Risk-Based HSE Governance Framework for Enhancing the Resilience of Critical Industrial Infrastructure in Saudi Arabia

Abstract

Saudi Arabia's industrial growth is predicated on infrastructure and the disruption of that infrastructure can have a cascading effect on the safety of workers, the safety of the communities around it, the environment and the delivery of essential services. Traditional HSE (health, safety and environment) arrangements tend to look at these various aspects in isolation through separate compliance, occupational and process safety regimes. This critical integrative review looks at how risk-based governance can bring those various regimes together in a way that enables infrastructure resilience. A structured, purposive evidence synthesis was conducted on 30 DOI identifiable publications from the period 2020 to 2025 covering critical infrastructure, major accident prevention, organisationalbehaviour, emergency preparedness and digital assurance. Six interdependent governance functions are identified: strategic accountability, system wide risk intelligence, verified safety barriers, workforce participation, adaptive emergency capability and independent learning. A lifecycle framework is then developed which links asset criticality, cross sector dependencies, tolerable service interruption, decision rights and measurable recovery performance. The review makes it clear that resilience cannot be assumed from the completion of an audit, the frequency of incidents or the acquisition of technology. Operators must be able to demonstrate that their controls are effective under changing conditions and that they can recover critical functions without transferring the risk of harm elsewhere. The framework provides a testable basis for Saudi industrial operators, infrastructure owners and regulators and recognises that locally calibrated thresholds and prospective validation will be required.

UNDER PEER REVIEW IN IJAR

1 Introduction:

Critical industrial infrastructure is really more defined by the consequences of its failure than by the size of the facility. A petrochemical complex will be reliant on a continuous supply of electricity, industrial water, communications and logistics. A power generation facility will be reliant on fuel supply and the integrity of its control networks. When one service fails the traditional notion of asset boundaries provides very little protection against the propagation of the disturbance via the shared utilities and the operating decisions of the various facilities. Saudi Arabia's industrial diversification makes this issue even more important as the degree of diversification, the level of integration and the rate of project delivery all tend to increase the number of interfaces that will need to be managed and assured. Governance therefore has to look at not just the probability of the initiating event but the pathways through which the consequences of that event will propagate and the capacity to maintain essential functions [1].

Occupational health and safety, process safety and environmental protection all make their own distinct contributions. OH&S is about preventing personal exposure and injury. Process safety is about containing the energy and materials that are hazardous. Environmental protection is about limiting the release of substances and the consequent damage to the environment. None of these are complete in the absence of an integrated approach where they are treated as separate reporting streams. There is evidence from the Saudi building projects that a proactive assessment of management practice is required rather than simply looking at the injury data [2]. The same is true of research into enterprise standards which suggests that the mere adoption of formal management systems doesn't answer the fundamental questions of who makes the risk decisions, which activities get the priority and how the controls actually work [3]. An integrated governance problem remains even when you have a very extensive set of documented procedures.

Workplace emergencies highlight another constraint: the procedures we design for a given operating state may well be unworkable if that state is simultaneously changed in terms of staffing, supply chains and access. The recent work on systematic workplace health emergency

UNDER PEER REVIEW IN IJAR

response is very clear on the value of integrating planning, operational support, performance monitoring and corrective learning [4]. Applying that insight to hazardous industrial networks however requires a very explicit treatment of catastrophic scenarios, infrastructure interdependencies and the authority to stop production. The research gap is not simply one of hazard identification. It is the lack of a practical account of how the evidence on exposure, protection, interdependencies and recovery is to be transferred between the executive, the site manager, the contractor and the external responders.

This review builds on that account without in any way purporting to quantify the current state of play at any particular Saudi facility. It looks at a fairly limited body of recent literature, distinguishes between the established facts and the various design propositions and then sets out a number of decision tests which could be used to falsify the proposals in future work. The contribution is a governance architecture in which resilience is an accountable operating capability rather than a mere marketing statement. The focus is specifically on the period 2020-2025 so that the current understanding of system complexity, working practices and digital monitoring is able to inform the design of the proposed arrangements.

2 Study aim and objectives

The study is about building a risk based HSE governance framework which will assist Saudi industrial operators in maintaining their safety critical functions prior to, during and after a disruption. The first objective is to identify the governance decisions which link occupational, process and environmental risk to operational continuity. The second is to compare the way that recent resilience work has approached interdependency, safeguards, adaptive response and recovery. The third is to turn those concepts into clear responsibilities, evidence requirements and assurance indicators for use in multi operator industrial networks. The fourth is to define the limitations and to specify the empirical tests rather than present an untested conceptual model as a ready made intervention. The central review question is: what governance arrangements enable

UNDER PEER REVIEW IN IJAR

risk information to inform the preventative, adaptive and restorative decisions across the life cycle of critical Saudi industrial infrastructure?

3 Review design and analytical approach

A critical integrative review was chosen as the study as it cuts across engineering reliability, institutional governance, occupational health and organisational resilience. The disciplines in question use very different units of analysis and are often measuring very different outcomes. A statistical meta-analysis would be combining non-comparable measures; a simple descriptive inventory would not in itself explain the mechanisms by which governance decisions impact on infrastructure performance. The review is therefore a purposive selection of the literature, with structured extraction, comparison of competing explanations and synthesis into a falsifiable framework. It is a conceptual review of the published evidence and not an empirical survey, a prospective experiment or an exhaustive census of the database records.

