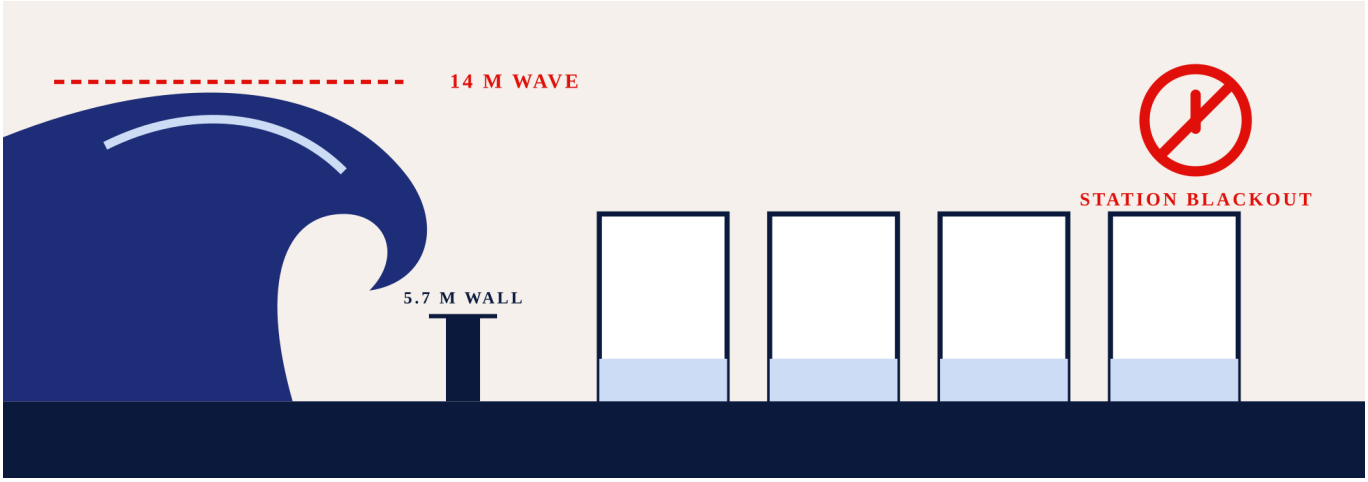


Fukushima Daiichi, 2011: a 5.7 m wall and a 14 m wave

A reliability and asset management reading of the nuclear accident, with five practical checks for owners of critical plant

Published by AFDARA & Co. · Version 1.0 · November 2026 · linkedin.com/company/afdara-co

ABSTRACT

On 11 March 2011 a magnitude 9 earthquake and the tsunami that followed struck the Fukushima Daiichi nuclear power plant in Japan. Waves over 14 m overtopped defences designed for 5.7 m and knocked out almost all power [1]. Cooling was lost, cores were damaged and radioactive material was released; more than 100,000 people were evacuated [2][6]. Japan's Diet commission called it "a profoundly manmade disaster" [3]. We review the case with a bow-tie view, a contributing-factor map, RCM and an ISO 55001:2024 lens, and turn it into five checks.

KEY FINDINGS

1. The tsunami hazard was underestimated, with insufficient defence in depth [1].
2. Since 2006 the regulator and operator knew a site-level tsunami could cause a total loss of power [3].
3. Preparation assumed that an extended station blackout would not happen [4].
4. The commission found "regulatory capture" and organisational root causes [3].

The accident was ultimately rated INES Level 7, the highest category on the International Nuclear and Radiological Event Scale [2]. UNSCEAR's 2020/2021 assessment found no adverse health effects among Fukushima residents that could be directly attributed to radiation exposure; evacuation and prolonged displacement created separate health and social risks, especially for vulnerable patients and older people [11][12][13].

01 Context and purpose

Fukushima Daiichi, operated by Tokyo Electric Power Company (TEPCO), had six reactor units on the Pacific coast; three were operating on 11 March 2011 [1]. A nuclear plant must keep cooling its reactor cores even after shutdown, which needs electrical power, water and working instruments. This brief is not about nuclear physics. It is about how an organisation treats a hazard it has been warned about.

About this brief. A practitioner interpretation from public sources by AFDARA & Co.; not legal or engineering advice, not peer-reviewed. Figures, evidence check and indicators are AFDARA tools, not taken from the investigation reports.

02 The sequence

The plant did what it was designed to do. The operating reactors shut down automatically when the earthquake was detected, and the emergency diesel generators started as designed [1].

