FERC Risk-Informed Decision Making Applied to Digital Protection Systems

Davis Erwin and Heather Torres, *Pacific Gas and Electric*
Dan Hertel, *Engineering Solutions, LLC*
Elaine Munch, *Shell Corporation (Retired)*
David Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Risk-informed decision making (RIDM) is used to identify, analyze, assess, and manage the risk of design choices by better understanding the consequences of failure. RIDM is used by NERC, NASA, FAA, FERC, and NRC. NRC explains it as follows: "We examine both the probability of an event and its possible consequences to understand its importance (risk). In other words, we ask our questions of what can go wrong, how likely it is, and what its consequences might be. The answers guide our requirements and regulatory attention to the issues that are most important to the health and safety of the public and the environment" [1].**

This paper introduces the value of RIDM to improve the reliability of safety- and protection-related energy control systems. Petrochemical, civil, and nuclear success stories illustrate the value of RIDM during design and operations. When applied to digital secondary systems (DSSs) for electric power, it is also useful for both the design of new installations and the operations and modifications to existing systems to satisfy proposed modifications to the NERC Reliability Standard TPL-001-5.1.

I. Introduction

Risk-informed decision-making (RIDM) processes essentially support teams to consider not only technical, business, and security constraints, but also social, safety, and environmental considerations to make choices and meet goals. Risk management requires making decisions about identification, analysis, assessment, control, prevention, mitigation, and communication of risks in a cost-effective way.

In this paper, we present RIDM as a tool to identify, analyze, assess, and manage risk of design choices by better understanding the consequences of failure. RIDM is used by many safety-related organizations, including NERC, NASA, FAA, FERC, and NRC to answer simple but important questions, which NASA describes in [2] as follows:

Risk is operationally defined as a set of triplets:

- The scenario(s) leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage).
- The likelihood(s) (qualitative [such as anticipated component unavailability based on a professional opinion and experience] or quantitative [such as predicted component unavailability based on science and math applied to field data]) of those scenarios.
- The consequence(s) (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur.

It is clear that these scenarios and consequences may not be part of a typical technical engineering design focused on cost, schedule, and performance, which may not adequately consider public safety. For example, the NERC Reliability Standard TPL-001-5.1 is used for "establishing transmission system performance requirements within the planning horizon to develop a bulk electric system (BES) that will operate reliably over a broad spectrum of system conditions and following a wide range of probable contingencies" [3]. It does not fully consider public safety beyond the extent that public safety is adversely impacted by an unreliable BES.

When evaluating risk, it is often a challenge to decide an acceptable level of risk and how to prioritize correcting several issues that represent unacceptable risk. The FAA categorizes risk based on the predicted severity of the consequences of system failure, as shown in Table I. The FAA summarizes severity with respect to passengers as follows from [4]:

- Minor—inconvenience to passengers
- Major—discomfort to passengers
- Hazardous—fatal to a small number of passengers
- Catastrophic—fatal to all passengers

These severity categories are used to specify the level of appropriate resilience and redundancy of the aviation systems [4]. Table I illustrates the present NERC failure metrics for the electric delivery system (EDS) that are simply identified by number rather than impact and ranked by the amount of energy delivery interrupted due to a load-shedding event. Table I illustrates potential failure modes associated with the energy control system (ECS) that could cause the outages. Finally, Table I also illustrates possible additional risk-based metrics that could be added in the future to better illustrate the consequences of power system fault events.

TABLE I FAA AND NERC SEVERITY CATEGORIES [4]

FAA failure metrics		NERC failure metrics			Possible NERC failure metrics	
Severity category	**Passenger symptoms**	**Severity category**	**EDS interruption (MW)**	**ECS fault**	**EDS damage**	**Public safety**
Catastrophic	Fatal to all	5	≥10,000	Loss of process bus communications	$$$$$	Directly fatal
Hazardous	Fatal to few	4	5,000–10,000	Loss of process bus communications	$$$$	Indirectly fatal
Major	Discomfort	3	2,000–5,000	Loss of process bus communications	$$$	Discomfort
Minor	Inconvenient	2	300–2,000	Loss of process bus communications	$$	Inconvenient
—	—	1	<300	Loss of station bus communications	$	Not observed

Presently, an enterprise-wide gas and electric company is using the risk-based portfolio prioritization framework (RBPPF) geared towards the enterprise risk standard, which includes risk reduction, compliance, capacity, reliability, and other objectives. Within the system protection organization, the risk-informed budget allocation (RIBA) scoring methodology is used, which is based on historical data and overall relay health and failure rates.

Table II illustrates the categories for safety, and Table III illustrates the categories for environmental impact associated with RIBA. RIBA is a data-driven RIDM process "to improve transparency and accountability of business through the full integration of risk management, asset management, and investment management processes with the objective of safe, reliable, and affordable electric and gas service" [5].

TABLE II RIBA SAFETY CATEGORIES

Impact level	Safety
Catastrophic (7)	Fatalities: Many fatalities and life-threatening injuries to the public or employees
Severe (6)	Fatalities: Few fatalities and life-threatening injuries to the public or employees
Extensive (5)	Permanent/serious injuries or illnesses: Many serious injuries or illnesses to the public or employees
Major (4)	Permanent/serious injuries or illnesses: Few serious injuries or illnesses to the public or employees
Moderate (3)	Minor injuries or illnesses: Minor injuries or illnesses to many public members or employees
Minor (2)	Minor injuries or illnesses: Minor injuries or illnesses to few public members or employees
Negligible (1)	No injury or illness up to an unreported negligible injury

TABLE III RIBA ENVIRONMENTAL IMPACT CATEGORIES

Impact level	Environmental
Catastrophic (7)	Duration: Permanent or long-term damage greater than 100 years Hazard level/toxicity: Release of toxic material with immediate, acute, and irreversible impacts to surrounding environment Location: Event causes destruction of a place of international cultural significance Size: Event results in extinction of a species
Severe (6)	Duration: Long-term damage between 11 and 100 years Hazard level/toxicity: Release of toxic material with acute and long-term impacts to surrounding environment Location: Event causes destruction of a place of national cultural significance Size: Event results in elimination of a significant population of a protected species
Extensive (5)	Duration: Medium-term damage between 2 and 10 years Hazard level/toxicity: Release of toxic material with a significant threat to the environment and/or release with medium-term reversible impact Location: Event causes destruction of a place of regional cultural significance Size: Event results in harm to multiple individuals of a protected species
Major (4)	Duration: Short-term damage of up to 2 years Hazard level/toxicity: Release of material with a significant threat to the environment and/or release with short-term reversible impact Location: Event causes destruction of an individual cultural site Size: Event results in harm to a single individual of a protection series
Moderate (3)	Duration: Short-term damage of a few months Hazard level/toxicity: Release of material with a moderate threat to the environment and/or release with short-term reversible impact Location: Event causes damage to an individual cultural site Size: Event results in damage to the known habitat of a protected species
Minor (2)	Duration: Immediately correctable or contained within a small area
Negligible (1)	Negligible to no damage to the environment

Previous papers have expounded on the need to understand the impact of nonredundant protection systems via TPL-001-4 standard compliance steady-state and transient stability studies [6]. The proactive use of RIDM may have been useful to improve protection systems in the BES prior to several significant and public recent outages. FERC has documented greater frequency of extreme heat and cold weather events with predicted increasing frequency in the future. Between 2011 and 2023 in the United States at least seven major extreme cold and heat weather events affected the BES to the extent that some amount of load was shed. Load-shedding events during these weather extremes resulted in unacceptable economic impact, risk to life, and loss of life [7]. The consensus among experts suggests that climate change has made future conditions no longer predictable based on historical records. The extreme cold and heat reduce reliability and increase potential for cascading outages and widespread blackouts. Hindsight has led to NERC updating standards, requiring that every protection system installation affecting the primary equipment in the BES be made redundant [7].

As a consequence, among other actions, NERC Reliability Standard TPL-001-5.1 was modified to require redundancy of components and systems, excluding only single points of failure (SPOF) that are adequately monitored and faults that are automatically reported [6].

Protection components of both electromechanical secondary systems (ESSs) and digital secondary systems (DSSs) are subject to modifications to NERC Reliability Standard TPL-001-5.1 that require installing redundant components. Components have been clarified to include a "relay, power supply, [and] communications system associated with protective functions necessary for correct operation of a [communications-aided] protection scheme, and control circuitry required for normal clearing" [6].

Therefore, in reaction to unacceptable availability of primary and secondary power systems during weather-induced times of stress in the past, NERC modifications to Reliability Standard TPL-001-5.1 were subject to enforcement in July 2023. This may require redundant installation for each in-service nonredundant relay, direct current (dc) power supply, communications system, and control circuit (direct communications, wiring, auxiliary and lockout relays). Reliability is a concern for primary system components, including the BES, utility-scale, small-scale, and distribution power system assets. The risk to the BES, as predicted by NERC, is shown by the modifications to TPL-001-5.1 and the quantity of assets that it affects, as shown in Table IV [8] [9] [10] [11] [12] [13].

With multiple protection systems required for many assets, estimates range from one-half million to over one million relays and recloser controls for this subset of assets alone. Therefore, the compliance to future clarifications of TPL-001-5.1 will be formidable due to the quantity of protective devices associated with power system assets itemized in Table IV. The only SPOF components that may be excluded from the redundancy requirement are those with adequate monitoring and reporting of failures so that corrective actions may be initiated [3].