Literature search focused on peer-reviewed papers from 2020 to 2025 using a combination of the following terms: 'critical infrastructure', 'resilience', 'process safety', 'HSE governance', 'safety barriers', 'Saudi Arabia', 'occupational safety', 'interdependency', 'digital twin' and 'emergency response'. Article identity and relevance were ascertained via publisher records, scholarly repositories and DOI indexed bibliographic records. Papers were included if they addressed at least one of the following causal elements of infrastructure continuity, major hazard control, institutional accountability, safety culture, workforce protection or adaptive decision support. Papers outside the date range, without a DOI or not relevant to any of the above mechanisms were excluded and the final reference set comprised thirty items.

The analytical unit was a substantive rather than a numerical result. For each publication selected, the extraction looked at context, study or review design, risk mechanism, governance actor, proposed intervention, type of evidence and likely transferability to Saudi operations. The

UNDER PEER REVIEW IN IJAR

evidence was initially categorised into five areas: infrastructure criticality, barrier integrity, organisational practice, disruption management and measurement. Cross category comparison led to the six governance functions described below. Mechanisms with empirical support were clearly distinguished from those which were inferred. There are no made up screening totals, no pooled effect sizes, no Saudi accident rates and no claims of interviews conducted by the authors.

Quality was assessed in terms of the claims made: transparent methodology, appropriate unit of analysis, stated limitations and how much the conclusions went beyond the data. Case studies and computational examples can demonstrate feasibility without necessarily proving generalisable effectiveness. Surveys can identify associations without being able to prove accident prevention. The sources referenced in the report (via DOI) were all verified in the bibliographic search but full independent reproduction of all the underlying analyses was beyond the scope of the work. The synthesis that is presented is therefore intended to be of use in forming informed hypotheses and in making implementation decisions rather than to be a certification of the performance of any particular installation.

Interpretation was very sensitive to the evidence hierarchy. An observed association between a management practice and the survey responses was not presented as evidence of fewer catastrophic incidents. Engineering simulations were not simply discarded because they didn't involve any of the people in the workplace; they were used to explain the failure pathways and to establish the conditions under which future testing could be conducted. Findings which were in conflict in terms of emphasis were all retained as boundary conditions. This approach helps to avoid the risk of taking a heterogeneous body of evidence and turning it into a false sense of a single, homogeneous consensus.

UNDER PEER REVIEW IN IJAR

4 Conceptual foundations

Resilience of critical infrastructure goes well beyond resistance to physical damage. A system may be perfectly able to protect its own assets and yet be unable to provide the required service as a result of the unavailability of spares, communications, operators or downstream customers. The evidence reviewed describes resilience in terms of an interplay of technical, organisational and service performance characteristics (although the definitions and the boundaries of what is being measured vary considerably [5]). Indicator studies have also demonstrated that organisational capacity, the nature of the disruption and the restoration process must be considered as much as the physical integrity of the system [6]. For the purposes of governance this means that the operator must define the function to be protected, the level of degradation that is acceptable and the recovery objective before they can even consider what indicators to use. A resilience claim that makes no reference to service and to disturbance is meaningless.

Criticality is inherently relational. A fairly simple utility can be absolutely critical if a large number of assets rely on it and there is no readily available substitute capacity. The infrastructure reviews set out identification criteria that take into account the social, environmental and functional impacts [7]. Interdependency modelling shows why a facility based assessment is likely to underestimate the extent of cascading risk as the electricity, water, transport and information services all share both vulnerabilities and benefits [8]. Reviews of compound threats also point to the fact that models tend to focus on the capacity to absorb and recover from a disruption, with much less emphasis on the need for preparation, adaptation and social coordination [9]. A robust HSE assessment therefore has to be concerned with the initiating hazard, the pathway by which it propagates and the institutions which are responsible for the shared countermeasures.

Process safety resilience presents a rather different methodological problem. A review of the literature suggests there are a number of different approaches to assessing and managing resilient technical systems [10]. Quantitative work in this area has therefore argued for the use of

UNDER PEER REVIEW IN IJAR

disturbance, functionality and performance trajectory rather than a single unexplained resilience score [11]. In the framework under discussion loss prevention is absolutely fundamental; adaptability does not equate to being able to operate outside the engineered limits. A useful decision model will be one that can clearly differentiate between measures that reduce the likelihood of an event occurring and those that reduce the potential for escalation, preserve the minimum safe operating state or facilitate a rapid controlled recovery. That is the only way in which resilience language can be used without it simply being a way of hiding poor primary prevention.

The organisational literature provides another explanation. Resilience engineering reviews identify anticipation, monitoring, response and learning as capabilities which need to be evidenced through practice [12]. In the context of chemical plants, safety barrier research requires performance measures which relate to the protective functions, availability and adaptability of the barriers [13]. Research into maintenance environments also finds a link between resilient performance and the interaction between people, place and management systems [14]. The common thread is that you can't assess technical safeguards and human performance in isolation when work is being carried out in an uncertain environment. Resilience should not therefore be viewed as simply the ability of the workforce to make up for the deficiencies of the equipment or the lack of staff.

