Title

Risk assessment and management for interconnected critical infrastructure systems at the site and regional levels in California's Sacramento-San Joaquin Delta

Permalink

https://escholarship.org/uc/item/7394j8j2

Journal

International Journal of Critical Infrastructures, 12(1/2)

ISSN

1475-3219

Authors

Roe, Emery
Bea, Robert G
Jonkman, Sebastiaan N
et al.

Publication Date

2016

DOI

10.1504/ijcis.2016.075867

Int. J. Critical Infrastructures, Vol. x, No. x, xxxx

Risk Assessment and Management (RAM) for Interconnected Critical Infrastructure Systems (ICIS) at the Site and Regional Levels in California's Sacramento – San Joaquin Delta[1]

E. Roe[1,2*], R.G. Bea[1,2], S.N. Jonkman[1,3], H. Faucher de Corn[1], H. Foster[1,2], J. Radke[1,2], P. Schulman[1,4], R. Storesund[1,5]

1 Resilient and Sustainable Infrastructure Networks Project (RESIN)
University of California, Berkeley, CA, USA
E-mail: emery.roe@berkeley.edu; bea@ce.berkeley.edu;
s.n.jonkman@tudelft.nl; henri.decorn@gmail.com;
h_foster@pacbell.net; ratt@berkeley.edu;
rune@storesundconsulting.com

- Corresponding author

2 Center for Catastrophic Risk Management
University of California, Berkeley, CA, USA

3 Delft University of Technology, Faculty of Civil Engineering and
Geosciences, Delft, the Netherlands

4 Mills College, Oakland CA, USA

5 Storesund Consulting, Kensington, CA, USA

Abstract: This article summarizes research-in-progress for improved risk assessment and management (RAM) of critical infrastructures that interconnect across California's Sacramento-San Joaquin Delta. The need for improved RAM is patent in the Delta as elsewhere: A "patch and pray" stalemate has developed which focuses on short-term

---

[1] The University of California Berkeley RESIN project has been supported by the National Science Foundation (NSF) under EFRI Grant No. 0836047. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF. The authors acknowledge the many contributions of Dr. Kofi Inkabi during the first two years of the project. Conor Henley and Rachel Marzion undertook much of the work for the transportation analysis. Other current and former UC Berkeley students have been instrumental in the research and include: Kristi Black, Miles Brodsky, Carmen Cheung, Anna Harvey, Lynn Hiel, Jessica Ludy and Mary Matella. We also benefited from discussions with many in the public and private sectors. We single out Don Boland of the California Utilities Emergency Association and Sonny Fong of the California Department of Water Resources for their support at critical stages of the research. The three *IJCI* reviewers are especially thanked for their close reading. Any errors that remain are those of the authors alone. Readers interested in background material to the activities described in this article are referred to the RESIN website and its periodic updates at http://ccrm.berkeley.edu/resin/.

reactive marginal maintenance and emergency response and recovery systems, all pushing infrastructures—and their engineers, designers and operators—increasingly to their performance edges and beyond. The research focuses on water supply, transportation, energy and flood protection systems, all of which are embedded in a dynamic ecosystem and showing clear signs of deterioration. Provisional findings of research activities are discussed. This article addresses critical infrastructure modeling uncertainties and ways to better understand, reduce or otherwise accommodate human/organizational and informational uncertainties in any RAM focused at the interconnected critical infrastructure system level.

Keywords: critical infrastructures, risk assessment and management, flood risk, models, vulnerabilities, resilience, Sacramento-San Joaquin Delta

Bibliographical notes:

Emery Roe is a practicing policy analyst working on science, technology and environmental controversies. He specializes in developing better management strategies in large technical systems for the provision of high critical services, such as electricity and water. He is author or co-author of many articles and books, including *Taking Complexity Seriously* (1998), *Ecology, Engineering and Environment* (2002) and *High Reliability Management* (2008).