TABLE IV QUANTITY OF DOCUMENTED BES, UTILITY-SCALE, SMALL-SCALE, AND DISTRIBUTION POWER SYSTEM ASSETS

NERC BES transmission circuits	26,330
NERC BES transformers	5,642
NERC BES generators	3,120
Subtransmission circuits	30,295
Non-BES transmission transformers	50,983
Utility-scale generators > 20 MW	4,521
Small-scale generators <= 20 MW	13,649
Utility electric distribution feeders	198,501

II. INTERNATIONAL STANDARDS AFFECTING DSS

IEC 61508 [14] provides guidance about the safety of DSS, specifically process bus (PB) communications as part of the digital trip circuit, the international standard for functional safety for electrical, electronic, and programmable electronic devices. It illustrates the improvement to availability and system safety provided by the automatic fault detecting and self-alarming within a device. Failures that jeopardize the safety of equipment or people due to a device being unavailable to perform its intended function are referred to as dangerous failures. Failure modes that are observable via self-testing are referred to as detectable, while those that are not observable are considered undetectable. Therefore, a dangerous detectable (DD) SPOF failure can trigger an alarm and prompt corrective action and repair. Dangerous undetectable (DU) SPOF failures reduce the reliability of BES and increase the potential for cascading outages and widespread blackouts. Digital devices may be capable of self-testing, self-detecting of faults, and self-announcing of detected faults. For example, DSS field sensing and digital message exchange require several interdependent tasks, including signal digitization, source logic processing, message encoding, source communications processing, message publishing, message transferring, message subscribing, message reception monitoring, receiver communications processing, message decoding, and receiver logic processing. The protection signal transfer, via messages through a communications system or digital control circuit, includes the following subset of tasks:

- Message publication
- Message transfer
- Message subscription
- Message reception monitoring

Reception monitoring makes DD potential faults with alarms that trigger corrective action.

To make the components' protection signal transfer via messages through a communications system or digital control circuit redundant, it is necessary to create one or more additional systems that also perform each of the four tasks. Also, they must provide complete overlap of tasks such that should any component be removed or fail in service, another component will operate and all four tasks will remain completely functional. Particularly relevant to TPL-001-5.1 is the task of message reception monitoring, which needs to exist

in more than one component to be redundant. Two duplicated systems with reduced functionality may act as duplicates but are not redundant. It is important to understand that other standards written for the process industry and adopted by some for use in DSS, such as IEC 62439-3:2021 technologies that are not redundant, have no message subscription delivery monitoring or fault detecting and, therefore, no fault reporting. These technologies do have methods to detect that a potential network path is active, but not that protection signal messages are being delivered, and so they will not satisfy TPL-001-5.1 redundancy or the monitoring and reporting exclusion.

Even though TPL-001-5.1 compliance may only require changes to relays, dc power supplies, communications systems, and control circuits that affect the BES, it may be difficult to know which of those are based on the potential for cascading outages. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico [15]; therefore, each utility in that area is directly affected by this pending modification, and others will be indirectly affected.

Also, it may be important for utilities to optimize the availability of their protection system components to improve safety and performance as the climate and supply mix changes on the grid with distributer- and inverter-based resources.

III. NERC Requirements and RIDM for DSS

RIDM is introduced in this paper as a tool to help prioritize when to implement redundancy or monitoring and reporting to protection system components. RIDM is a tool that emphasizes the proper use of risk analysis for risk-informed decisions impacting technology, cost, schedule, and safety, including loss of life. For example, FERC uses RIDM within dam safety practices to assess the likelihood of hydraulic loading, system response to hydraulic loading, and consequences of failure to estimate risk. This paper explains the use of RIDM and, as an example, applies it to evaluate the design of DSSs, and similarly, the communications-bandwidth loading, system response to message transit affected by the loading, and consequences of failure to estimate risk that a trip signal will be affected.

As with dams, pipelines, aircraft, and spacecraft, RIDM is shown to inform DSS decisions regarding risks associated with technology investments and to improve the understanding of consequences associated with vulnerabilities that have not been identified using other evaluation techniques.

The process enables utilities and stakeholders to evaluate emerging IEC 61850 PB and digital trip circuit designs, including the:

- Mismatch between the utility cost and performance expectations versus the actual resources required to mitigate risks to achieve those expectations.
- Misunderstanding and miscommunication of risks associated with competing alternatives and understanding that product failure is predictable and not simply uncertain.
- Misunderstanding that the relay, communications system, and digital control circuit failures are all the same and not deterministic or measurable.
- Failure to consider the consequences of poor design choices, including cost overruns, cancellation, failure, and loss of life.

IV. Terminology and Definitions Risk

Risk terminology is not always consistent among industries or even purposes within industries. However, by and large, the concepts are sound for safety, insurance, finance, and other industries internationally. For the use in this paper, the following relevant definitions are from [16], written for work in dam engineering and safety management but equally relevant to other engineering design and safety purposes, including petrochemical product delivery, nuclear power stations, and DSS:

- Risk—A measure of the probability and severity of an adverse effect to life, health, property, or the environment.
- Risk Analysis—Risk analysis is the use of available information to estimate the risk to individuals or populations, property or the environment, from hazards. Risk analyses generally contain the following steps: scope definition, hazard identification, and risk estimation. The risk analysis process involves the scientific characterization of what is known and what is uncertain about the present and future performance of the dam system under examination.
- Risk Evaluation—Risk evaluation is the process of examining and judging the significance of risk. The risk evaluation stage is the point at which values (societal, regulatory, legal, and owners) and value judgments enter the decision process, explicitly or implicitly, by including consideration of the importance of the estimated risks and the associated social, environmental, economic, and other consequences in order to identify and evaluate a range of alternatives for managing the risks.
- Risk Assessment—Risk assessment is the process of making a decision recommendation on whether existing risks are tolerable and present risk measures are adequate, and if not, whether alternative risk reduction measures are justified or will be implemented. Risk assessment incorporates the risk analysis and risk evaluation phases.
- Risk Management—Risk management is the systematic application of management policies, procedures and practices to the tasks of identifying, analyzing, assessing, communicating, mitigating, and monitoring risk.
- ALARP—As low as reasonably practicable. Human activities and natural phenomena present risks and are possible sources of harm. The term "risk" implies that harm to people and the environment needs to be considered both in terms of the magnitude of the

possible harm and its likelihood. Safety is achieved by ensuring that risks are maintained as low as reasonably practicable (ALARP) [16].

V. Risk Assessment of Protection Systems

When developing a risk-informed program for the evaluation of protection system replacement and health, it is important to have several key understandings of the relay asset and how it is performing in the utility system:

- Ability to identify the failure of the equipment
- Probability of failure of the equipment
- Ramification of the failure
- Accuracy of the data being collected
- Availability of the asset
- Maintenance activity associated with the asset
- Overall health of the system
- Documentation on manufacturer, model, firmware, and installation date of each installed device (Fig. 1 illustrates relay type versus age in service for an example population of relays)

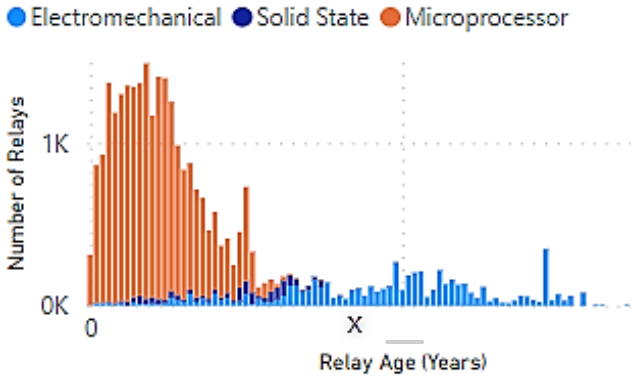

Fig. 1. Example of relay population—type vs. age.

As part of the risk assessment for the protection system components, the following analysis and data sets should be included as part of the risk evaluations:

- Analyze necessary transient stability studies for maintenance/failure of relay systems and other electric components within the utility system.
  - Impact of fault-clearing time and sequence of fault clearing
  - Accurate databases that document design redundancy/monitoring for all components of a protection system
- Analyze system coordination for maintenance/failure of relay systems and other electric components within the utility system.
- Analyze relay failure based upon age, manufacturer, and model.
- Analyze performance data of the relays and protection systems.
- Analyze relay failures that result in a trip or safety mode failure.
- Analyze maintenance reports to determine if systemic problems are occurring between the maintenance cycles.
- Analyze/determine the probability of failure due to historical utility data.
- Analyze/determine the probability of failure relative to manufacturer advisement.
- Analyze/determine the ability to monitor failures of the equipment via alarms or annunciation—this is generally unavailable for electromechanical and solid-state relays.
- Determine the risk associated with environmental issues, such as wildfires.
- Understand the protective schemes, bus configurations, and criticality of the location.
- Understand the overall substation, such as space limitations, age of wiring, nonstandard configurations, protective schemes, bus configurations, and criticality of the location.
- Determine the potential impact on the system—this is not simple because there are several factors that need to be considered, such as the state of the system, failure mode of the equipment, and what failed.
- Determine the accuracy of the relay asset data collection systems.
- Understand the risk of running a relay during its useful life to its expected lifecycle.

VI. RIDM in Practice

RIDM is a tool that is used to analyze risk associated with a design or operation by emphasizing consequences of failure and complements other necessary decisions. Risk information is one input to RIDM, which improves safety but is sometimes left unused because it affects cost, schedule, and performance (CSP) decisions. However, when used appropriately, it guides the design or operations team to make decisions that appropriately consider the health and safety of the site and of the public.

The International Atomic Energy Agency (IAEA) Safety Standards on nuclear reactor design and operation reflect that "both deterministic and probabilistic analyses contribute to reactor safety by providing insights, perspective, comprehension, and balance" [16]. "When the term 'risk' is used to describe a number, as opposed to the abstract concept of risk, in Reclamation practice, it can refer either to the probability of the adverse event or to the mathematical expectation of the adverse consequence" [17]. The prediction of the adverse event is the annualized failure probability (AFP) and the deterministic or mathematical expectation of the consequence of primary concern due to failure known as the annualized life loss (ALL). Once a potential failure mode (PFM) is analyzed using tools (such as event trees and failure mode analyses) and danger to human life is estimated, the risk is plotted on a risk portrayal (RP) chart as an AFP-ALL pair [17]. The graphical portrayal of AFP-ALL coordinates that provide contours for each PFM has been referred to as an f-N

chart [16], and more recently, as an RP chart. An RP diagram illustrates the AFP or (f) of a minimum number (N) of fatalities per year as estimates of ALL. This method is preferred because the total risk of failure over all PFMs is shown, all mathematical expressions are obvious and expressed, and it replaces the expression "f-N chart" with the more general risk portrayal chart. As shown in Fig. 2, the zigzag is a dashed visual guideline dividing the chart in two. The diagonal guideline segment connecting the two horizontal segments represents a progressive reduction in the AFP threshold as the potential life loss increases. PFM estimates that are below guidelines will plot below the line while those with estimates above guidelines will visually plot above the line. This simple visualization makes the chart easy to use and understand, but it must be recognized that risk analysis goes well beyond these simple plots. These are visual guidelines and not tolerability limits.