Research into construction safety indicates that large projects are no more likely to have robust adaptive practices than small projects; you have to look at the evidence of monitoring, anticipation and learning directly [15]. The same applies to offshore culture assessment where the value of triangulation (interviews, field observation, incident learning, leading indicators and management system review) is clear and a single survey should not be the final word [16]. Research into offshore fatigue shows just how easily apparently stable levels of procedural compliance can mask the very real pressures on the operational side which the supervisor will find extremely difficult to detect [17]. All of this underpins the need for a governance model in which frontline intelligence is able to challenge the assumptions of the executive and in which

UNDER PEER REVIEW IN IJAR

assurance looks at the conditions of work rather than just at the documents that have been produced.

5 Saudi operating context and the principal governance problem

Saudi industrial infrastructure is a very diverse risk landscape covering hydrocarbon processing, utilities, desalination, ports, industrial transport and the various construction interfaces. The governance scale is often much broader than just one employer as you have shared contractors, energy supplies, emergency routes and communications. Saudi construction research has shown that the regulatory regime can have an effect on how risk factors are translated into actual management practices, although the findings from individual sectors don't necessarily provide any indication of a uniform national performance [18]. The framework takes local legal requirements, client standards and permit conditions as mandatory inputs to the asset specific governance register. It does not suggest that one single matrix is sufficient to achieve legal compliance.

Environmental exposure has to be viewed as an industrial systems problem too. A recent study on Gulf coastal resilience identifies heat, flooding and sea level rise as the relevant hazards for the region [19]. The mechanism of industrial governance is not simply about the direct damage of the weather. Ambient conditions can have a simultaneous effect on outdoor work, electrical reliability, transport access, cooling demand and the ability to mobilise in an emergency. Climate scenarios should therefore be assessed in terms of their impact on the ability to maintain critical functions within safe operating envelopes. An emergency plan which has only been validated against a single failure may in fact give a false sense of security when heat, utility disruption and reduced workforce availability all occur at the same time.

Three practical tensions arise. One is that the production schedule is all about throughput and will in many cases incentivise you to go ahead and do things, whereas the major hazard

UNDER PEER REVIEW IN IJAR

governance side of things will at times require you to allow for delay, a shutdown or a redesign. The second is that contractors will be very much aware of the changing conditions on the ground but may not have the standing to challenge a plan that has been approved by the owner. The third is that digital monitoring gives you a massive amount of information, but that doesn't necessarily mean you have a better understanding of who needs to act. Risk based governance is the mechanism for dealing with those tensions. You need to have decision thresholds established in advance of the pressure coming on, you need to have the responsibilities clearly traceable across organisational boundaries and you need to have the exceptions visible to independent oversight. It's all about the quality of the decisions you make under constraint rather than the quantity of risk registers you produce.

Another issue of context is the geographical extent of an emergency. Industrial networks span municipal and administrative boundaries whereas the immediate response resources may be purely local. Governance will therefore need to pre-determine who exchanges notifications with whom, who has the authority to confirm the status of shared services and who has the standing to challenge a proposed restart. This is relevant even in the case of no major release as a prolonged loss of industrial water or electricity could well have the effect of transferring risk onto the public services which are dependent upon them.

6 Synthesis: six mutually dependent governance functions

Strategic accountability starts with a board approved statement of risk appetite which clearly distinguishes between intolerable life safety and environmental consequences and commercial losses which are acceptable to take. The executives need to identify the services whose failure would have wider societal implications, assign accountable asset owners and require written justification for any significant deviation. It's not acceptable to just hand the whole thing over to the HSE department. The technical authority responsible must have the power to require additional protection or to call a suspension of operation and the corporate risk committee must be aware of the exposure to dependency, the cumulative effect of deferrals and the cost of the

UNDER PEER REVIEW IN IJAR

various resilience options. Effective escalation is about turning engineering evidence into a decision rather than simply an observation.

System wide risk intelligence requires a living map of the physical and organisational dependencies. Every safety critical function must be linked to its utilities, its control architecture, its specialist staff, its vendors, its access routes and its credible external threats. The assessment must include low probability, high consequence events, simultaneous failures, planned maintenance and degraded modes. Risk ranking by itself is not enough. For each estimated consequence you need to identify the assumption upon which it is based and state what would invalidate that assumption. A useful register is dynamic and should record changing operating conditions, weak signals and uncertainty as well as risk treatment decisions. Ownership of the register should be with operations and engineering with HSE providing the structured challenge.

Verified barrier integrity is the key to demonstrating that a safeguard is present as opposed to merely that it will perform its safety function when required. The barrier inventory should be multi-layered and cover prevention, detection, isolation, containment, emergency protection and environmental mitigation. The owner must define the operating limits, the proof test intervals, the response to impairment, the bypass authority and the compensatory measures. The barrier information should include unavailability due to maintenance backlogs, shared power systems or unreliable instrumentation. A small number of protections being unavailable can become very consequential if they are subject to the same common cause. The governance therefore needs to look at the correlated impairments rather than simply at the aggregate of the nominal inspection completion percentages.

Workforce participation is a source of operational intelligence rather than just a consultation exercise. There should be mechanisms in place that allow workers and contractors to report things such as incomplete permits, heat, fatigue, conflicting instructions and unexpected configurations without fear of reprisal. Supervisory decisions should record how the issues were dealt with, including any instances where production was changed as a result. Competence

UNDER PEER REVIEW IN IJAR

should be scenario specific: a worker who is competent in the normal operation of a system may well not be competent in the diagnosis of an abnormal control response. Language access, quality of shift handover and contractor mobilisation are all factors which will impact on the reliability of the safeguards and must be considered in that context, especially where there are multiple employers on site.

