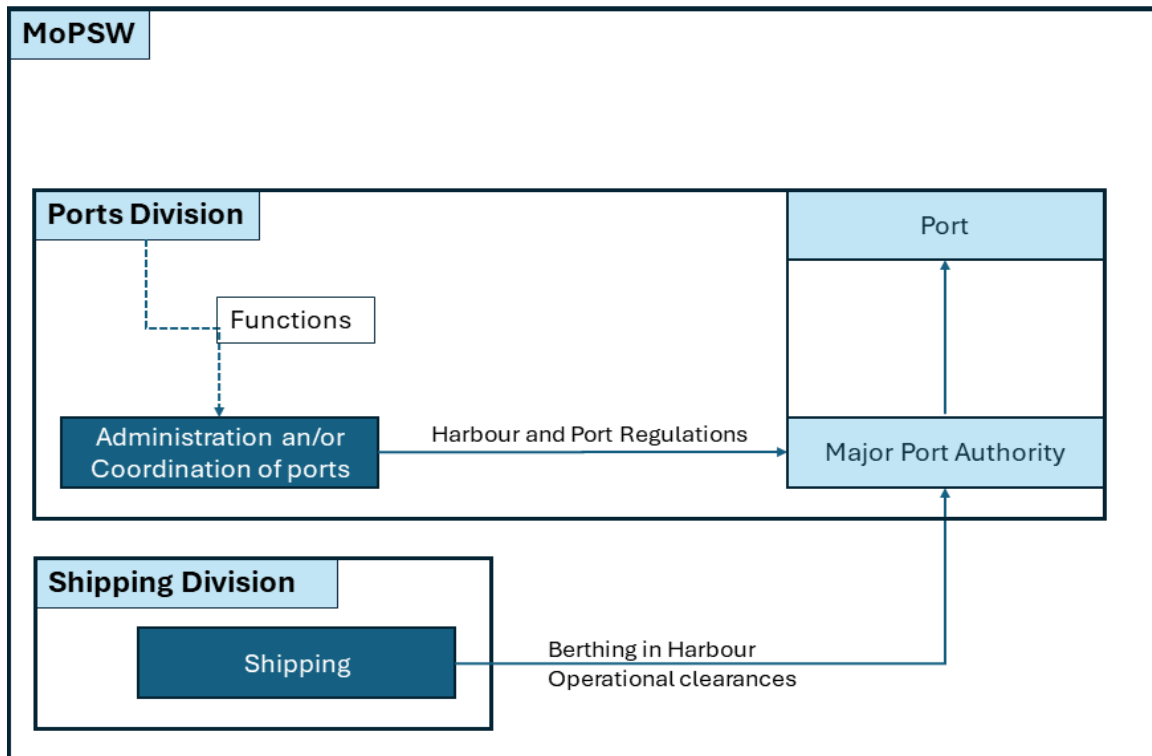


Fig 3: A macro level functional schema of the Ports Division and the Shipping Division of the MoPSW, highlighting their roles in a ship's berthing process.

Source: Adapted by the Author from the MoPSW

The significance of this relationship lies in the interface between the two systems. The operational act of berthing a vessel depends simultaneously upon infrastructure, harbour operations, navigation management and regulatory oversight. Neither division requires detailed understanding of the other's internal functioning. What matters is whether the interconnected functions necessary for safe and timely berthing remain operational.

The examples illustrated in the figures demonstrate that SoS does not eliminate complexity. Rather, it reorganises complexity into manageable analytical units and reveals the interfaces through which disaster vulnerabilities frequently emerge. Once such system boundaries, dependencies, and interfaces have been identified, the next analytical step follows naturally — understanding how hazards affect the critical functions performed by these systems. This forms the basis of a function-oriented approach (FOA).

### Function-Oriented Approach (FOA)

Once systems, interfaces and dependencies have been identified through a SoS framework, the next analytical step becomes understanding how hazards affect the functions performed by those systems. This forms the basis of a function-oriented or function-based approach (FOA).

The FOA places analytical emphasis not upon infrastructure or organisations themselves, but upon the functions they perform and the conditions required to sustain them.<sup>14</sup> In this sense, FOA operates within the SoS framework. While SoS identifies systems, boundaries and interfaces, FOA evaluates the vulnerability of the functions performed across those relationships.