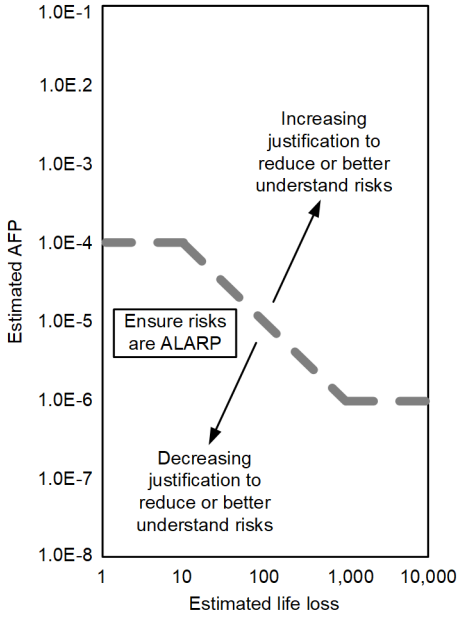

Fig. 2. Annotated risk portrayal chart [17].

A. *Identify and Explore Safety-Related Issues and Consequences to Complement CSP*

The aim of RIDM is to use scientific data as evidence and apply critical thought but not to replace the detailed engineering analysis done as part of the formal design. One difference between RIDM and traditional vulnerability analysis and mitigation relevant to this paper is the process to identify issues. RIDM is separate from, and strictly in addition to, engineering and economic analysis. Therefore, it may not need to be as detailed, and the effort is scalable to be appropriate or complete enough to bring safety issues to light by:

- Placing boundaries around a portion of the design or operating practice. Again, this is not a complete and sufficient evaluation but does allow broad analysis of specific issues.
- Discussing characteristics, and even decisions, that may appear insensitive, such as how much loss of life is tolerable. As updated in 2022, ALARP discussions often use f-N or RP charts [17], as shown in Fig. 3, to illustrate loss-of-life estimates and imply acceptance criteria, or reasonability, of non-zero deaths. As in Fig. 3, RP curves or contours are often shown as straight lines on a logarithmic graph. Positions in the bottom left represent lowest risk, and positions in the top right indicate the most risk.

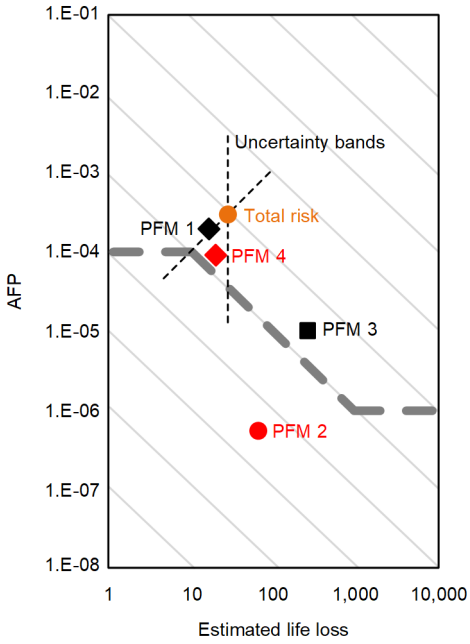

Fig. 3. Risk portrayal chart. The faint diagonal lines are ALL contours, with ALL increasing toward the upper right [17].

- Recognizing that, despite best efforts, there is no zero-risk path and quantifying uncertainties as probabilistic and deterministic risks.
- Seeking and evaluating scenarios that challenge traditional and comfortable assumptions.

Challenging assumptions and recognizing weaknesses in proposed worst-case scenarios.

VII. Integrated RIDM

The nuclear industry uses a systematic process that integrates RIDM into major decisions influencing safety. The goal is to optimize safety without inappropriately limiting operations by integrating RIDM (IRIDM process) to satisfy principles from [16]:

- Defense-in-depth is maintained.
- Safety margins are maintained.
- Engineering and organizational good practices are taken into account.
- Insights from relevant operating experience, research and development, and state-of-the-art methodologies are taken into account.
- Adequate integration of safety and security is ensured
- Relevant regulations are met.

Each decision should include a metric that is reviewed to understand its performance in action.

VIII. RIDM AND IRIDM

RIDM is a powerful tool for designing protection and control systems, and the IRDIM framework illustrates that, when possible, it improves the operation of in-service systems. By developing and monitoring performance metrics, the effectiveness and consequences of various design choices are determined in real time. Sufficient observable, calculable, or measurable indicators are necessary to understand the system performance and safety and provide either confidence or concern. Metrics for systems and components, including failure rates, vulnerability to malicious communications, and susceptibility to undetectable faults, may not satisfy original performance metrics or service-level agreements and may indicate corrective action should be taken. These same observed, calculated, or measured metrics are useful to other design teams when evaluating probabilistic processes.

According to the IAEA, the results of probabilistic and deterministic analysis are complementary to one another. The IAEA recommends the use of a structured and integrated framework to consider the results and impact of deterministic and probabilistic techniques called IRIDM. Details may change as new information becomes available and as IRIDM is applied to different designs and technologies. However, "IRIDM depends on the integration of a wide variety of information, insights and perspectives, as well as the commitment of designers, operators, and regulatory authorities to use risk information in their decisions" [16].

IRIDM is similar to the limited vulnerability design (LVD) concept, which "is an iterative design technique that improves system performance by identifying application gaps, evaluating the risk they represent, and then mitigating the risks" [18]. However, the additional value of IRIDM is how the safety issues for analysis are collected. LVD focuses on continuously measuring and improving a design.

From [16]—Using LVD supports the clear, complete, and candid assessment of gaps, risk, and control of vulnerabilities using steps listed [as follows]:

- Identify gaps during initial design review, understand risk associated with each gap.
- Choose which gaps to mitigate, and how to mitigate them, based on CSP.
- Apply mitigation controls to limit vulnerability and document and explain the remaining gaps identified and accepted in the design review as appropriate.
- Perform factory acceptance testing and then continuously monitor the in-service system for undetected gaps (previously unknown and new vulnerabilities and threats); monitor the performance of mitigation controls, common vulnerabilities and exposures, and supplier service bulletins to evaluate new in-service gaps [18].

The IRIDM process is similar and complementary by emphasizing external environmental and technical safety concerns and total consequences of failure. For example, an Ethernet failure may not simply result in undelivered packets, but also a subsequent failure to trip a breaker, which leads to equipment damage, an outage, and danger to the public. The risk is not static and, therefore, IRIDM and LVD both include the creating and monitoring of metrics. The IRIDM process is illustrated in Fig. 4.

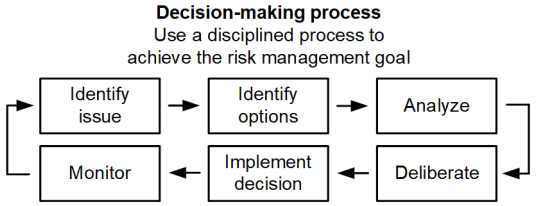

Fig. 4. IRIDM process.

IX. RIDM AND FAILURE ANALYSIS IN DSS

The IAEA safety standards on nuclear reactor design and operation reflect that "both deterministic and probabilistic analyses contribute to reactor safety by providing insights, perspective, comprehension and balance" [19].

If a process or behavior with an output is measurable and repeatable and affected only by the initial conditions, the input is considered deterministic. For example, the time to transfer power flow information within a digital message via a direct cable between two programmable electronic devices is deterministic. It can be staged, tested, observed, measured, and repeated.

A process or behavior for which some element of randomness plays a role in the output is considered probabilistic. For the purpose of this paper, probabilistic outcomes are actually part deterministic and part random, rather than entirely random. For example, the products among others in service in identical conditions that fail, if any of them do, may appear random. However, based on historical data of device failure in the past, the quantity of failures for a specific population of devices is predictable and known as the failure rate. The mean time to fail (MTTF) is the time duration that the product functions correctly from the time it starts or resumes operations until it fails in service, as illustrated in Fig. 5.

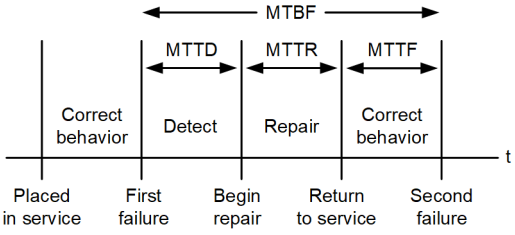

Fig. 5. Failure and repair cycle.

To understand the impact to predicted system availability, the deterministic analysis is performed on the effort to repair or replace a known failed device to return it to service, known as the mean time to repair (MTTR), as shown in Fig. 5. The MTTR is the time duration between the notification of the failure and completion of the repair, in which the device is tested and returned to service.

The time duration between a failure and failure detection is known as the mean time to detect (MTTD), as shown in Fig. 5. The MTTD is deterministic when devices have self-testing, fault monitoring, and self-announcing of failures. However, the

MTTD is probabilistic when devices do not automatically detect and announce failures because the time between failure and detection cannot be known. A failure of an unmonitored device or component will be detected if it fails when called upon to correct a problem, and the result is a power system fault. In this case, the detection and the power system fault are simultaneous, but the device failure could have been present and hidden for an undeterminable period of time. This phenomenon is one of the reasons for the suggested modifications to NERC TPL-001-5.1. Traditionally, failures of in-service secondary system devices are detected when they are removed from service and tested periodically. If a failure is detected during periodic testing, it is repaired and the unit returned to service. If a failure is detected during periodic testing, it means that the power system was vulnerable to a hidden failure for an undetermined period of time or that the test process induced the failure. The fact that each failure could manifest itself moments after or before a periodic test means that the MTTD could be moments or years. Secondary system periodic testing is traditionally done on 5-year and 10-year cycles (some are on a 6-year or 2-year cycle), and they are evaluated for self-monitored DSSs. Since the MTTD of nonmonitored devices is between moments and the full periodic test cycle, engineers traditionally use the mean, or half, of the periodic test cycle.