Adaptive emergency capability is incorporated into the command arrangements for restoration planning. Emergency exercises will need participants to make choices between controlled shutdown, isolation, sheltering, evacuation, alternative supply and phased restart under the scenario of impaired communications. Restoration is not simply about getting back to output as quickly as possible; a premature restart could in fact turn a contained incident into a major accident. The recovery criteria must include a safe system state, verified protective functions, environmental clearance, available staffing and agreed interface conditions with the operators of any dependent systems. The exercises will be designed to test the assumptions under those criteria, including how decisions will be communicated to the public responders and to the owners of adjacent infrastructure.

Independent learning closes the governance loop. Reviews of incidents, near misses, precursor conditions and successful recoveries should be looking at why the decisions that were made at the time were the right ones rather than just looking at the individual as the source of error. The assurance team need to check that the recommendations made previously have in fact changed what is actually done. They also need to determine whether good performance is the result of actual risk reduction or is simply due to under-reporting, unusually benign circumstances or a temporary workaround. Learning becomes strategic when the patterns of repeated deferrals, control bypasses and dependency failures actually impact on the capital plans, the terms of the contract and the incentives for leadership. Without that feedback risk based governance slowly becomes yet another documentation exercise.

UNDER PEER REVIEW IN IJAR

These six functions are interdependent. Accountability without trustworthy operating intelligence leads to absurdly tolerant statements; intelligence without barrier verification becomes a very sophisticated form of prediction; barriers without workforce involvement are invisible; response plans without cross-operator coordination will underestimate the extent of cascading loss; and learning without decision authority will fail to change the investments. A mature programme doesn't score the individual functions and then take an average. It will identify the weak links that can negate otherwise good performance and will have named decision owners to deal with those. Table 1 takes the synthesis and turns it into auditable evidence and the associated governance tests.

The order in which improvements are funded is important. You need to start by identifying the exposures that have both high consequence and a lack of (or poor) independent protection. From there you prioritise risk elimination, robust engineering changes and reduced dependency concentration before you go any further and start buying more dashboards. Where you have two controls that are equally good, you want to prefer the one whose failure state is visible, whose failure can be tested and whose maintenance is sustainable. The point is not to have maximum redundancy everywhere, it's to have defensible protection at the interfaces where failure could potentially propagate.

Table 1. Governance functions, evidence requirements and assurance questions.

Governance function	Evidence required	Primary assurance question
Accountability	Critical services; risk limits; named authorities	Can serious exceptions change production or investment decisions?
Risk intelligence	Dependency map; credible concurrent scenarios	Are shared utilities, contractors and changed conditions represented?
Barrier integrity	Functional standards; test	Can essential protections

UNDER PEER REVIEW IN IJAR

	history; impairment log	perform when called upon?
Workforce participation	Reports; competence tests; handover quality	Can weak signals be raised and resolved without retaliation?
Emergency adaptation	Joint exercises; command rules; restart tests	Can safe recovery occur with services and communications degraded?
Independent learning	Trend reviews; action verification; capital changes	Do lessons produce observable changes beyond document closure?

7 Proposed risk-based HSE governance framework

The proposed model has three tiers. At the strategic level there is an Industrial Infrastructure Risk Council which defines service criticality, intolerable harms, investment priorities and inter-operator responsibilities. At the asset level the technical authorities are responsible for hazard scenarios, dependency maps and performance specifications for safety critical barriers. At the operational level the supervisors and operators are responsible for monitoring the live situation, escalating deviations and carrying out safe state actions. Information flows both ways with the executives providing the resources and the decision limits and the field evidence being able to require an escalation or lead to a change in the strategic assumptions. Figure 1 shows the accountability relationships and the points at which independent assurance must be brought in.

The framework is implemented via a recurring 7 step decision sequence: define the essential service; establish the hazard and dependency context; identify the intolerable consequences; select and verify the preventive and mitigative controls; define the action thresholds and intervention authority; rehearse the disruption and restoration decisions; and then revise the assumptions based on operational evidence. Each step has a defined output and a named owner. The sequence is deliberately cyclical as the infrastructure configuration, the contractor

UNDER PEER REVIEW IN IJ

arrangements and the environment all change. Figure 2 illustrates the feedback loop from scenario intelligence through to field decisions, assurance and capital allocation.

Performance measurement should be a combination of the three indicator families. Exposure indicators would cover hazardous operating hours, number of simultaneous operations and dependency concentration. Control indicators would measure the availability of specific controls, number of unresolved test defects, number of overdue protective maintenance actions and the time taken to resolve material impairments. Capability indicators would measure the ability to recognise abnormal situations, decision latency, ability to communicate effectively under degraded conditions, controlled recovery time and the quality of lessons learned. A composite score should not hide a failure of a high consequence barrier and individual critical exceptions must be visible. Where a quantitative estimate is used there must be an associated uncertainty range and failure dependencies.

Recent work on resilience indices points to the value of looking at the causal links between the various indicator components rather than just using the standard weighted scores [20]. Quantitative process system models have also shown that the way in which failures propagate across human and technical functions can alter the time profile of service loss [21]. These are all very promising approaches, but the proposed framework doesn't specify some unproven national threshold. Rather it would be for each operator to define a small number of scenario-specific measures and then demonstrate through independent challenge that their chosen thresholds are in fact indicative of real protection and real recovery capability.