Robert Bea is a professor in civil and Environmental Engineering at UC Berkeley and the PI for the RESIN project at UC Berkeley. He has 55 years of experience in engineering and management of design, construction, maintenance, operation, and decommissioning engineered systems including offshore platforms, pipelines, and floating facilities. He began the stream of research that underlies this proposal in 1988 as a lead investigator of the catastrophic fires and explosions onboard the Piper Alpha platform in the North Sea. His research has involved investigations of the grounding of the Exxon Valdez, sinking of the passenger ferries Herald of Free Enterprise and the Estonia, failure of the NASA Columbia shuttle and the failure of the New Orleans hurricane protection system during hurricane Katrina.

Sebastiaan (Bas) Jonkman Ph.D. is an assistant professor at Delft University and a Post Doctoral Researcher/ Visiting Scholar at UC Berkeley (Feb – Aug 2011). His research focuses on natural hazards and risk management, with a specific emphasis on flood risks. His PhD, completed at Delft University in the year 2007 (the Netherlands), examined loss of life estimation and flood risk assessment. He has worked for the Dutch government (Rijkswaterstaat) and Royal Haskoning (an engineering consultant). Bas has done flood risk management research and consulting in the Netherlands, United States (New Orleans and California), Vietnam, Cambodia, Indonesia and Romania.

H. de Corn obtained a BS from Ecole Polytechnique in France in 2009 before pursuing a MS at U.C Berkeley in civil engineering. From 2010 to 2011, he was part of the UC Berkeley RESIN team as a full time researcher. His research interests include quantification of human and organizational factors in risk assessments of critical infrastructures.

Howard Foster Ph.D. is a senior researcher in Geographic Information Science at UC Berkeley. He specializes in the application of digital library technology to characterize, access and retrieve spatial data and the development of federated, collaborative geographic information systems. He is developing methodology for the visualization of multi-attribute spatial information. He developed the information systems supporting this study and will be responsible for their maintenance into the future.

John Radke is an Associate Professor in the departments of Landscape Architecture & Environmental Planning, and City & Regional Planning at UC Berkeley. He specializes in building and applying spatial metrics to environmental problems. Within the RESIN Project he has developed the spatial components of the hazards and risk models used in this project. He has led the assessment of the impact of levee failures on the accessibility of the transportation network.

Paul Schulman is a Professor of Government at Mills College in Oakland, California. He has done extensive research on large-scale technical systems and high-reliability organizations, including NASA and the Apollo project, nuclear power plants, air-traffic control systems and most recently, the California electrical grid. He has been a consultant to the Lawrence Livermore National Laboratory, the Atomic Energy Control Board of Canada and the California Independent System operator. He has written *Large-Scale Policy Making* (Elsevier, 1980), numerous articles in academic journals and, with Emery Roe, *High Reliability Management* (Stanford University Press, 2008).

Rune Storesund, D.Eng., P.E., G.E. is a civil and geotechnical engineer with over 10 years of engineering planning, design, and construction experience and has worked on a variety of projects throughout California and the United States. He has participated in all aspects of engineering projects; from preliminary reviews to detailed analyses to construction observations and post-project monitoring. Rune holds a BA in Anthropology from the University of California, Santa Cruz; from the University of California Berkeley, he holds a BS in civil and environmental engineering, a MS in geotechnical engineering, and a Doctorate of Engineering (D.Eng) in Systems Engineering (“Life-Cycle, Reliability-Based River Restoration”). Within RESIN he utilizes his expertise to help develop a new interdisciplinary methodology for risk-based assessment and management of Interconnected, Interdependent, Interactive Complex Infrastructure Systems (I3CIS).

Risk Assessment and Management (RAM) for Interconnected Critical Infrastructure Systems (ICIS) at the Site and Regional Levels in California's Sacramento – San Joaquin Delta

ABSTRACT: Abstract: This article summarizes research-in-progress for improved risk assessment and management (RAM) of critical infrastructures that interconnect across California's Sacramento-San Joaquin Delta. The need for improved RAM is patent in the Delta as elsewhere: A "patch and pray" stalemate has developed which focuses on short-term reactive marginal maintenance and emergency response and recovery systems, all pushing infrastructures—and their engineers, designers and operators—increasingly to their performance edges and beyond. The research focuses on water supply, transportation, energy and flood protection systems, all of which are embedded in a dynamic ecosystem and showing clear signs of deterioration. Provisional findings of research activities are discussed. This article addresses critical infrastructure modeling uncertainties and ways to better understand, reduce or otherwise accommodate human/organizational and informational uncertainties in any RAM focused at the interconnected critical infrastructure system level.