A. RIDM Integrated Into DSS Availability Requirements

First, the true consequences of a failed DSS must be evaluated—not simply the nuisance of a failed data path, but the worst-case consequences of an undelivered protection signal. Though the audience should apply this to their specific situation, there is an example of a dramatic electric power system fault in Sao Paulo, Brazil, on November 1, 2019. Both transmission and distribution circuits were involved after vegetation created two simultaneous two-phase short circuits. The primary circuit breaker did not operate due to a mechanical failure. The backup breaker did not operate when the system that intended to perform breaker failure protection for the primary breaker failed to operate when protection signals were not delivered [4]. It appears that the components of this system were out of service at the time, and this condition was not monitored, detected, or reported. The result was more significant than the most significant worst-case scenario predictions when the transmission-level fault remained energized for 110 seconds over a heavily populated urban area, due to the failure to transfer protection signals in a secondary system [4]. In this case, the high-voltage fault remained energized over 1,300 times longer than a traditional clearing time between 40 ms to 80 ms.

Second, the inverse of the number of failures in a population over time should be used as failure rate data to analyze the probabilistic risk of a future device failure while in service. Using the "known failure rate while in service" results for several components being considered for a design will yield best results. Because future failure rates of potential use of the components are not deterministic, it is impossible to be certain how many will fail in a given year. As described in IEC 60870, the failure rate from historical data is used to predict the number of failures that a population of devices will experience over a period of time expressed as the mean time between failures (MTBF), as shown in Fig. 5 [20]. The MTBF is the time it takes to get the system running again as intended after a failure. The unavailability of a device is expressed as a probability that it will not perform its intended purpose and may lead to the worst-case scenario [20]. Examples of data from multiple suppliers are illustrated in Table V.

TABLE V MTBF DATA IN YEARS REPORTED BY SUPPLIERS

OT Ethernet switch, individual port	500; 3,198
IT Ethernet switch, individual port	29; 130
IPC 610 Class DSS device, Ethernet board	800; 68,750
Industrial-grade DSS device, Ethernet board	65; 647
Fiber-optic connection	5,000
Hardwire termination	5,000

And third, the deterministic risk of the DSS being unavailable to protect against the worst-case scenario for given probabilistic MTBF values should be analyzed. Wiring terminations and electromechanical, numerical, and digital devices fail over time. A 5,000-year MTBF per wiring point is the predicted realistic field failure rate per wiring point [20]. It is typical and deterministic to assume that all devices can be repaired with an MTTR of 48 hours after an alarm. The MTTD is immediate for self-detecting and self-reporting devices and predicted to be the mean (1, 3, or 5 years) of the various periodic test cycles (2, 6, and 10 years) for unmonitored electromechanical devices and hardwire terminations. As shown in figure 4a, the MTTR divided by the MTBF provides a unitless value representing unavailability [21]. See (1).

$$\text{Unavailability } q = \frac{\text{MTTR}}{\text{MTBF}} \tag{1}$$

The unavailability for devices in Table V and various values for the MTTD are illustrated in Table VI. This shows how the design and operation availability of a device changes with the MTTD. For example, assuming an average testing interval of 2 years and a period of 2 days to make the repair, the unavailability value of copper contact wiring with an MTBF of 5,000 years is 200. Whereas, a monitored fiber connection with similar factors has an unavailability value of 1 which is 200 times smaller than the copper wiring unavailability value of 200. This allows us to predict that a monitored fiber connection will be 200 times more available to convey a digital trip signal than an unmonitored copper wire contact.

It is very important to understand that unavailability is not an indication of the risk that a product will fail over time—that is MTBF. Unavailability is a unitless value that gives the relative likelihood that a device is failed in service at some point during the time being considered. As shown in Table VI, the longer it takes to detect a failure, the less available the same device is predicted to be. The device quality does not change, but its availability to perform its intended function does change with the MTTD.

TABLE VI UNAVAILABILITY, q, FOR VARIOUS MTBF AND MTTD GIVEN A 48-HOUR MTTR • 10^{-6}

	Unavailability; q • 10^{-6} (where bigger is bad)			
	Automatic MTTD	**1 year MTTD**	**3 years MTTD**	**5 years MTTD**
MTBF				
500 years	10	2,000	6,000	10,000
800 years	6	1,250	3,750	6,250
5,000 years	1	200	600	1,000

As a simple example, considering the battery on a smart phone and the monitoring and deterministic reporting of the remaining capacity on the display, the user can imagine that there is no display of the remaining battery capacity to influence actions, such as recharging the phone or placing it in airplane mode. The phone has not changed; however, probabilistic analysis reveals that the predicted likelihood that it will be available for them to make an important call is much lower. The predicted availability to make an important call will be the highest when a user carries both a phone and battery and each one monitors battery life and indicates it via a display. However, the probabilistic analysis shows that if a user carries a phone and an extra battery but neither monitors battery life, the predicted availability for them to make an important call will be less than the phone with battery life monitoring and no extra battery.

The MTBF is the sum of the MTTD, MTTR, and MTTF. The MTTF reflects product quality, and the MTTD and MTTR represent the product serviceability. Serviceability is the ability for a technician to maintain, diagnose, and repair a device and return it to service. The ease with which this may be accomplished is influenced by automatic monitoring and reporting as well as with the availability and visibility of diagnostic information and performance measures, collectively referred to as useability. Devices that are less serviceable and useable may require replacement rather than repair. The mean time to replace (also MTTR) a device affects the MTBF calculation the same as the mean time to repair a serviceable device. However, using low-MTBF devices and those with poor serviceability has other consequences. While it may be possible to maintain a suitable level of system availability through the frequent manual replacement of failed nonserviceable devices, the many other consequences include the:

- Cost of storage and transport of additional inventory of spares.
- Cost of staff managing inventory and frequent replacement.
- Additional downtime when replacement inventory is unavailable.
- Cost of technician training and performance for managing diagnostics and repair.

The international standard for functional safety for electrical, electronic, and programmable electronic devices, IEC 61508, illustrates the benefit to availability and system safety provided by automatic fault detecting and self-alarming within a device. Failures that jeopardize the safety of equipment or people due to a device being unavailable to perform its intended function are referred to as dangerous failures. Failure modes that are observable via self-testing are referred to as detectable, and those that are not are considered undetectable. DD failures with an automatic MTTD can trigger an alarm and prompt corrective action and repair. DU failures without an automatic MTTD place people and systems at risk with unknown and unattended in-service failures.

An accurate and calculated MTBF is essential for the engineering analysis of probabilistic details, such as reliability, dependability, and service life of devices and components.

X. RIDM USE IN THE REAL WORLD

Numerous examples of deadly industrial catastrophes due to ineffective or missing risk analyses exist, and many have been studied at length as cautionary tales. We chose instead to document successful results from several industries to demonstrate the value of RIDM. Each example includes engineers that acted on their obligation to hold paramount the safety, health, and welfare of the public.

A. RIDM in Dam Design

Dam safety has long been a priority of the U.S. Federal Government and state dam safety agencies. FERC-regulated dam projects, as well as federal projects operated by the U.S. Army Corps of Engineers (USACE) and the U.S. Bureau of Reclamation, often use RIDM in their evaluation and determination of design alternatives that will reduce risk to the downstream public.

A recent project is demonstrative of the positive conclusions of the design and oversight teams, which undoubtedly save lives and downstream destruction and economic consequences. In this case, issues were detected by monitoring and physical surveillance, which prompted a dam safety modification study with proposed rehabilitation on the dam facilities as corrective actions. This modification plan included a proposal for a cofferdam based on flood risk with crest elevation below the crest elevation of the original dam.

Addicks and Barker Dams, which lie to the west of downtown Houston, Texas, were constructed in the mid-1940s as an integral part of the Buffalo Bayou and Tributaries project and have been operated by the USACE. With the growth of Houston's population and aging of the projects, PFMs were identified and plotted as circles on the Addicks Dam f-N chart in Fig. 6. This work was done prior to the nomenclature and visualization changes related to the RP chart [17], so societal risk represented by the use of a technology, activity, process, or design is graphically represented by its position on an f-N chart. The horizontal axis shows the calculated predicted number of deaths that may result, and the vertical axis represents the calculated predicted frequency or annual probability of the event happening. The presumed socially acceptable tolerance of risk, number of deaths, and probability of occurrence are shown as a straight line on an f-N logarithmic plot. Using this method, risk aversion is exponentially related to the severity of the consequences of an event. Two parallel social tolerance

lines are used to create an ALARP band. The region above the band is considered unacceptable risk, and risk reduction is required; between the lines is the ALARP band, where risk may be tolerable if mitigation is considered too extraordinary, and below is where no further risk reduction is necessary.

Fig. 6 represents an example f-N chart created by a member of the construction review team. Each circle in Fig. 6 represents the consequences of each potential PFM event, as determined by PFM analysis (PFMA). The overall total project risk is an aggregate of the PFMs and is plotted as a diamond on the f-N chart, which can be seen in Fig. 6 to hold risks that are above tolerable risk levels. So, as it stood, the dam was determined to present unacceptable risk of failure and required modification.

The population at risk was calculated at over one million people, with the loss of life of the PFMs at about one thousand. Economic damage was calculated at over a hundred billion dollars.