Assurance roles must remain separate from operational ownership. Ops own the plant condition; Engineering own the technical adequacy; HSE own the way the human and environmental consequences are represented; independent assurance then test the overall case. Where there is overlap of functions, a separate reviewer should be looking at the key decisions and the unresolved intolerable hazards.

UNDER PEER REVIEW IN IJAR

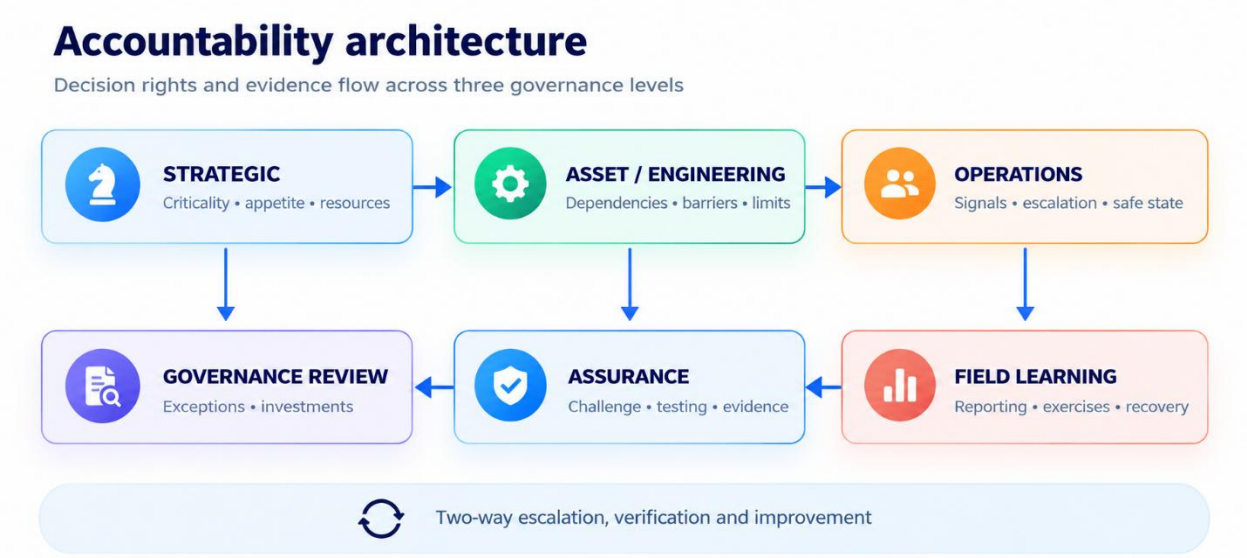


Figure 1. Three-level governance architecture with independent assurance and two-way field intelligence.

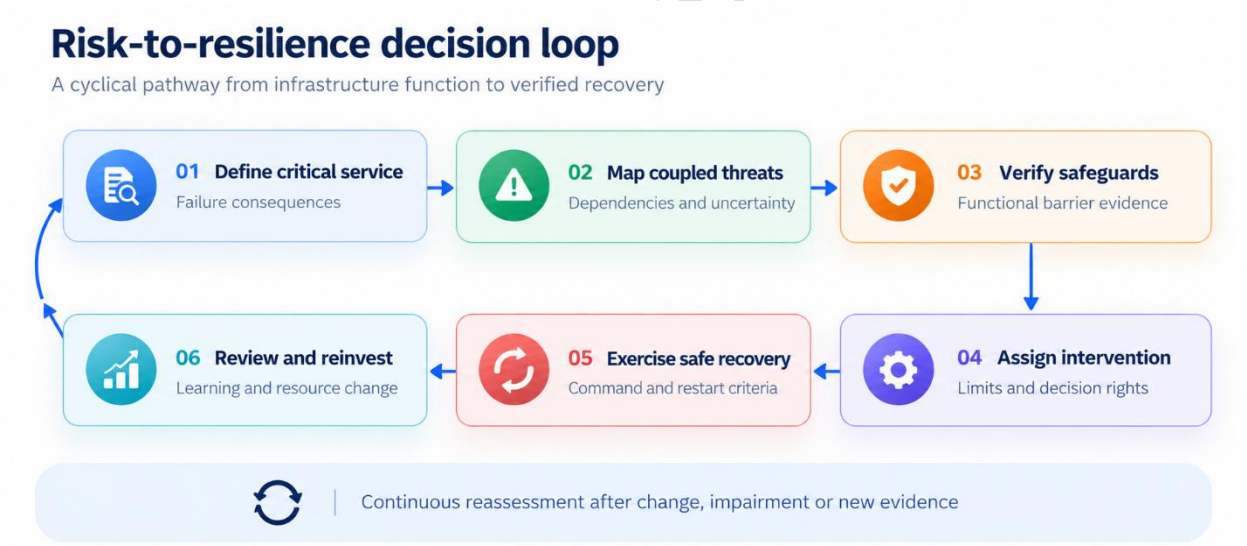


Figure 2. Proposed iterative sequence for critical-service protection, intervention and verified recovery.