Then the design basis was exceeded. The first large tsunami wave reached the site about 46 minutes after the earthquake. The larger waves were estimated at over 14 m; the defences were designed for a maximum of 5.7 m [1]. The flooding caused the loss of all power sources except

one diesel generator, 6B, with no other significant power on or off site; Units 1–4 lost instrumentation and control [1].

Escalation, unit by unit. The earthquake cut off external power; the tsunami then flooded on-site electrical and heat-removal equipment, causing a prolonged station blackout [1][2]. Cooling then diverged by unit. Unit 1's isolation condenser was not effectively cooling after power loss. At Unit 3, operators manually stopped high-pressure injection after reactor pressure fell while an alternative injection route was still being established; the interruption and delayed adequate injection were specific to that unit [4][10]. Unit 2 followed a different sequence. Hydrogen from severe fuel damage caused explosions that damaged the Unit 1 and Unit 3 buildings; the Unit 4 building was also damaged, likely by hydrogen from Unit 3. Unit 4 did not suffer core damage [2][10]. The NAIIC also noted a possibility that the earthquake itself damaged safety equipment at Unit 1, which could not be fully examined [3].

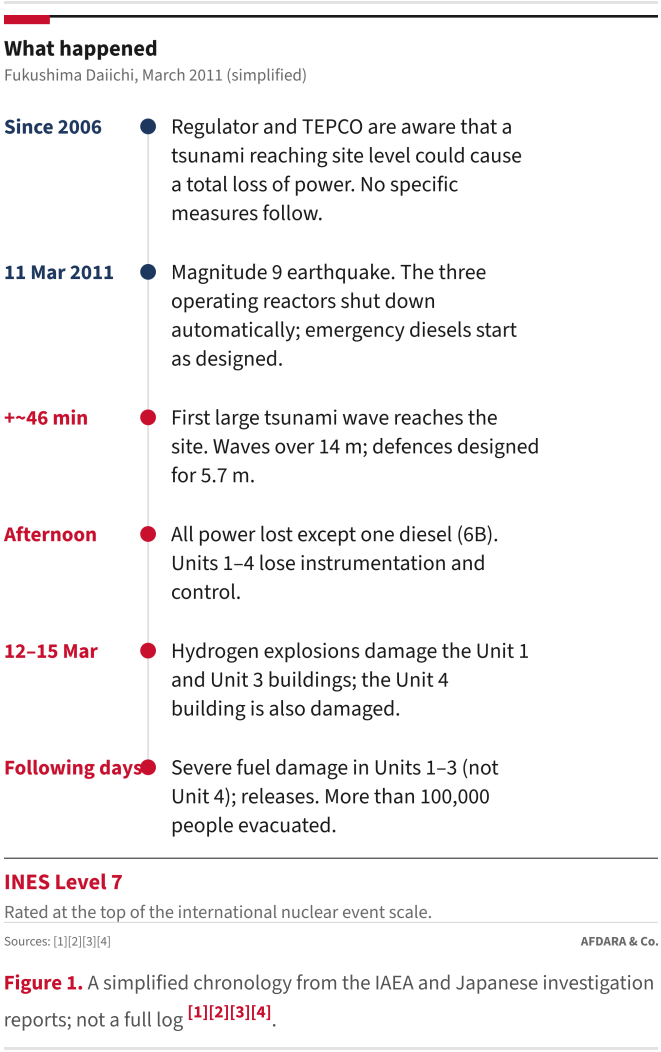


Figure 1. A simplified chronology from the IAEA and Japanese investigation reports; not a full log [1][2][3][4].

03 Reliability and barrier analysis

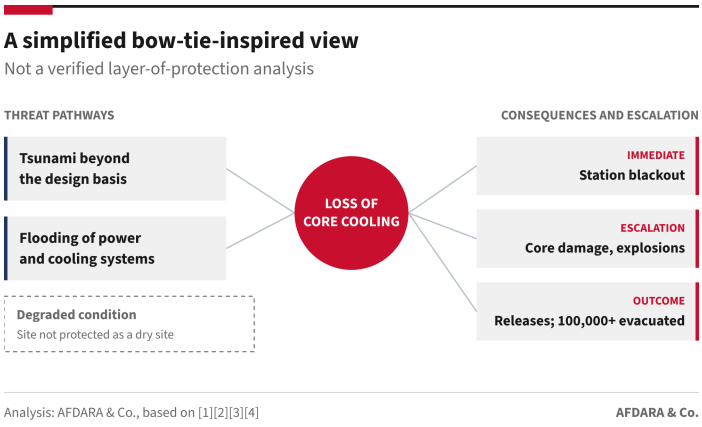


Figure 2. A qualitative cause–consequence sketch, not a probabilistic safety assessment [9]. Controls that failed or were unavailable: *prevention* — a design basis that covered credible tsunamis, a dry site; *mitigation* — protected AC and DC power, alternative cooling ready for use, severe-accident procedures and drills for multiple units [1][2][4].