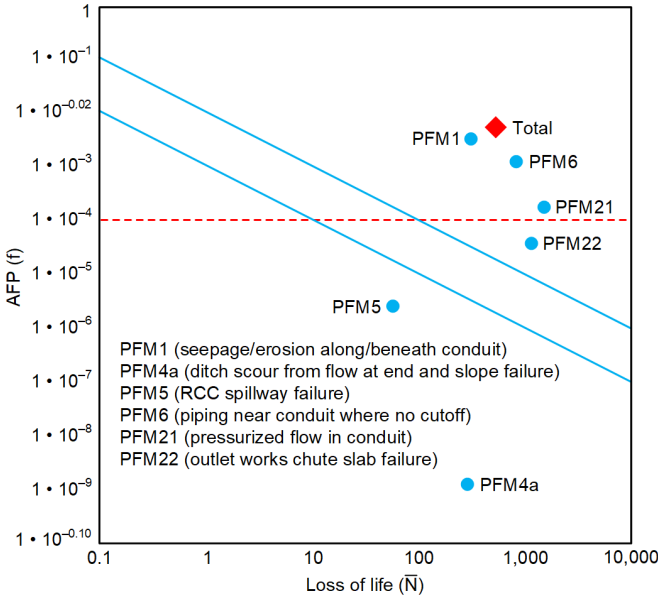

Fig. 6. Example of Addicks Dam f-N chart with no action plan.

The constructability review team observed that the dam safety modification study recommended a comprehensive approach, rehabilitating or replacing various elements, each of which could independently potentially lead to dam failure. Fig. 7 represents an example f-N chart created by a member of the constructability review team. As shown in Fig. 7, the dam safety modification team proposed that implementation of the preferred alternative rehabilitation plan would bring the facilities risk within tolerable risk guidelines.

The plan included that a significant cofferdam be constructed for the purpose of protecting the work area and the downstream public. The implementation of the preferred alternative plan and related temporary cofferdam is shown in Fig. 8.

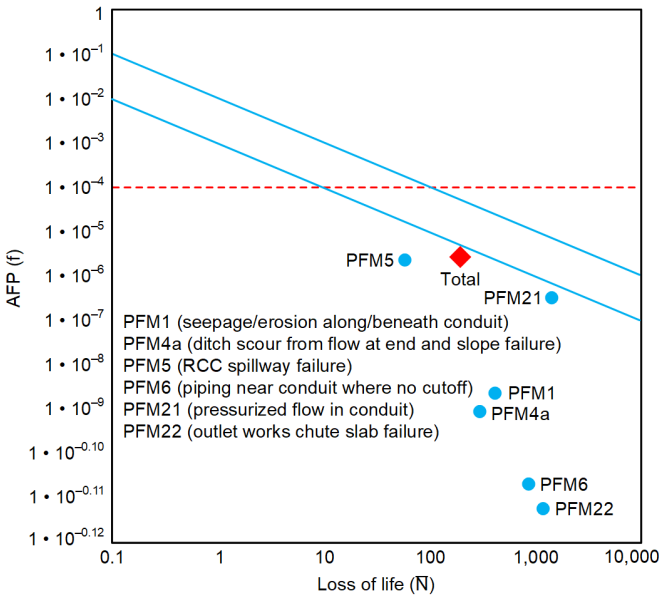

Fig. 7. Example of Addicks Dam f-N chart with preferred alternative.

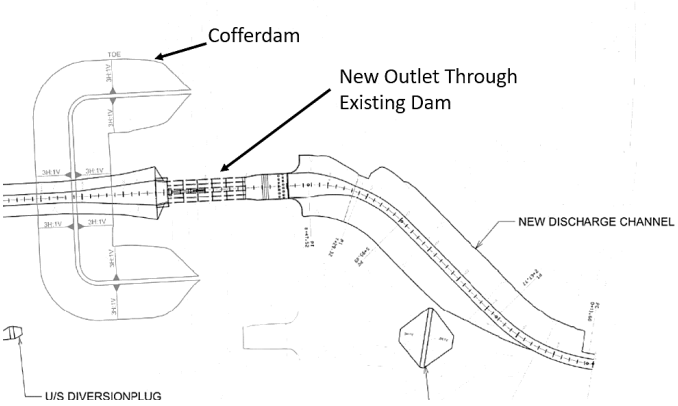

Fig. 8. Outlet design showing upstream cofferdam.

A subsequent review of the preferred alternative plan by an oversight committee team identified that the initial PFMA, illustrated in Fig. 8, did not consider risks associated with construction activities or sequencing of work. In this case, the oversight committee team determined that the proposed elevation of the temporary cofferdam would not adequately protect the population at risk from severe natural events during construction. Based on this assessment, the total risk of the preferred alternative plan was calculated to be well above the ALARP band and held unacceptable risk.

At the time of design, these projects were about 60 years old, with the highest recorded reservoir pool elevations well below the initial design crest elevation of the cofferdams. This crest elevation of the proposed cofferdam was influenced by weather data and previous pool levels well below the cofferdam design. However, the oversight committee team, in concurrence with the dam safety modification team, re-evaluated the cofferdam crest elevation through RIDM procedures and determined that any crest elevation below the current dam elevation introduced an entirely new risk to the downstream public, the population at risk. This late determination was more qualitative, driven by the one million persons at risk. Further, the oversight teams were influenced by USACE's Safety Criteria for Risk

Management Plans (Civil Works Review Policy, EC 1165-2-209), requiring robustness, redundancy, and resiliency. With this risk also considered, the preferred modification plan included unacceptable risk to the project and the population. Based on this, the cofferdams were redesigned to the full height or crest elevation of the existing dams, and the aggregated risk fell below the ALARP band due to acceptable predicted risk. This illustrates the need to perform an analysis of the construction process and not just the end result of the modifications. This is referred to as a construction PFMA (CPFMA).

Subsequent to the start of construction, each of these dams and reservoirs experienced two new record-breaking pool elevations in 2017 and 2018, well above anything experienced in their 60-plus-year life. If the cofferdams had been built to the original proposed height, they would have been overtopped by either the 2017 Hurricane Harvey or the following storm surge in 2018 and would have breached and failed catastrophically. See Fig. 9 photo of the Addicks Dam cofferdam, preventing a breach of the construction site on Addicks Dam, allowing the adjacent piping in the dam structure to gradually release floodwater.

Fig. 9. Addicks Dam cofferdam in February 2018, which was not overtopped and prevented failure of the dam while allowing moderate release of floodwater [22].

In this case, RIDM techniques identified a newly introduced vulnerability, illustrated probabilistic storm danger, led to deterministic cofferdam elevation, and successfully weathered a 1,000-year flood.

B. RIDM in Refining Operations

The petroleum and petrochemical industry have long integrated RIDM into their design and operating practices. Incidents in the petroleum industry tend to result in a lower (but nonzero) human impact because the population density inside the fence line is fairly low, but incidents can have substantial environmental, reputational, and financial costs related to repair and production loss. These costs, as well as risk to humans, are typically included in RIDM reviews.

One of the givens in petroleum refining is that the crude diet can change to take advantage of available supplies and pricing. At a West Coast refinery in the early 1980s a substantial investment was made in installing new downstream units and retrofitting some of the upstream units to safely run heavier crudes. One of the upstream modifications of existing units was the replacement of portions of the sour water treating system, which removed sulfur in the off gas, the mixture of gases generated during the refining process. This is done by using the widely used chemical reactant, amine. At the time that a new column for the unit was designed, the cracking of highly stressed carbon steel in the presence of amines was a well-known phenomenon—basically, the welding of any material results in high localized stresses in and adjacent to the weld zone. A decision was made to fabricate the column using stainless steel, as it had exhibited strong resistance to cracking in laboratory corrosion studies. What was known in the scientific community but not to those specifying materials in the refining industry was that the welds on medium– to high-carbon stainless steel, in the presence of amine, were robbed of their corrosion resistance during the welding process. The chromium in the stainless steel bonded with carbon at the high temperature generated during welding and depleted the weld and weld zone of chromium, essentially giving these sensitized areas the chemical resistance of carbon steel known, as stated previously, to be susceptible to cracking.

1) RIDM Integrated Into Inspection Procedure

The in-service inspection of piping and methods of repair are risk-informed operations that have well-documented best-known methods based on first principles and historical data that provide guidance. However, in this case, the petrochemical community had little historical data on austenitic stainless steel welds. The interval and extent of inspection for each piece of refinery equipment is based on RIDM. During the first internal inspection of the new stainless steel vessel, cracks were visually noticeable in the welds and weld zone of a large manway. Because cracking can occur but not be visible to the naked eye, all vessel welds were then examined by dye check—a relatively quick and dirty inspection technique in which a penetrating dye and developer are sprayed onto the suspected surface, making cracks more visible. Additional cracks were found by this method.

Hydrocarbon leaks from refinery equipment can result in the release of hydrogen sulfide gas (which is immediately life-threatening) and hydrocarbon vapors (which can ignite and cause fires and explosions), neither of which are necessarily confined to inside the fence line and may endanger the general public beyond it. Both of these potentials existed for this vessel, and the engineer in charge (EIC) of the inspection was well aware of this. Furthermore, he had recently completed a continuing education course that dealt with weld sensitization in stainless steel and knew what the crack morphology could be, and he was uncertain that the dye-check methodology had found all of the cracks. He used his recently acquired knowledge and intuition as part of a probabilistic analysis and pushed for further inspection using a new but as-yet un-scaled-up method of ultrasonic crack detection.

This additional inspection request was controversial—the vessel had not failed, the inspection was expensive and would have resulted in a startup delay, and the risk was perceived by

the operating group as exaggerated. Because of his assessment of risk and recently obtained knowledge, the EIC was able to successfully challenge his colleague's assessment of risk exaggeration and perform the ultrasonic inspections. These inspections found subsurface cracking and provided data for a deterministic analysis of which welds to repair. A weld procedure specific for the service was developed and used in the repair, and plans for subsequent inspections were modified to include a rigorous examination for cracking.

There is no doubt that one man's obstinate stand prevented the potential loss of life and probable financial burden. He recognized that the failure of a weld could result in catastrophic infrastructure failure. He determined that visible welds were corroded and predicted that other corrosion was not visible. Controversial but essential inspections proved him right and laid out the groundwork for repairs. As a positive-outcome engineering example, after the expense and effort of the RIDM process, inspection, and repairs the site went back into production and has functioned for decades without an event caused by a failed weld in this service. The incident has been shared through professional organizations, and design standards have been changed to prevent this type of cracking.

As a side note unrelated to this incident, the American Petroleum Institute formalized the use of RIDM in their recommended inspection practices in the early 2000s. Many states have adopted their recommended practices as law.