8 Digital assurance, automation and the limits of prediction

Digital systems can be a force for good in terms of governance in that they can provide trustworthy evidence of control performance. Research into digital twins has identified applications in safety assessment and in emergency management, as well as pointing to issues of interoperability, modelling uncertainty and security [22]. Application of predictive methods to industrial resilience has shown that useful inference is contingent upon the quality of the data, the transparency of the assumptions and the care with which incomplete observations are interpreted [23]. Reinforcement learning studies have demonstrated the potential for the identification of prospective intervention strategies for chemical processes, though it is clear that successful simulation of a scenario does not in itself justify the implementation of an intervention in the real world without appropriate domain validation and with human oversight [24]. The lesson is that technological sophistication must always be secondary to the safety case and to operational authority.

The problem is especially pronounced when natural hazards impact industrial plant. The recent reviews of technological accidents arising from natural hazards all point to the need to marry resilience with major accident scenarios [25]. Simulation on digital twins also shows how the various stages of risk management can be assisted by virtual models, as long as the outputs from the models are treated as decision support rather than as a demonstration of safety [26]. A more specific example of the utility of such an approach is work on tunnel fire systems which shows the benefit of linking in sensor observations, prediction and emergency visualisation [27]. The applicability of such an approach is of course only going to be transferable once you've looked at the data on data completeness, sensor failure modes, network dependence and the differences in operating context.

For a Saudi operator the practical assurance path starts with a well defined use case (detect an impaired barrier, anticipate an unsafe interaction, support emergency information exchange). The next questions are who will validate the model, who will act on the alert and what happens if the

UNDER PEER REVIEW IN IJAR

data is late, inconsistent or missing. Cyber compromise, contractor access and the common mode of cloud dependence all need to be part of the hazard analysis. Any decisions which would change the conditions for emergency isolation, evacuation or restart will need to be subject to a specified human approval and be logged in a traceable manner. Digitalisation only delivers resilience if the organisation is still able to act safely in the absence of the digital tool.

9 Application across asset lifecycles and scenarios

The framework is relevant right through the lifecycle of the system; before construction, during commissioning, throughout operation and at the time of major modification. The earliest opportunity to deal with dependencies or to provide physically separated reserves is in the design phase. Commissioning is the opportunity to test that the ownership of the barriers, the operational procedures and the emergency interfaces survive the transition from the project team to the permanent operator. Operational governance then has to deal with maintenance deferrals, concurrent activities and temporary workarounds. At the time of modification, configuration management should go back to the original criticality assumptions rather than simply assume that any new system which is connected will inherit an acceptable risk profile.

The Saudi tunnel work illustrates the range of confined space, ventilation, fire, electrical and emergency planning hazards that can exist in one project [28]. Work in the oil and gas sector also suggests that safety culture and the way the organisation is set up are important in the face of a significant health threat (though again the small sample sizes of the observational studies preclude any broad causal inferences) [29]. This helps to separate out the sector specific protective measures from the more general governance requirements. Table 2 provides some scenario based decisions for different industrial settings. The examples in the table are applications of the synthesis rather than any actual measured frequencies of incidents or any empirical ranking of the Saudi facilities.

UNDER PEER REVIEW IN IJAR

Infrastructure resilience should be built into procurement and contracting. The contract can assign responsibility for interface testing, incident information exchange, critical spares and joint exercises and at the same time protect the right to stop work if it is unsafe. Performance based contracting has to be done with care as a contract which rewards low numbers of reported injuries could have the effect of discouraging transparency. The supplier should be rewarded on the basis of evidence of barriers, competence, closure of serious defects and willingness to provide dependency information. The contract should also define how the contractor's digital systems will interface with the owner's incident command structure, particularly in the event of an outage when the normal access arrangements will not be available.

Table 2. Illustrative disruption scenarios and priority governance decisions by asset class.

Infrastructure setting	Credible combined disruption	Priority decision evidence
Hydrocarbon processing	Loss of power with abnormal pressure	Protective-system independence; safe isolation; verified restart
Power and industrial utilities	Simultaneous load and cooling constraint	Critical load hierarchy; reserve supply; operator coordination
Desalination and water networks	Intake or electricity disruption	Quality safeguards; redundancy; customer priority and restoration
Industrial ports and logistics	Hazardous cargo incident with blocked access	Mutual notification; access alternatives; joint emergency command
Tunnels and industrial transport	Ventilation failure during smoke event	Detection integrity; safe evacuation; responder communication

UNDER PEER REVIEW IN IJAR

10 Discussion and implications

The review makes a clear distinction between organisational preparedness and demonstrated resilience. Preparedness is what the operator says they will do; resilience is what the connected system is actually able to maintain, contain and recover from when the assumptions are stressed. This is important for regulators, for board reporting and for infrastructure investment. Asset reliability metrics are still useful, but resilience also depends on escalation authority, the skill of the people on site, the public consequences of an incident and the performance of the third party networks. A good safety record in itself does not prove that the system is adequately protected against a very rare catastrophic scenario.

The framework also makes very clear what risk based governance is not. It is not a mechanism to allow you to substitute cost benefit analysis for your statutory duties to protect. It is not a justification for passing on the risk of work to contractors or to the communities around you. Where you have high severity hazards you need to have clear limits, you need to have documented technical justification and you need independent review. Resilience investment should ideally be about eliminating the source of vulnerability before you go down the route of having to have emergency workarounds. Early design research into process systems has shown the value of looking at the potential for severe impacts and the level of design vulnerability prior to construction locking in the costs of the various dependencies [30]. This is a view of HSE as a contributor to industrial reliability rather than one of uninterrupted production.