KEYWORDS: Keywords: critical infrastructures, risk assessment and management, flood risk, models, vulnerabilities, resilience, Sacramento-San Joaquin Delta

1. Introduction

1.1 Background

With good reason, engineers and the engineering professions have viewed interconnected technical systems positively. History is full of advanced technologies and structures that benefit humankind. In the past, many people (and not just engineers) felt that these benefits exceed the costs of unexpected disruptions and failures emerging from increasingly complex and sophisticated systems. There has been growing concern, however, that vulnerabilities arising in what society considers strategically interconnected infrastructures pose new threats to those demonstrated benefits. Critical infrastructures are defined as assets and systems essential for the provision of vital societal services and include large engineered supplies for water, electricity, telecommunications, transportation and financial services [1].

Engineering communities have responded to the challenge of interconnected critical infrastructures in two related ways: Many primarily focus on better approaches to design out vulnerabilities, while others recognize vulnerabilities missed at the design or construction stages must be mitigated in subsequent operations and redesign. The UC Berkeley RESIN (Resilient and Sustainable Infrastructure Networks) initiative takes up the challenge in the following way. We seek to develop improved risk assessment and management (RAM) strategies for use by engineers throughout all stages of the any infrastructure's life cycle (from design to decommission) so as to reduce interinfrastructural vulnerabilities and optimize the benefits of cross-system interconnectivity. If vulnerability reduction and interconnectivity optimization are promoted through better RAM strategies, the resilience and sustainability of the infrastructures' critical services will be enhanced.

Why do engineers need improved RAM approaches for resilient and sustainable critical infrastructures? First, risk analysis is typically the charge of specific units within individual infrastructures; fewer approaches deal with explicit risk (that is, the probabilities and consequences of failure) at "the system of systems" scale, that is, the level of interconnected critical infrastructure systems (ICIS). A major feature of our research has been to take RAM methods proven at the infrastructure level and modify/extend them to the ICIS level. Second, a number of existing RAM methodologies are limited by their assumptions about and estimation of the various types of uncertainties that pervade infrastructural development and decisionmaking and we see methods that correct for that (more below). Last, key terms, including "resilience" and "sustainability," are under-conceptualized and rarely operationalized within infrastructures, let alone the ICIS level. The RESIN initiative in the National Science Foundation's Directorate of Engineering seeks to address these issues explicitly.

The specific goal of the UC Berkeley's RESIN Project (hereafter, "Project") has been to develop and validate approaches and strategies for risk assessment and management of interconnected infrastructure systems operating in the California Sacramento-San Joaquin Delta (hereafter, "Delta") and beyond. Practically, this has meant the development of

RAM methods that better address four general categories of uncertainties of major concern to engineers as risk assessors of infrastructures: (i) natural variabilities (Type 1), (ii) modeling uncertainties (Type 2), (iii) human/organizational factors (Type 3), and (iv) informational uncertainties related to data utilization in all stages of an infrastructure's life cycle (Type 4 uncertainty). The first two types of uncertainties can be treated as intrinsic. The last two are grouped as extrinsic in nature. This article has focused on the emerging methodological importance of modeling (Type 2) uncertainties, while underscoring the ongoing need to better understand, reduce or otherwise accommodate the extrinsic (Types 3 and 4) uncertainties in any RAM focused at the ICIS level.

This ambitious aim led to a set of Project activities that seek to better integrate human and organizational factors into risk analysis, assess connected networks of critical infrastructures, and develop new approaches for incorporating and modeling a wide range of uncertainties in risk assessments. This mandate, in turn, required an interdisciplinary approach from the outset. By mid-2011, our interdisciplinary team had involved more than 20 researchers from five disciplines: engineering, social sciences, environmental sciences, city and regional planning (most important, geographical information system specialists), and law. The interdisciplinary activities and research methods enabled us to develop and use the ICIS perspective as a unique platform to zoom in, out and across levels of analysis in terms of how infrastructures, their components, and their services interconnect. Our research to date has undertaken analyses of specific levees as well as site visits, discussions and a tabletop exercise with key decisionmakers, including state and federal infrastructure managers, emergency response officials, and support staff. As part of the methodological development of RAM approaches appropriate for the ICIS level of analysis, our research has also focused on the development of Geographical Information System (GIS) databases and their use in risk assessments and simulations.