C. *2011 Tohoku Earthquake Impact on Japanese Nuclear Power Plants*

In 2011, five Japanese nuclear power plants, as shown in Fig. 10, were directly affected by the Tohoku earthquake and tsunami [23]. However, the impact on the Fukushima Daini nuclear power station (NPS) owned by Tokyo Electric Power Company (TEPCO) and the Onagawa NPS owned by Tohoku EPCO was dramatically different due to the use of RIDM in the design and operation of the latter.

Fig. 10. Nuclear power plants on northeastern coast of Japan affected by the 2011 Tohoku earthquake and tsunami (01: Higashidori, 02: Onagawa, 03: Fukushima Daiichi, 04: Fukushima Daini, and 05: Tokai Daini) [23].

"The Fukushima Daiichi nuclear power plant confronted severe core damage in three of its nuclear reactors; Reactors 1, 2, and 3 melted down and hydrogen explosions occurred" [24]. An immense number of radioactive substances were released into the environment, during and after the event; roughly 167 workers were exposed [25], and more than 1,800 square kilometers of land were contaminated [26]. "The Fukushima Daiichi 2011 event was a large-scale and long-term nuclear contamination natural hazard-induced technological (natech) event. The catastrophe was rated as Level 7 on the International Nuclear and Radiological Event Scale (INES) of the IAEA—the same rank as the Chernobyl nuclear disaster in 1986" [27].

The Fukushima Daiichi nuclear power plant disaster in 2011 was not only a natech event, but was declared to be a profoundly manmade disaster by Dr. Kiyoshi Kurokawa, the chairman of the Fukushima Nuclear Accident Independent Investigation Commission. The 2011 Fukushima Daiichi NPS accident was actually a man-made natech disaster in which a cascade of industrial, regulatory, and engineering failures occurred [28].

Though the Onagawa NPS received the highest impact from both the earthquake and the tsunami, due to being closest to the epicenter of the 2011 Tohoku earthquake, as shown in Fig. 10, it did not experience a catastrophic natech event. Instead, "it kept its integrity and managed to successfully bring its nuclear reactors to a cold shutdown" [28].

The destruction of the Fukushima Daiichi NPS is well-documented, but equally researched is the nonfailure of the Onagawa NPS due to Tohoku EPCO design decisions about risk, which were based on past tsunami tide elevations. These decisions about risk to the NPS based on awareness of previous events were championed by the vice president of Tohoku EPCO, Yanosuke Hirai, between 1960 and 1975. "According to certain narratives, as a child, he visited an ancient Shinto shrine that kept alive the legend of a destructive earthquake and tsunami in 869 CE. This visit impacted him for life and determined his actions taken later on, particularly towards Onagawa NPS. In 1963, he became a member of the Coastal Institution Research Association and continuously emphasized tsunami risk and the actions required to mitigate it. He took into account and examined folk tales, old records, books, and results of surveys on past tsunamis in the Onagawa area and Sanriku coast" [23]. Tides as a result of tsunami are measured as incremental elevations above the tide level at the Onahama Port situated on the eastern coast of Honshu Island, in the Fukushima Prefecture. Yanosuke Hirai refused to compromise designs with respect to safety of NPS, and so he opposed the initial design elevation of 3 meters above the Onahama Port suggested by his colleagues. Against their advice, Yanosuke Hirai proposed a design more resistant to tsunami. He informed the president of Tohoku EPCO that the 869 Jogan tsunami, 1611 Keicho tsunami, and 1896 Sanriku tsunami were events that should be considered possible in the 20th century and won approval to raise the plant elevation to 14.8 meters above the Onahama Port. Yanosuke Hirai had based this elevation in part on the 869 Shinto shrine records that documented how people had fled to previously unaffected high ground only to be surprised and killed by a tide much higher than they anticipated.

Tohoku EPCO used different methods to design seawall height and initial land elevation when choosing NPS construction sites. The design of Fukushima Daiichi was done without the same thorough review of historical information and its lower site elevation of 10 meters above the Onahama Port created great operational risk. In fact, rather than focusing on the earthquake and tsunami risk for the design, the site elevation was lowered to accommodate construction as well as equipment delivery more easily from sea-going vessels. Further, "over the operation phase, the awareness and concerns about earthquake and tsunami risk were also not in place at Fukushima Daiichi" [27].

1) *RIDM Integrated Into Decisions to Position and Protect the Onagawa NPS*

First, Yanosuke Hirai challenged assumptions by his colleagues and the inadequacy of their proposed countermeasures to a tsunami. He proposed a more dramatic worst-case tsunami scenario.

Second, Yanosuke Hirai used historical data to analyze the probabilistic risk of a future earthquake and associated tsunami, as shown in Table VI. While his colleagues may have claimed that the future was uncertain, Hirai established the probability of a strong earthquake and an associated tsunami with his analysis.

TABLE VII EARTHQUAKES AND TSUNAMIS IN NORTHEASTERN JAPAN OVER THE CENTURIES [23]

Name	Date	Magnitude	Intensity
Jogan	07.13.869	8.6	4
Keicho Nankaido	01.31.1605	7.9	4
Keicho Sanriku	12.02.1611	8.1	4
Empo Sanriku	04.13.1677	8.1	2
Empo Boso-oki	11.04.1677	8.4	2.5
Kansei Sanriku	02.17.1793	7.1	2
Meiji Sanriku	06.15.1896	7.6	3.75
Showa Sanriku	03.03.1933	8.5	3.5
Tokachi-oki	05.16.1968	8.0	2

Third, he analyzed the deterministic risk of damage at various proposed NPS elevations for given probabilistic tsunami elevations. Hirai used scientific evaluation to predict the height of a worst-case tsunami, added a safety margin, and proposed a site elevation and height of a seawall.

In the end, Hirai refused to agree that a future earthquake was uncertain; instead, he proposed a worst-case scenario based on probabilistic risk scenarios and countermeasures based on deterministic risk scenarios for the Onagawa NPS, while the Fukushima Daiichi NPS design lacked the same rigor. As mentioned, the Onagawa NPS tsunami-resistant design included a main plant elevation of 14.8 meters above the Onahama Port and included a seawall elevation of the Onahama Port plus 14 meters, while the meager Fukushima Daiichi design margins included a main plant elevation of 10 meters, seawall elevation of 4 meters, and breakwater elevation of 5.5 meters above the Onahama Port. Both NPSs experienced tsunami waves estimated at 13 meters, as a result of the Tohoku earthquake that reached a 9.0 moment magnitude, the largest ever recorded in Japan [29].

The Onagawa NPS experienced very little damage, and the equipment had "a remarkable rate of survival" [30], while the Fukushima Daiichi failure became a large-scale and long-term nuclear contamination natech event.

D. *DSS Design for Reliability Based on International Standards*

Differences in predicted unavailability of the same device, with and without automatic fault detection and reporting, as shown in Table VII, show the increased risk of a device being unavailable to perform its intended function when called upon. Essentially, they represent a fault waiting to happen because they are out of service and not alarmed. The importance of this concept, and the risk that it represents to DSSs, is further illustrated in the following:

- The lack of automatic failure detection and self-announcement of alarms creates DU faults, as described in the international standard for functional safety for electrical, electronic, and programmable electronic devices, IEC 61508 [14].
- The prolonged MTTD due to lack of automatic failure detection creates high risk to systems due to low predicted product availability, as described in the IEC 60870 fault analysis [20]. Undetected faults remain as hidden failures for the duration of the MTTD.
- The only acceptable exclusions to redundant relay, dc power supply, communications system, and control circuits (direct communications, wiring, and auxiliary and lockout relays) are these SPOFs with appropriate monitoring and reporting of failure, as described in NERC TPL-001-5.1 [6].
- TR 61850-90-12 describes two types of failures that the grid may experience as overfunction (unwanted trip) and underfunction (missing trip when required) [31]. DSS communications failures may experience a data breach (wrong data not recognized as such can cause an overfunction) and persistency breach (no data or data too late can cause an underfunction). The standard demonstrates mathematically that repair prompted by failure monitoring is shown to greatly improve availability due to a shortened MTTD. It further clarifies that "redundancy itself is useless if not constantly supervised" [32].
- IEC 62439-3:2021 PRP and HSR duplication technologies that are not redundant have no message subscription fault detection and, therefore, no fault reporting. Neither technology can detect a failure or warn of a failure in service, and so the standard clearly states that monitoring is essential or the methods help little. In spite of no data path delivery monitoring, "redundant devices and links are useless without network management supervising redundancy and calling for maintenance actions" [32].

1) IEC 62439 Hides Cyber Intrusion and Creates Hidden Failures

The inability of IEC 62439-3 methods to detect communications failure, when implemented as per the standard, was demonstrated in [33], which describes two failure modes that were created and how no failures were detected. The paper describes a communications-aided protection and digital

message control circuitry scheme required for fault clearing that was staged to transfer Sampled Values (SV), Generic Object-Oriented Substation Event (GOOSE), Precision Time Protocol (PTP), and Manufacturing Message Specification (MMS) as part of a protection system digital trip circuit example. However, when each failure was created and left unrepaired in the system, faults were not detected, and no alarm was generated. "In [the] Portugal substation, there [was] no activation of failure alarms of SV, GOOSE, PTP, or MMS messages in any IED of the system. That was the expected result, since the recovery for a PRP system is 0 ms" [33]. The IEC 62439-3 PRP technology provides no recovery, and the standard clearly points out that faults require manual detection and repair. The paper [33] incorrectly gives the impression that the system recovered and corrected the fault; however, the IEC 62439-3 includes no message subscription monitoring and, therefore, no fault detection or recovery. With one of the two duplicate data paths working, messages were delivered without interruption for a single fault. However, it also prevented the detection of the intentionally created failures, and those faults would remain until manually corrected. The intentional disabling of failure detection described in the paper [33] not only creates hidden failures in the protection system, but also disables the detection of cyber attacks and network reconfiguration. Since IEC 62439-3 eliminates the fault detection of failures, including LAN segment breaks and reroutes as well as the insertion of malicious hardware, data capture and injected messages will be undetectable.