Implementation requires institutional differentiation. At board level the relevant question is whether the exceptions and concentrations of dependency are visible before they become emergencies. At plant level it's whether the protective functions work when challenged and whether degraded operation is controlled. At workforce level it's whether people can report a

UNDER PEER REVIEW IN IJAR

change that will affect a decision without fear of reprisal. At interface level it's whether the utilities, the local responders and the neighbouring operators all have a reasonably accurate picture of how failure will propagate. Those questions take the broad ambition of resilience and turn it into a set of decisions that can be reviewed, tested and where appropriate, reversed.

11 Research agenda and limitations

Prospective evaluation should involve a before and after comparison of the participating sites as a result of the governance changes, using consistent definitions of major barrier impairment, abnormal condition escalation and time to safe recovery. Multi-site designs should look at asset type, contractor dependency, climate exposure and the maturity of the management systems. Scenario based exercises could be used to assess whether a joint command arrangement reduces decision delay in the event of a shared utility failure. Qualitative interviews should be used to look at the conflicting incentives and the circumstances under which workers do report weak signals. The research should also look at whether the addition of further sensors leads to any improvement in intervention quality or simply results in a larger volume of unprocessed alarms.

The review has significant caveats. It's based on a deliberately constructed set of 30 recent DOI identifiable publications rather than a fully replicated database wide search and so cannot claim to be publication complete. A lot of the evidence comes from outside the Saudi industrial context and the results from construction, healthcare and offshore applications would not be directly transferable to a petrochemical facility. The proposed relationships are purely conceptual with no original facility data, no expert panel, no field trials and no validation of threshold values. Any claims of effectiveness, journal acceptance or verified similarity scores would be premature. Local regulatory applicability would need to be confirmed on a per asset basis.

UNDER PEER REVIEW IN IJAR

12 Conclusion

The resilience of Saudi Arabia's critical industrial infrastructure cannot be achieved through a series of isolated HSE (Health, Safety and Environment) procedures or by monitoring injury statistics. It is dependent on a decision making system which takes into account the inter-connectedness of services, can identify the consequences that are simply intolerable, can verify the protective barriers in place, can incorporate the intelligence of the workforce and can co-ordinate restoration across asset boundaries. This paper reviews the recent literature to distil six governance functions and a cyclical implementation framework which links strategic accountability with operational evidence. The key practical test is whether a credible signal of a deteriorating level of protection can lead to the timely and appropriate action to be taken before a disruption becomes a cascading crisis.

The framework is in essence a transparent starting point for adaptation rather than a certified operating procedure. Its value is in the traceability of each decision: what function is the primary one, what scenario is the threat to that function, what mitigations are being relied upon, who has the authority to intervene and what evidence is required to restart. Future Saudi case studies should look at whether this level of traceability actually leads to improved safety and recovery outcomes in the face of real world combined threats. That would be the point at which risk based HSE governance moves from a defensible concept to an empirically validated capability for infrastructure management.

UNDER PEER REVIEW IN IJAR

References

1. Qureshi MMR (2023) Building proactive organizational resilience against the risk of major process safety incidents. Process Safety Progress 42(1):48–55. https://doi.org/10.1002/prs.12411

2. Choudhry RM, Zafar I, Almatawa MS (2023) Proactive approach to measure safety management on building projects in Saudi Arabia. Advances in Civil Engineering 2023:6306157. https://doi.org/10.1155/2023/6306157

3. Kelíšek A, Studená J, Buganová K, Hudáková M (2025) The degree of risk management implementation in enterprises in the Slovak Republic. Systems 13:427. https://doi.org/10.3390/systems13060427

4. Farshad AA, Yarmohammadi S, MotalebiGh M, et al (2025) A systematic model for health systems to prevent and respond to health emergencies in the workplace. BMC Health Services Research 25:1585. https://doi.org/10.1186/s12913-025-13693-7

5. Mottahedi A, Sereshki F, Ataei M, Qarahasanlou AN, Barabadi A (2021) The resilience of critical infrastructure systems: A systematic literature review. Energies 14:1571. https://doi.org/10.3390/en14061571

6. Osei-Kyei R, Almeida LM, Ampratwum G, Tam VWY (2022) Systematic review of critical infrastructure resilience indicators. Construction Innovation 23(5):1210–1231. https://doi.org/10.1108/CI-03-2021-0047

7. Rathnayaka B, Siriwardana CSA, Robert D, Amaratunga D, Setunge S (2022) Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. International Journal of Disaster Risk Reduction 78:103123. https://doi.org/10.1016/j.ijdrr.2022.103123

8. Sun W, Bocchini P, Davison BD (2022) Overview of interdependency models of critical infrastructure for resilience assessment. Natural Hazards Review 23(1). https://doi.org/10.1061/(ASCE)NH.1527-6996.0000535

UNDER PEER REVIEW IN IJAR

9. Wells EM, Boden M, Tseytlin I, Linkov I (2022) Modeling critical infrastructure resilience under compounding threats: A systematic literature review. Progress in Disaster Science 15:100244. https://doi.org/10.1016/j.pdisas.2022.100244