A common-cause failure. Redundancy works only if the redundant trains do not fail together. One flood took out nearly all power sources at once [1]. The IAEA mission recommended a "dry site" concept where practicable [1].

The design basis was a belief. The IAEA concluded that the tsunami hazard was underestimated and that defence-in-depth provisions for tsunamis were insufficient [1]. Its 2015 report adds that large uncertainties remain in predicting natural hazards, and that people and organisations should continuously challenge the prevailing assumptions [5].

Preparation stopped at the design basis. The government investigation committee found TEPCO had not prepared adequately for tsunami risks beyond the design basis, and that preparations were built on the assumption that an extended station blackout would not happen [4].

04 Contributing causes and organisational learning

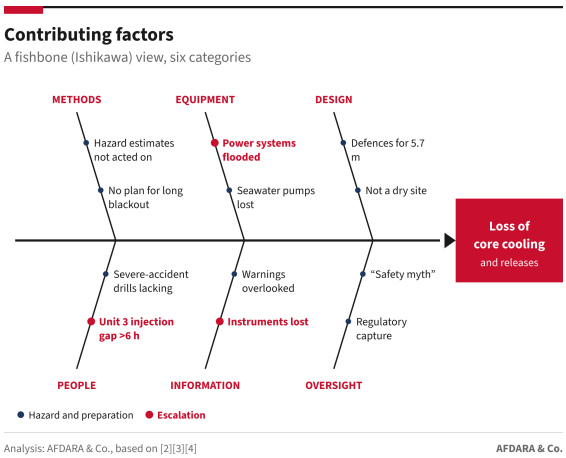


Figure 3. A workshop aid by AFDARA & Co.: a contributing-factor map for structuring discussion. It is a practitioner interpretation, not the investigators' causal analysis [2][3][4].

One selected branch (workshop aid). Why were the cores damaged? Cooling was lost. Why? Nearly all power was lost. Why? Flooding from a tsunami bigger than the design basis. Why was the design basis too low? Warnings were overlooked and the regulator did not require action [1][3]. Real causation had several branches.

Recorded signals. The NAIIC found that since 2006 the regulators and TEPCO had been aware of the risk of a total power outage if a tsunami reached the site level, and that researchers had repeatedly warned of tsunamis above the design assumptions. The regulator knew TEPCO had not prepared measures but gave no specific instructions [3].

Culture and oversight. The NAIIC described "regulatory capture" and placed the root causes in the organisational and regulatory systems, not in any individual [3]. The government committee described a "myth of safety" that serious accidents could never occur [4].

RCM QUESTION	APPLIED TO THE TSUNAMI DEFENCES
1 Function	Keep the site dry up to the design flood.
2 Functional failure	Overtopped by a flood beyond the design basis.
3 Failure mode	Design basis lower than the credible hazard [1].
4 Effect	Flooding of power and cooling systems across several units.
5 Consequence	Safety and environmental: common-cause loss of core cooling.
6 Proactive task	No age-based maintenance task closes the hazard gap; proactive controls are hazard reassessment, inspection of flood pathways and barriers, and interim protection.
7 If no proactive task	Redesign: engineered upgrade of protection and protected backup power.
Operational rule	Separately: when new hazard evidence exceeds the design basis, record the gap and set interim measures and a date.

Table 1. RCM questions (after SAE JA1011 [8]; not a quotation), applied by AFDARA & Co. to the site flood defences. A teaching adaptation, not a JA1011 conformity evaluation; JA1011 sets minimum criteria for a process to be called RCM and does not define one specific process.

> **TAKEAWAY**
>
> Redundancy is not protection if one event can defeat every train. Ask what single event takes out all your backups.

05 A retrospective ISO 55001 lens

Viewed retrospectively through ISO 55001:2024, the case raises questions about context, risk, emergency planning, competence and oversight. These are illustrative questions, not an audit or a finding of nonconformity. ISO 55001 complements rather than replaces nuclear safety regulation and IAEA safety standards [7].

HISTORICAL CONTROL ISSUE IN THIS BRIEF	ILLUSTRATIVE ISO 55001:2024 QUESTION TODAY
External hazard estimate not updated	4.1 Understanding the organization and its context · 6.1 Actions to address risks
New hazard evidence not acted on	9.3 Management review · 10.2 Nonconformity and corrective action
No plan for extended loss of power	8.1 Operational planning and control
Drills did not cover severe, multi-unit events	7.2 Competence
External oversight and escalation	4.2 Interested parties · 5.1 Leadership · 6.1 Risks · 10.2 Corrective action (do not infer a regulator's ISO nonconformity)

Table 2. Selected illustrative mappings [7]. The clauses do not set hazard levels or nuclear safety requirements.