2) RIDM Integrated Into DSS Design

When considering protection system designs, evaluation begins with the question: What is the minimum level of available protection necessary to allow the primary asset to remain energized and in service?

When that question is answered to the satisfaction of the asset owner, the design team next creates a component-level theoretical design for further analysis. To become better informed about risk, failure, and unavailability, scenarios are considered for each of the components of the proposed protection system. A component fault is a failure that creates unavailability, and a maintenance activity is scheduled unavailability of a protection system component. The design team evaluates the subsequent degradation to protection system availability to see if it still meets the minimum level necessary for the primary asset to remain energized and in service. If not, a risk reduction action is proposed, such as making that component redundant. Historically, this process has revealed that the most vulnerable components are telecommunication routes and CTs.

As an example, for a 500 kV line to remain in service, all of the following protection features must be available:

- At least one level of communications-assisted protection system (POTT, DIFF, etc.)
- At least one level of non-communications-assisted protection system
- At least one level of direct transfer trip

As is often the case, if a line segment has only two guaranteed independent telecommunication routes, the protection system must still meet the minimum level stated previously, even if one of the routes experiences a failure.

Also, some of the 500 kV breakers only have two CTs and, therefore, the failure of one must result in a protection system that meets the minimum level stated previously.

In some cases, the risk analysis of device unavailability due to failure or maintenance activities reveals that two redundant relays may be inadequate. Triple redundant relays may be used to keep redundant protection in service during repair, maintenance, and future replacement.

As a simple illustration of the benefit of using RIDM, a DSS design can be considered for reliability. First, we challenge several assumptions:

> Assumption—Once installed, relays and other devices are assumed to work properly, and it remains uncertain if they will fail. This is false, as seen in NERC TPL-001-5.1; the protection system is not assumed to be error free, and it is anticipated that some devices will fail in service. As engineers, it is our responsibility to understand and predict failure modes as well as supervise them to trigger corrective actions.
>
> Assumption—If the relay does not operate, backup protection will operate within 80 ms. This is false, as seen in Brazil, where backup protection failed as well and the fault remained energized for 110 seconds.

Next, we evaluate a scenario that challenges a traditional and comfortable assumption.

> Assumption—PRP will provide redundancy to protection system communications and digital control circuits. This is false; redundancy means the addition of one or more systems that completely provide another source of critical components, and PRP eliminates the critical function of monitoring. Two duplicated systems with reduced functionality may act as duplicates but are not redundant. Without monitoring, a duplicate PRP data path may have a fault that will remain a hidden failure on the system until manually found via testing or because it causes a BES fault.

Finally, we quantify uncertainties as probabilistic and deterministic risks. Since low unavailability reduces the likelihood that a device is failed in service, , it will improve the design availability and reliability. The RIDM analysis shows that systems using PRP, as defined in the standard IEC 62439-3, will experience faults that become hidden failures. Protection systems with a 6-year maintenance cycle have probabilistic risk of a PRP hidden failure proportional to the predicted 3-year MTTD.

So, the consequences of protection system failure may not be contained within the substation fence line and may endanger the general public beyond it. PFMA reveals that it may cause a

significantly long BES fault-clearing time. IEC 62439-3 PRP failures disguise cyber hacking and create prolonged hidden failures that are not detectable or repairable, which elevates the vulnerability of protection systems based on PRP above tolerable risk levels, according to NERC TPL-001-5.1.

The following solution may be considered provocative or unpopular from an international standardization perspective but is a superior safety solution. IEC 62439-3 PRP is a proprietary protocol that requires a commercial agreement with the owner to use it, and its behavior is documented in the international standard IEC 62439-3. When a relay supplier innovates a solution to provide fault detection, the availability is improved, but the technology becomes a sole-source solution. International standards are not readily updated or modified to correct mistakes, and so the enhancement may never be added to the standard in order that other suppliers may provide it as well. Therefore, this design choice to add fault detection to IEC 62439-3 PRP may be unattractive from a standardization perspective but greatly improves safety and reliability. In fact, since the fault detection is immediate, the MTTD changes from 3 years to 2 days.

RIDM methods reveal design choices that will reduce the probability that a hidden failure is present in a protection system by a factor of 547. Further, it is apparent that without monitoring, IEC 62439-3 methods will not be sufficient to exclude power system components from being made truly redundant, related to modifications to NERC TPL-001-5.1

XI. Summary

"The tragedy at Fukushima Daiichi was not an 'accident' in the sense that it could not have been anticipated. From a geologic perspective, there were many 'red flags' related to the probability of a tsunami event and its scale. I think that one of the important lessons is that we have spent too much time using risk assessments to demonstrate that a reactor site is safe and not enough time imagining how it might fail" [34].

Examples in this paper illustrate that professionals need to analyze deterministic and probabilistic risk with local and specific knowledge guided by experience. Those that promote design choices without adequate risk assessment create a moral hazard when they are individually protected from the consequences of their actions. Moral hazard can also be created by engineers and trusted professionals that adopt technology and procedures with known or unknown failure modes and do not disclose that they create unintended consequences. They transfer the vulnerability onto others by not explaining and revealing failure modes and consequences, due to lack of knowledge or a personal feeling that failure is unlikely. Similarly, at Fukushima, "perhaps most importantly, many believed that a severe accident was simply impossible" [35].

As engineers, it is our responsibility to identify and mitigate risk and not allow protection and safety systems to be driven to failure. It is unacceptable to attempt to explain away a lack of design for resilience that produces a failure as an act of nature. As with the Tohoku earthquake, "the calamity was not simply an 'act of god' that could not be defended against. We believe the Fukushima accident—like its predecessors—was preventable" [35].

Uncertainty is a lack of information and awareness about an event or failure. Risk is the measurable chance that failure will occur, and as engineers, we use data-driven tools to predict risk to understand and address vulnerabilities. An important role of engineering is differentiating between the two and replacing uncertainty with managed risk based on science and math using tools including RIDM.

The IEEE code of ethics includes language that we commit ourselves to the "highest standards of integrity, responsible behavior, and ethical conduct in professional activities" [36]. It prioritizes the preservation of public safety ahead of personal growth, conflicts of interest, unlawful conduct, offer and acceptance of honest criticism, and continuous competence through learning. It concludes by requiring that we strive to ensure this code is upheld by colleagues and coworkers. Although not pleasant, it is sometimes necessary to disagree with a colleague, supervisor, or management structure if they do not uphold these values. RIDM is a tool that can depersonalize issues and make vulnerabilities public to promote corrective action in the event that others are not appropriately concerned. For example, some safety experts feel that the lack of tsunami safety at Fukushima was attributable to the management structure. Some suggested that management "tolerated or encouraged the practice of covering up problems" [35].

XII. Conclusion

Not all that suffer are victims. Relevant to this paper, not all systems that suffer from environment-influenced failure are victims of unpredictable natech failure. Examples in this paper illustrate the use of RIDM to avoid predictable failures; however, numerous natech BES failures between 2011 and 2023 created many unwitting public victims due to inadequate availability during extreme cold and heat weather events. Inadequate design is not a victim of weather events even when the protection system suffers failures. However, the public at large suffers unacceptable economic impact, risk to life, and loss of life during weather extremes.

The value of RIDM as a tool is illustrated in hindsight to better understand engineering choices associated with well-known past failures with respect to their consequences.

In conclusion, real-world success examples explain how the American Petroleum Institute security risk assessments prevented explosions caused by material degradation in petroleum refining operations and how the use of RIDM to understand the consequences of competing design choices related to dam safety that ultimately led to the prevention of catastrophic failure and loss of life during Hurricane Harvey in 2017. RIDM is then demonstrated to evaluate potential choices to satisfy the monitoring of communications channels and control circuity related to TPL-001-5.1.

The preoccupation with failure is not bad; as an engineer, it is a fundamental part of RIDM and successful designs.

XIII. Acknowledgment

We gratefully acknowledge the contributions of Ron Schwartz. Ron was a long-time employee of Schweitzer Engineering Laboratories, Inc. (SEL), served on the board of directors, and served many years as the senior vice president for quality. He was gracious and forthcoming with his knowledge of how to identify, measure, and improve processes to improve quality. He instilled in those that learned from him that engineers are responsible to understand and mitigate risk and how to use failure analysis as a tool to improve reliability. Ron was an inspiring, fun, creative, and helpful mentor, and friend.

We gratefully acknowledge the teachings of James Dolezilek. Jim was a successful artist and farmer who taught others to create or repair things on their own as he did. He instilled in others the process to first understand the relevant first principles and then use grit and determination to apply available tools and materials to solve problems. Jim was a fun, loving, helpful, resourceful, and creative teacher and father.

XIV. References

[1] "Risk and Performance Concepts in the NRC's Approach to Regulation," July 2020. Available: nrc.gov/about-nrc/regulatory/risk-informed/concept.html.

[2] H. Dezfuli, M. Stamatelatos, G. Maggio, C. Everett, R. Youngblood, P. Rutledge, A. Benjamin, R. Williams, C. Smith, and S. Guarro, *NASA Risk-Informed Decision Making Handbook*, April 2010. Available: ntrs.nasa.gov/api/citations/20100021361/downloads/20100021361.pdf.

[3] "Project 2022-02 Modifications to TPL-001 and MOD-032." Available: nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx.

[4] D. Dolezilek, "Hidden in Plain Sight: Anticipating and Avoiding Hidden Failures in Communications Assisted Protection," Montana Smart Energy Solutions Laboratory MSESL, Bozeman, MT, April 2021. Available: youtube.com/watch?v=lnTjb9bFx08.

[5] J. Markland and J. Martin, "SMAP Workshop," August 2015. Available: cpuc.ca.gov/-/media/cpuc-website/divisions/safety-policy-division/meeting-documents/smap-1-02-pgepresentationsmapworkshop_08032015.pdf.

[6] I. Anand, M. Chapariha, M.Rahmatian, G. Webster, S. Alaeddini, D. Erwin, S. Hayes, W. Winters and B. Varughese, "Challenges in Analyzing Single Points of Failure Based Tripping Sequence and Fault Clearing Time for TPL-001-5.1 Compliance," proceedings of the Western Protective Relay Conference, Spokane, WA, October 2022.