This perspective differs from the conventional inventory-based approach commonly adopted in disaster risk assessment:

### **Inventory-Based Approach**

1. Identify hazards potentially affecting a facility or organisation.
2. Assess risks as functions of probability and consequence.
3. Assign risk scores and implement mitigation measures.

Such approaches remain useful and widely applied. However, their analytical framing does not always prioritise functions and dependencies, particularly where vulnerabilities emerge indirectly through interconnected infrastructure and organisational relationships. Planning may, therefore, become centred on identifying what hazards can physically affect a facility, while giving comparatively less attention to disruption of the enabling functions upon which system performance depends.

The Texas power crisis provides an illustrative contrast. Certain elements of electrical and gas infrastructure were vulnerable to severe cold and lacked adequate winterisation. Yet one of the principal contributors to the crisis did not arise through immediate destruction or complete infrastructure failure. Instead, disruption developed progressively through degradation of natural gas extraction and processing systems, reducing fuel availability to power generation precisely when electricity demand increased.

An inventory-oriented assessment might principally enquire whether extreme cold could damage generating or transmission infrastructure. A function-oriented assessment asks an additional question: can cold conditions degrade the fuel supply function upon which electricity generation depends? The distinction is significant. The crisis evolved not solely through infrastructure damage but through sequential degradation of interdependent functions whose consequences cascaded across the grid.

This illustrates an important characteristic of FOA. Disaster impacts do not always manifest themselves through complete failure or physical destruction. Functions may degrade, become delayed or operate below required thresholds, even while remaining physically intact. Such degradation may, nevertheless, generate consequences comparable to complete system collapse.

Operationally, a function-oriented assessment may be implemented through a relatively straightforward sequence:

1. Identify the critical function performed by a system or sub-system.
2. Identify the dependencies and interfaces enabling that function.
3. Assess how hazards may disrupt, degrade or interrupt those dependencies.

---

<sup>14</sup> Erik Hollnagel, “An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change” (Sweden, 2012)

4. Evaluate the consequences of functional degradation or failure.
5. Identify measures necessary to sustain, substitute or restore the function.

The Fukushima Daiichi disaster provides a useful illustration of how this analytical shift changes the framing of disaster risk.

The IAEA assessments highlight several important observations:

- Both the reactors and emergency power systems underwent risk-assessment against multiple threats, including *tsunamis*.
- While the reactor systems were considered resilient, the probability and consequences of losing emergency power were insufficiently appreciated, partly owing to limited historical precedent regarding *tsunami* magnitude.
- Disaster planning and structural design were framed largely around what a *tsunami* could physically do to emergency systems, rather than the consequences arising if those systems could no longer perform their function.

The functional perspective of the plant may therefore be represented as shown in Fig 4.

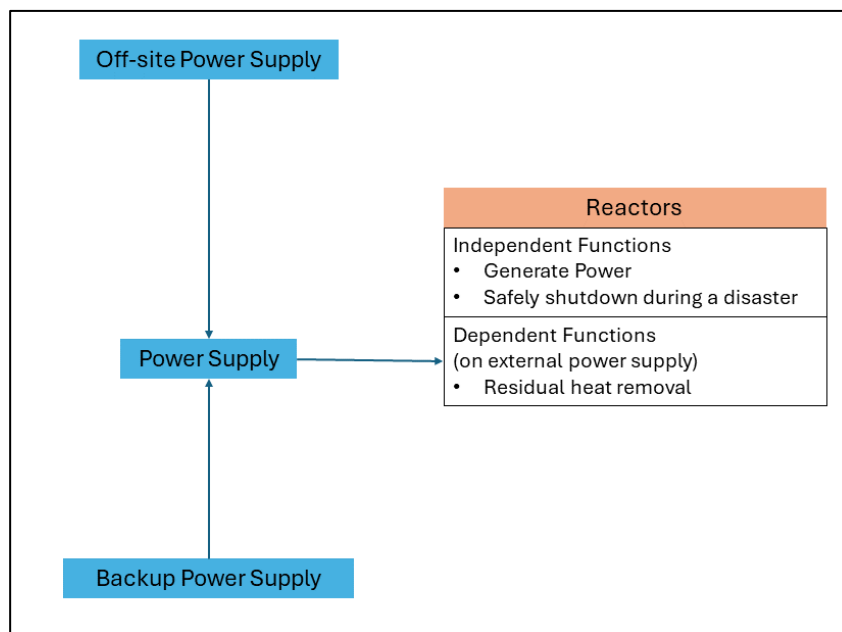


Fig 4: A functional schema of the Fukushima reactor and emergency power supply as safety systems

Source: Adapted by the Author from the IAEA

The figure should be interpreted as a dependency schema rather than a structural diagram. The central requirement was not reactor integrity alone but safe shutdown and residual heat management, both dependent upon sustained electrical power supplied either through off-site or emergency systems.