06 A design-basis screen

CONDITION	POSSIBLE EFFECT	SAFER ACTION
New study shows a larger hazard than design	Defences overtopped	Record the gap; interim measures; dated decision
Backup trains share one location or support system	Common-cause loss	Physical separation or protected backup
Procedures assume support systems survive	No plan when they fail	Plan and drill for loss of power, water and instruments
Several units on one site	Staff and equipment overwhelmed	Multi-unit scenarios in plans and drills
Oversight relies on the operator's word	Gaps stay open	Independent review with authority to require action

Table 3. Illustrative condition–effect–action screen; not a safety assessment or regulatory requirement.

Evidence check (AFDARA heuristic). For each critical control, look for evidence that it *exists*, is *understood*, is *implemented* (sampled records and observations) and *performs* under defined conditions. Fukushima Daiichi had defences, redundant power and procedures [1]; the gap was performance beyond the design basis.

07 Five practical checks and risk-linked monitoring

1. **Re-test your design basis.** Review external hazards (flood, storm, heat, earthquake) against current evidence at a set interval [1][5].
2. **Hunt for common causes.** For each backup system, ask what single event would defeat it and its partner [1].
3. **Plan for losing the support systems.** Write and drill procedures that assume no power, no instruments and no normal water [2][4].
4. **Act on warnings with dates.** Log every new hazard warning, the decision taken, the owner and the date [3].
5. **Challenge the assumption.** Hold a yearly session where the team argues against the plant's key safety assumptions [5].

Illustrative indicators

INDICATOR	DEFINITION TO SET	RESPONSE RULE
Design-basis reviews overdue	External hazards not reviewed in the set interval	Schedule review
Open hazard gaps	New evidence above design basis with no closed action	Board-level escalation
Common-cause findings open	Backups sharing a single point of failure	Owner and date
Severe-scenario drills	Drills including loss of power and instruments, per plan	Schedule missed drills
Warnings logged and closed	Hazard warnings with recorded decisions	Review open items

Thresholds and monitoring frequencies are AFDARA heuristics and must be set by risk assessment and applicable regulation, not read as ISO 55001 or statutory limits. Indicators give early warning, not prediction.

QUESTION FOR YOUR TEAM

What single event would take out your main system and all its backups at the same time?

References

1. IAEA (2011). Mission Report: IAEA International Fact Finding Expert Mission of the Fukushima Dai-ichi NPP Accident following the Great East Japan Earthquake and Tsunami, 24 May–2 June 2011. (Copy hosted by Taiwan Nuclear Safety Commission.) nusc.gov.tw
2. IAEA (2015). The Fukushima Daiichi Accident: Report by the Director General and Technical Volumes. STI/PUB/1710. www-pub.iaea.org
3. The National Diet of Japan, Fukushima Nuclear Accident Independent Investigation Commission (NAIIC) (2012). The Official Report: Executive Summary. nirs.org
4. Investigation Committee on the Accident at Fukushima Nuclear Power Stations of TEPCO (2012). Executive Summary of the Final Report, 23 July 2012. cas.go.jp
5. IAEA (2015). Fukushima Daiichi Accident: Report by the Director General, GC-59 side event presentation (Flory). iaea.org
6. IAEA (2015). The Fukushima Daiichi Accident: brochure and Director General's message. iaea.org
7. ISO 55001:2024. Asset management: Asset management system: Requirements. ISO, Geneva. iso.org
8. SAE JA1011_202411 (revised 5 November 2024). Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes. SAE International. doi.org
9. de Ruijter, A. and Guldenmund, F. (2016). The bowtie method: A review. Safety Science 88, 211–218. doi.org
10. National Academies of Sciences, Engineering, and Medicine (2014). Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants, Chapter 4. nationalacademies.org
11. UNSCEAR (2022). UNSCEAR 2020/2021 Report, Volume II: Levels and effects of radiation exposure due to the accident at the Fukushima Daiichi Nuclear Power Station. unscear.org
12. Nomura, S. et al. (2013). Mortality risk amongst nursing home residents evacuated after the Fukushima nuclear accident. PLOS ONE 8(3): e60192. journals.plos.org
13. Tanigawa, K. et al. (2012). Loss of life after evacuation: lessons learned from the Fukushima accident. The Lancet 379(9819), 889–891. thelancet.com