This article reports on findings to date. Project activities remain a work in progress, and our final recommendations and methods will be left to the Project’s last year (2012). This article focuses on one of several themes emerging across Project activities as well as those activities. The connecting theme—the importance of assessing and managing modeling (Type 2) uncertainties better—is drawn out as we discuss Project’s site, regional and infrastructure-wide activities. We appreciate that improved risk assessment and management across critical infrastructures is of interest to more than engineers (e.g., cybersecurity specialists and others in CI(P) programs). However, this article centers on the engineering communities.

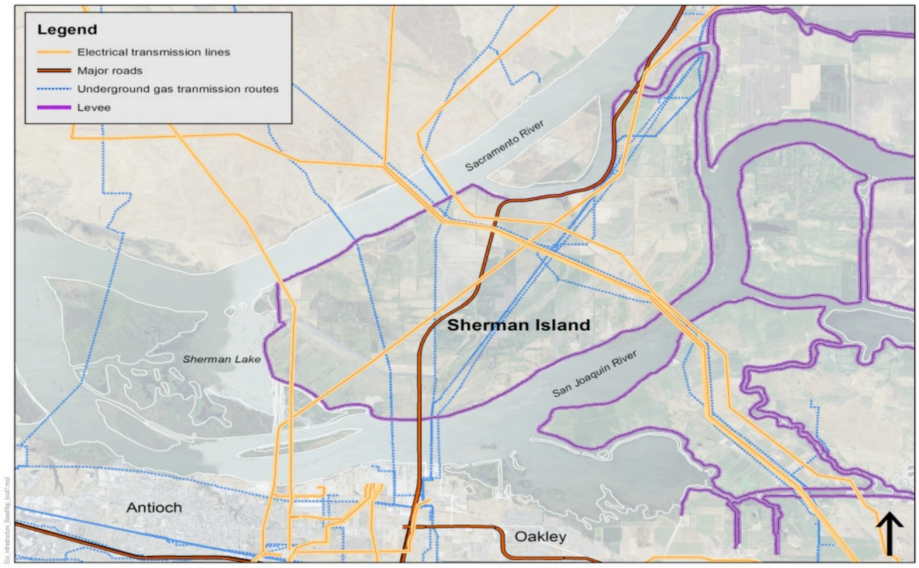
1.2 Sherman Island and the Sacramento-San Joaquin Delta

The area focus of Project research is the Sacramento-San Joaquin Delta, which has been called California’s “infrastructure crossroads.” The interconnections at the crossroads are live policy and management issues for counties, state agencies and the U.S. federal government. The infrastructures of research interest are those, which public and private entities uniformly acknowledge as of manifest importance. These include large-scale water supplies that supply over 20 million residents; a flood protection and levee system which past research has shown to be at great risk; an electricity transmission grid key to California and western North America; and a multimodal transportation system (roads, rail and shipping) that extends throughout the Pacific Rim. In the process of undertaking the research, we also found telecommunications, like electricity, to be a key infrastructure. These critical infrastructures take on added importance because the Delta itself is a one-of-a-kind aquatic-terrestrial ecosystem of international significance that could be harmed were the infrastructures to fail in certain ways.