10. Chen C, Li J, Zhao Y, Goerlandt F, Reniers G, Liu Y (2023) Resilience assessment and management: A review on contributions on process safety and environmental protection. Process Safety and Environmental Protection 170:1039–1051. https://doi.org/10.1016/j.psep.2022.12.072

11. Yang M, Sun H, Geng S (2023) On the quantitative resilience assessment of complex engineered systems. Process Safety and Environmental Protection 174:941–950. https://doi.org/10.1016/j.psep.2023.05.019

12. Ranasinghe U, Jefferies M, Davis P, Pillay M (2020) Resilience engineering indicators and safety management: A systematic review. Safety and Health at Work 11(2):127–135. https://doi.org/10.1016/j.shaw.2020.03.009

13. Yuan S, Yang M, Reniers G, Chen C, Wu J (2022) Safety barriers in the chemical process industries: A state-of-the-art review on their classification, assessment, and management. Safety Science 148:105647. https://doi.org/10.1016/j.ssci.2021.105647

14. Pilanawithana NM, Feng Y, London K, Zhang P (2022) Developing resilience for safety management systems in building repair and maintenance: A conceptual model. Safety Science 152:105768. https://doi.org/10.1016/j.ssci.2022.105768

15. Bhattacharjee K, Bugalia N, Mahalingam A (2024) An analysis of safety practices for small, medium, and large construction projects: A resilience engineering perspective. Safety Science 169:106330. https://doi.org/10.1016/j.ssci.2023.106330

16. McSweeney K, Curry J, Curtis R, et al (2023) Development of a comprehensive multi-component toolkit for offshore safety culture assessment. Process Safety and Environmental Protection 175:78–87. https://doi.org/10.1016/j.psep.2023.05.030

17. Wang X, Sasangohar F, Payne S, Mehta RK (2024) Safety culture and worker fatigue management in the offshore oil and gas industry: An interview study. International Journal of Industrial Ergonomics 102:103614. https://doi.org/10.1016/j.ergon.2024.103614

UNDER PEER REVIEW IN IJAP

18. Rehman MA, Ishak MSB, Adeleke AQ (2024) The moderating effects of statutory laws and regulations of risk factors and management in the Kingdom of Saudi Arabia construction industries. Business, Management and Economics Engineering 22(1):53–76. https://doi.org/10.3846/bmee.2024.19883

19. Almheiri A, Montenegro JF, Ewane EB, Mohan M (2024) Climate change hazards and the resilience of coastal cities in the Gulf Cooperation Council countries: A systematic review. City and Environment Interactions 24:100177. https://doi.org/10.1016/j.cacint.2024.100177

20. Amer L, Erkoc M, Celik N, Andiroglu E (2023) Operationalizing resilience: A deductive fault-driven resilience index for enabling adaptation. Process Safety and Environmental Protection 177:1085–1102. https://doi.org/10.1016/j.psep.2023.07.082

21. Sun H, Yang M, Wang H (2024) An integrated approach to quantitative resilience assessment in process systems. Reliability Engineering & System Safety 243:109878. https://doi.org/10.1016/j.ress.2023.109878

22. Zio E, Miqueles L (2024) Digital twins in safety analysis, risk assessment and emergency management. Reliability Engineering & System Safety 246:110040. https://doi.org/10.1016/j.ress.2024.110040

23. Vairo T, Pettinato M, Reverberi AP, Milazzo MF, Fabiano B (2023) An approach towards the implementation of a reliable resilience model based on machine learning. Process Safety and Environmental Protection 172:632–641. https://doi.org/10.1016/j.psep.2023.02.058

24. Szatmári K, Németh S, Kummer A (2024) Integration of resilience engineering and reinforcement learning in chemical process safety. Process Safety and Environmental Protection 181:343–353. https://doi.org/10.1016/j.psep.2023.11.027

25. Valente M, Ricci F, Cozzani V (2025) A systematic review of resilience engineering applications to Natech accidents in the chemical and process industry. Reliability Engineering & System Safety 255:110670. https://doi.org/10.1016/j.ress.2024.110670

26. Virando GE, Lee B, Kee SH, Yee JJ (2024) Digital twin simulation and implementation in safety risk management process. IEEE Access 12:195671–195695. https://doi.org/10.1109/ACCESS.2024.3519704

UNDER PEER REVIEW IN IJAP

27. Zhang X, Jiang Y, Wu X, et al (2024) AIoT-enabled digital twin system for smart tunnel fire safety management. Developments in the Built Environment 18:100381. https://doi.org/10.1016/j.dibe.2024.100381

28. Baghdadi A (2024) Evaluation of safety management during tunnels construction in Saudi Arabia. International Journal of Engineering Technologies and Management Research 11(4). https://doi.org/10.29121/ijetmr.v11.i4.2024.1449

29. Guzman J, Recoco GA, Pandi AW, Padrones JM, Ignacio JJ (2022) Evaluating workplace safety in the oil and gas industry during the COVID-19 pandemic using occupational health and safety vulnerability measure and partial least square structural equation modelling. Cleaner Engineering and Technology 6:100378. https://doi.org/10.1016/j.clet.2021.100378

30. Vesey F, Hoseyni SM, Cordiner J (2023) Development of an industrially applicable model for the qualitative resilience assessment of process systems at the early design stage. Journal of Loss Prevention in the Process Industries 86:105199. https://doi.org/10.1016/j.jlp.2023.105199

UNDER PEER REVIEW IN IJAR