[7] Federal Energy Regulatory Commission, Department of Energy, "Transmission System Planning Performance Requirements for Extreme Weather," Federal Register, Vol. 88, No. 120, June 2023.

[8] "Element Inventory." Available: nerc.com/pa/RAPA/tads/Pages/ElementInventory.aspx.

[9] "Generating Availability Data System (GADS)." Available: nerc.com/pa/RAPA/gads/Pages/GeneratingAvailabilityDataSystem-(GADS).aspx.

[10] "Form EIA-860 Detailed Data With Previous Form Data (EIA-860A/860B)," U.S. Energy Information Administration, June 2023. Available: eia.gov/electricity/data/eia860.

[11] "Preliminary Monthly Electric Generator Inventory (Based on Form EIA-860M as a Supplement to Form EIA-860)," U.S. Energy Information Administration, July 2023. Available: eia.gov/electricity/data/eia860m/.

[12] "Annual Electric Power Industry Report, Form EIA-861 Detailed Data Files," U.S. Energy Information Administration, August 2023. Available: eia.gov/electricity/data/eia861/.

[13] GeoPlatform ArcGIS Online, "Homeland Infrastructure Foundation Level Database (HIFLD)," June 2023. Available: hifld-geoplatform.opendata.arcgis.com/datasets/geoplatform::transmission-lines/explorefilters=eyJWT0xUX0NMQVNTIjpbIlVOREVSIDEwMCJdfQ%3D%3D&showTable=true.

[14] IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 1: General Requirements*, 2010.

[15] "About NERC," North American Electric Reliability Corporation. Available: nerc.com/aboutnerc/Pages/default.aspx.

[16] *Risk-Informed Decision Making Guidelines*, Federal Energy Regulatory Commission, March 2016, Chap. 1, "Introduction to Risk Informed Decision Making." Available: vdocuments.mx/ferc-risk-informed-decision-making-decision-making-guidelines-chapter-1-124.html?page=1.

[17] D. Galic, "Updates to Reclaimation's Public Protection Guidelines," U.S. Department of the Interior, Bureau of Reclamation. Available: ussddamsandleveesbulletin-digital.com/damq/0223_summer_2023/MobilePagedArticle.action?articleId=1890407#articleId1890407.

[18] M. Silveira, D. Dolezilek, S. Wenke, and J. Yellajosula, "Cyber Vulnerability Assessment of a Digital Secondary System in an Electrical Substation," proceedings of the 74th Annual Conference for Protective Relay Engineers, College Station, TX, March 2021. Available: selinc.com.

[19] International Nuclear Safety Group, "A Framework for an Integrated Risk Informed Decision Making Process," INSAG-25, International Atomic Energy Agency, Vienna, 2011.

[20] M. Ross, J. Bettler, A. Sprenger, J. Silva, A. Wade, D. Dolezilek, M. Silveira, and R. Abboud, "Case Study: Defining and Measuring Protection Signal Transfer Speed, Latency, and Reliability Within Digital Trip Circuits," proceedings of the 75th Annual Conference for Protective Relay Engineers, College Station, TX, March 2022.

[21] D. Dolezilek, "Case Study of a Large Transmission and Distribution Substation Automation Project," August 1999. Available: selinc.com.

[22] G. Hammer, "Cofferdam Performance Hurricanes Harvey & Irma – 2017," proceedings of the Third Workshop on Case Histories in Dam Safety Risk-Informed Decision Making, Miami, Florida, May 2018.

[23] M. Ibrion, N. Paltrinieri, and A. Nejad, "Learning from Non-Failure of Onagawa Nuclear Power Station: An Accident Investigation Over its Life Cycle," Results in Engineering, ScienceDirect, 2020. Available: sciencedirect.com/science/article/pii/S2590123020300931.

[24] A. Omoto, *Reflections on the Fukushima Daiichi Nuclear Accident, Springer*, Cham, December 2014, Chap. 8, "Where Was the Weakness in Application of Defense-in-Depth Concept and Why?" pp. 131–164. Available: rdcu.be/dihVH.

[25] D. Uesako, "STAMP Applied to Fukushima Daiichi Nuclear Disaster and the Safety of Nuclear Power Plants in Japan," Massachusetts Institute of Technology, Cambridge, MA, June 2016.

[26] "The National Diet of Japan," Fukushima Nuclear Accident Independent Investigation Commission, The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission, Executive Summary, the National Diet of Japan, Japan, 2012. Available: nirs.org/wp-content/uploads/fukushima/naiic_report.pdf.

[27] National Research Council, *Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants*, The National Academies Press, Washington, DC, 2014.

[28] C. Synolakis and U. Kânoğlu, "The Fukushima Accident Was Preventable," Tsunamis: Bridging Science, Engineering and Society, The Royal Society, October 2015.

[29] Government of Japan, "Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety: The Accident at TEPCO's Fukushima Nuclear Power Stations," Nuclear Emergency Response Headquarters, Tokyo, June 2011. Available: iaea.org/report-japanese-government-iaea-ministerial-conference-nuclear-safety-accident-tepcos-fukushima-nuclear-power-stations.

[30] Government of Japan, "IAEA Mission to Onagawa Nuclear Power Station to Examine the Performance of Systems, Structures And Components Following the Great East Japanese Earthquake and Tsunami," Onagawa and Tokyo, Japan, July/August, 2012. Available: iaea.org/report-japanese-government-iaea-ministerial-conference-nuclear-safety-accident-tepcos-fukushima-nuclear-power-stations.

[31] IEC TR 61850-90-12:2020, *Communication Networks and Systems for Power Utility Automation – Part 90-12: Wide Area Network Engineering Guidelines*, 2020.

[32] IEC 62439-3:2021, *Industrial Communication Networks – High Availability Automation Networks – Part 3: Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR)*, 2021.

[33] A. Rodriguez, C. Polanco, I. Otarola, and J. Uzcategui, "Redundancy Techniques in a Digital IEC 61850 Substation PAC system," PAC World, December 2021. Available: pacw.org/redundancy-techniques-in-a-digital-iec-61850-substation-pac-system-2.

[34] J. Berger and J. Garthwaite, "Stanford Experts Discuss the Lessons and Legacy of the Fukushima Nuclear Disaster," Stanford, March 2021. Available: news.stanford.edu/2021/03/11/lessons-fukushima-disaster-10-years-later/?utm_source=Stanford+Report&utm_campaign=4c92bf3f7f-EMAIL_CAMPAIGN_2021_03_11_06_07&utm_medium=email&utm_term=0_29ce9f751e-4c92bf3f7f-54326365.

[35] J. M. Acton and M. Hibbs, "Why Fukushima Was Preventable," Carnegie Endowment For International Peace, March 2012. Available: carnegieendowment.org/2012/03/06/why-fukushima-was-preventable-pub-47361.

[36] IEEE Board of Directors, "IEEE Code of Ethics," June 2020. Available: ieee.org/content/dam/ieee-org/ieee/web/org/about/corporate/ieee-code-of-ethics.pdf.

XV. Biographies

Davis Erwin received his BSEE and MSEE from New Mexico State University and is a registered professional engineer in California. He has been with PG&E system protection since 1999, supporting 500 kV protection systems and remedial action scheme implementation. He is presently the senior manager of the group. He was a member of the NERC standard drafting team for PRC-012-2, serves as the vice chair of the WECC Remedial Action Scheme Reliability Subcommittee, and is a member of the NERC System Protection and Control Working Group.

Heather Torres is an expert protection engineer, earned a BSEE from California State University Sacramento, and earned an MBA from University of Phoenix. Heather has 20 years of protection experience with 2 years as the supervisor of the PG&E northern system protection group, which included developing Lean Six Sigma Black Belt and IAM certifications. Heather provides PG&E protection support for generator interconnection projects on the transmission system, which includes performing or overseeing initial scoping, feasibility studies, generation modeling, and system protection impacts of all transmission interconnections, reviewing interconnection locations and protection requirements for each transmission interconnection. Heather is lead of the PG&E protection asset relay replacement program, which includes the evaluation and replacement of a fleet of more than 31,000 relays, and provides support to the financial and implementation teams.

Dan Hertel is a private consultant, performing construction cost estimating and constructability review at Engineering Solutions, LLC. Dan is a registered professional engineer and engineering consultant. With his 40-year background in the construction of dams, pipelines, and other water resource projects, Dan provides constructability reviews, cost estimates, value engineering, risk management, and engineering support services to the engineering profession. He has been a private consultant since 2010, providing services on major dam projects in the United States for a variety of federal, state, and local agencies and engineers. His career includes 20 years as vice president with Barnard Construction Company, one of the USA premier dam constructors. During his career at Barnard Construction Company, Dan held positions as chief estimator, operations manager, and manager of business development. Dan is a member of the Association of State Dam Safety; past president, vice president, and treasurer of the United States Society on Dams; and a member of the International Committee on Large Dams.

Elaine Munch, PE (retired), worked for over 30 years in the petroleum refining and petrochemical industries. Her primary focus was facilities engineering, including inspection, maintenance, and replacement/upgrade of process equipment.

David Dolezilek, is a principal engineer at Schweitzer Engineering Laboratories, Inc. (SEL) and has three decades of experience in electric power protection, automation, communication, and control. He develops and implements innovative solutions to intricate power system challenges and teaches numerous topics as adjunct faculty. David is a patented inventor, has authored dozens of technical papers, and continues to research first principles of mission-critical technologies. Through his work, he has created methods to specify, design, and measure service-level specifications for digital communication of signals, including class, source, destination, bandwidth, speed, latency, jitter, and acceptable loss. As a result, he helped coin the term operational technology to explain the difference in performance and security requirements of Ethernet for mission-critical applications versus IT applications. David is a founding member of the DNP3 Technical Committee (IEEE 1815), a founding member of UCA2, and a founding member of both IEC 61850 Technical Committee 57 and IEC 62351 for security. He is a member of the IEEE, the IEEE Reliability Society, and several CIGRE working groups.