We have adopted a "zooming in/zooming out/zooming across" approach to understanding how interconnected critical infrastructure systems operate. In terms of zooming in to how an ICIS exists at the site level, our methods and approaches have been developed and initially tested for one of the Delta's major western islands. Sherman Island (Figure 1), roughly 40km^2 with 29 km of levees [2], has been called "the cork in the bottle" of the Delta because of the critical infrastructures that pass under, on and over it. These include: natural gas pipelines: regional and inter-regional electricity transmission lines; two deepwater shipping channels that run alongside the island; and the presence of State Highway 160 (a link between major expressways Hwy 80 and 4, and a "short-cut" to California's state capitol and regional hub). In addition, the air shed above the Island and over the Delta is regulated at certain times of the year for emissions, while the Pacific Flyway, subject to international treaty, passes overhead and adjacent to the Lower Sherman Island Wildlife area (the remnant left after a 1969 levee breach). To give some perspective on the financial importance of these infrastructures, the 2009 five-year plan prepared for the Reclamation District for Sherman Island [2] quotes figures that estimate the closure of Highway 160 alone would cost approximately $70,000 per day of forgone benefits, while the cost of a two month outage of two major transmission lines to be some $42 million.

Sherman Island is also the gateway that, if flooded, would greatly increase the likelihood of saltwater intrusion into the Delta. The Delta not only serves those 20 million and more California residents and supports about 750,000 acres of irrigated farmland [3]. Over 2.5 million-acre feet of fresh water is transferred through the Delta each year [3]. Key informants have reiterated the strategic importance of Sherman Island to the management of the large-scale State Water Project (SWP) by the California Department of Water (DWR). A principal reason why DWR manages Sherman Island, chairs its Reclamation District and has made major improvements in its levees is because these efforts reduce the probability of having to shut down SWP pumps due to saltwater compromising Delta freshwater. (A major levee breach of Sherman would act as a big "gulp" drawing saltwater into areas supplied by freshwater rivers).

Figure 1 Sherman Island study area



As for zooming out, Sherman Island is a very useful platform for thinking through disciplinary or infrastructure-specific approaches and uncertainties associated with the conceptual modeling of interconnected critical infrastructures on a wide scale. The spatial region of the Sacramento-San Joaquin Delta is not coterminous with the geographical area covered by the specific infrastructure systems that cross the Delta. This is important, because water and electricity infrastructures, for example, are managed as systems. This means a failure of one or more elements co-located below, on or above Sherman Island (or any Delta island for that matter) has to be considered in terms of the design and management requirements of the infrastructure systems in which those elements play a part. An infrastructure system may be resilient precisely because it can bounce back from the loss of one of its elements. To assume the Delta region is its own "ICIS" can be very misleading, since the infrastructures involved are not actually managed and operated as systems contiguous with that region. The policy and management implications are considerable, as we shall see throughout this article.

In addition to using Sherman Island to zoom in and out with respect to different units and levels of analysis for ICIS RAM, the island also underscores the need to move across any given level of analysis in order to understand the fuller range of infrastructural interconnections. A closer look at Sherman Island in Figure 1 shows that an ICIS extends beyond a site of co-located elements of multiple critical infrastructures. For there are stretches of the Sherman Island levees that are not just elements in a Delta-wide flood protection system but also elements in other critical infrastructures. *The very same structure serves multiple infrastructure functions*. There is a stretch of Sherman Island levee over which part of Highway 160 runs; other stretches serve as the waterside banks of the deepwater shipping channels. There is another stretch that serves to protect a large wetland berm providing ecosystem services in terms of fishing and habitat. Moreover, any stretch of levee breaching on Sherman Island would directly increase the probability of DWR's State Water Project failing, given the intrusion of saltwater following the loss of the island. If such stretches of levee fail, so too by definition do the same structural elements fail in the deepwater shipping channel, Highway 160, the state's water supply, or the Delta's endangered habitat.

Consequently, an incompletely specified model or models of how the ICIS starts from the ground up and operates at different scales during different time periods adds considerable uncertainty to engineer-based RAM analyses. What is needed is a suite of methods and approaches that zoom in, out and across multiple level of risk analysis. This has significant repercussions for the calculation of the probability and consequences of interinfrastructural failure (Pf and Cf respectively), as described below.