The reactors shut down automatically following the earthquake, as designed. However, safe post-shutdown management required electricity for monitoring, cooling, and residual heat removal systems. The disaster therefore emerged not from continued fission within the reactor core but from loss of the supporting function enabling residual heat management.

The FOA consequently reframes disaster analysis from a broader and more adaptable perspective. Rather than asking solely what hazards may damage a facility, the enquiry becomes: what conditions are necessary for a critical function to continue, and how may hazards compromise those conditions? This shift provides a comparatively hazard-agnostic framework through which diverse threats — including climate extremes, cyber-attacks, supply disruptions, workforce shortages and concurrent disasters — may be analysed through a common functional lens.

### **Implications for Ministerial Disaster Management Planning**

Contemporary resilience and critical infrastructure literature increasingly recognises that disasters affecting complex infrastructure rarely remain confined to individual assets or administrative jurisdictions. Concerns over cyber-attacks, climate-induced disruptions, supply-chain vulnerabilities and compound disasters have progressively shifted attention towards interdependencies, cascading failures and continuity of essential functions. While such ideas are neither entirely new nor exclusive to disaster management, their systematic integration within large-scale ministerial disaster management planning remains uneven.

This observation is important because ministerial disaster management plans (DMPs) need not follow identical planning architectures. The nature of a ministry's domain and the logic through which disruption propagates should influence how disaster risk is organised and assessed.

The Disaster Management Plan prepared by the Ministry of Health and Family Welfare (MoHFW), for example, reflects a planning problem different from that faced by the MoPSW.<sup>15</sup> The MoHFW oversees healthcare systems and emergency medical response, organised largely through territorial jurisdictions and service-delivery networks. Consequently, its DMP naturally emphasises spatial coordination, surge capacity, and geographically distributed response arrangements. This distinction does not imply that health emergencies are geographically confined — the COVID-19 pandemic demonstrated otherwise — but that the operational architecture of health emergency management remains predominantly territorial.

The planning problem encountered by MoPSW differs in an important respect. Maritime systems are often not spatially localised in the same manner as healthcare systems. Their vulnerabilities are instead topologically localised — concentrated within networks, interfaces, and dependencies, whose consequences may propagate far beyond the originating site. Ports,

---

<sup>15</sup> Department of Health & Family Welfare, *Departmental Disaster Management Plan 2018* (Shimla: Government of Himachal Pradesh, 2018), <https://hpsdma.nic.in/WriteReadData/LINKS/DMP%20-%20Dept%20of%20Health%20%20Family%20Welfare%20-%2020189948d1fb-b092-40d4-82d8-dc9214f23cad.pdf>

shipping routes, logistics corridors, and fuel-supply chains, all operate through interconnected systems extending across ministries and, frequently, across national boundaries as well.

A disruption occurring at a single maritime interface may, therefore, generate consequences that are disproportionate to its geographic footprint. Port outages, shipping disruptions, or failures at transfer facilities, may affect refinery operations, industrial supply chains, or energy systems, despite being physically distant from the originating event. The cascading logic resembles the Fukushima and Texas cases discussed earlier, where disruption propagated through functional dependencies rather than physical proximity alone.

This distinction carries important implications for ministerial DMP architecture. Planning approaches organised principally around territorial response and localised impacts may be insufficient where disruption propagates through infrastructure networks and institutional interfaces. Ministries such as MoPSW, therefore, require greater emphasis upon inter-organisational coordination, interface vulnerabilities and continuity of critical functions extending beyond individual facilities.

The SoS–FOA framework provides one means of addressing this challenge. Its principal value lies not merely in identifying hazards, but in organising assumptions, responsibilities and dependencies in a form that remains analytically transparent and capable of being updated over time.

This characteristic becomes institutionally significant because DMPs are not static documents. Under India’s disaster management framework, ministries are required to prepare, review and periodically revise their plans through formal administrative processes. Yet the assumptions underpinning disaster planning — including dependencies, organisational arrangements and emerging vulnerabilities — evolve continuously between formal revisions.

The SoS–FOA schema may, therefore, serve as an institutional memory supporting this process. By explicitly identifying systems, interfaces and critical functions, the framework allows newly recognised threats — including cyber risks, autonomous systems, climate-induced disruptions and supply-chain stresses — to be assessed without requiring the complete redesign of the underlying analytical logic. In so doing, it preserves continuity not merely of documented risks, but of the reasoning and assumptions upon which planning decisions were originally based.

### **Conclusion and Way Forward**

The disasters and planning-challenges discussed in this article highlight an increasingly important reality of contemporary disaster risk-reduction and management (DRRM) — the most consequential failures within complex systems do not always originate through direct physical destruction or localised hazards. Rather, they frequently emerge through disruption of critical functions, degradation of dependencies, and cascading effects propagating across interconnected systems. The Fukushima and Texas crises, as also the organisational disruptions observed during events such as 9/11 and the COVID-19 pandemic, all demonstrate that vulnerabilities may remain obscured when planning focuses principally upon hazards affecting facilities or administrative entities in isolation.

This article has argued that such challenges are particularly relevant for ministries responsible for complex infrastructure and service networks. Conventional hazard- and inventory-based approaches remain necessary components of DRRM and continue to provide valuable mechanisms for assessing exposure, probability and consequence. Yet for networked systems

operating through multiple organisational and infrastructural dependencies, these approaches may not consistently foreground the pathways through which disruption propagates. The System of Systems (SoS) and Function-Oriented Approach (FOA) frameworks discussed here provide one possible means of addressing this analytical gap by shifting attention towards interfaces, dependencies and continuity of critical functions.

The relevance of this perspective becomes especially pronounced within the Indian ministerial context. Ministries need not confront identical disaster management problems, nor should their DMPs necessarily follow identical planning architectures. As illustrated through the comparison between the MoHFW and the MoPSW, the logic through which disruption propagates matters. Health-sector planning frequently operates through territorially organised response systems, whereas maritime disruptions often propagate through networked and topological relationships extending across jurisdictions, ministries, and national boundaries. Consequently, disaster planning for such domains would benefit from frameworks designed to recognise cascading effects and inter-organisational dependencies.

The principal suggestion emerging from this discussion is, therefore, quite straightforward — future development and revision of ministerial DMPs for infrastructure-intensive and networked sectors should consider incorporating SoS and FOA principles within their planning methodology.

As a practical starting point, ministries need to undertake a systematic identification of systems, interfaces and critical dependencies prior to detailed hazard assessment. Such mapping will help clarify institutional responsibilities, identify shared vulnerabilities, and reveal potential pathways of cascading failure that extend beyond individual facilities or departments. A complementary consideration concerns assessment of critical functions themselves. Rather than limiting enquiry to what hazards may damage assets, planning exercises may additionally examine the conditions necessary for sustaining essential functions and the consequences arising from their degradation or interruption.

The SoS–FOA framework may also serve a broader institutional purpose. Disaster management plans are periodically reviewed through formal administrative processes,<sup>16</sup> while the assumptions underpinning them evolve continuously. By explicitly documenting systems, interfaces and functional dependencies, the framework provides a form of institutional memory that can support incremental adaptation between formal revisions and preserve continuity in disaster reasoning despite organisational change or emerging threats.

The purpose of this article has not been to prescribe a singular model for all disaster planning, but to suggest that DMP architecture should reflect the characteristics of the systems it governs. For ministries overseeing complex and interdependent infrastructure domains, a systems and function-oriented perspective may offer a useful direction for strengthening future DRRM practice.

---

<sup>16</sup> Government of India, *The Disaster Management Act, 2005*, sec. 37, [https://www.indiacode.nic.in/handle/123456789/18558?sam\\_handle=123456789%2F2505](https://www.indiacode.nic.in/handle/123456789/18558?sam_handle=123456789%2F2505)

***About the Author***

*Mr Tariq Ahmad is a Research Associate at the National Maritime Foundation. His research focus is on port adaptation, disaster- and climate-change resilience, maritime spatial planning, and the blueing of the economy. His background is in architecture and spatial planning (urban & regional). He may be contacted at [rsor1.nmf@gmail.com](mailto:rsor1.nmf@gmail.com).*