1.3 Research Activities

The roadmap for the rest of the article is as follows. Core RESIN research activities and progress to date are each first described. These include GIS database development (section 2), assessment of transportation networks (section 3), probability assessment of a levee stretch failing (section 4) and the effects of human and organizational factors in improved risk assessment and management at the site level (section 5). An approach for analyzing risk in interconnected infrastructure systems, starting at the site level and moving to wider scales, is presented in section 6. As the reader will become aware, critical terms, such as sustainability and resilience, are used in different ways. Section 6 ends with our provisional findings in regard to better defining these key terms at the ICIS level. Section 7 places improved RAM strategies within a management approach found to take infrastructure risk seriously, that of high reliability management. We conclude with two sobering observations on the Delta flood protection infrastructure specifically (section 8). Since this article has many sections, we indicate major findings and conclusions in each section.

2. RESIN's Geographic Information System

The RESIN project's geographic information system (GIS) was developed to support ICIS research efforts, including detailed infrastructure failure probability studies; identification and analyses of co-located infrastructure elements where common-mode failures across infrastructures seem likely [4]; visualization of infrastructure vulnerability studies [5] (see also section 3); loss-of-life studies during a major Delta storm or earthquake event; and use during real-time RAM exercises, involving infrastructure managers and emergency responders. In these ways, the technology of RESIN's GIS is to become a component of a proposed technology delivery system for improved multi-agency planning and management of ICISs developed by the end of the Project in 2012.

2.1 GIS Technology in RESIN

In light of the interdisciplinary orientation to RAM, RESIN's GIS supports a wide range of users (both GIS-savvy and non-technical): data developers, researchers, students, stakeholders and those in the general public. Because of the widespread geographic distribution of RESIN participants, geo-data and the provision of GIS services require a coherent, centralized and well-documented facility by which, over the Internet, data can be contributed, searched, described, accessed and backed-up.

Our GIS serves RESIN users at two levels: top-level core raw data services (core data are geographic databases) and interpretive map authoring and publishing services (mid-level). Both support various clients—Web browsers and proprietary clients, such as ArcGIS Desktop, ArcGIS Explorer, and ArcGIS for iPad. Core data are served by PostGIS [6, 7] and ArcSDE [8]. PostGIS can serve spatial data directly to open source servers and clients, supports a wide range of text and spatial search features, and acts as the data store for ArcSDE, which serves spatial data in real-time to GIS desktop clients. Map authoring and publishing services are supplied by ArcGIS Server and ESRI's GIS cloud facility—www.arcgis.com.

Digitally published maps do not contain the same amount of information as the geographic databases used to create them. Thus, the maps can be used to communicate generalized geographic information without giving away sensitive details—the importance of which is now discussed below.

2.2 ICIS GIS Challenges

In November 2009 RESIN undertook a Sherman Island site visit and discussion that included private industry representatives (California Utilities Emergency Association), California state agencies with representatives from the California DWR, Sherman Island Reclamation District members and staff, and researchers.

The challenges of creating a shared, common-pool data-store were quickly made evident: Privately-owned infrastructure providers would resist making basic GIS data publically available because of security, proprietary, liability, and other reasons. Our experience has been that even public agency data are often not shared. (For example, U.S. Department of Homeland Security's Infrastructure Program "Gold" level data requires a declared emergency before being made available to state and local jurisdictions [9]). In light of advice given at our site visit and from subsequent discussions, we concluded: (i) GIS for emergency management must provide for the hiding of proprietary and sensitive data held by participants; (ii) such a system should be based on in-house engineering and GIS expertise within the infrastructures concerned in their production of infrastructure-specific vulnerability and status maps; and (iii) while these participants will not share core data, they will be more willing to share interpreted maps, distributed with GIS publishing services, as described previously.

We began prototyping such a system based upon ArcGIS map services published on www.arcgis.com and demonstrated it on August 2010 in a one-day tabletop exercise around a major Delta storm scenario and its effects on infrastructure operation in the region, including infrastructure elements on Sherman Island. This RESIN sponsored exercise, which was held at the State Operations Center (SOC) of the California Emergency Management Agency (CalEMA), involved control operators of major water supply and electricity distribution infrastructures and emergency responders as well as support staff and other agency personnel. The focus was on how a major forecasted storm crossing the western side of the Delta would affect their respective operations. Considerable attention was given to developing the storm scenario with the advice of major local and state infrastructure and emergency response managers. Without going into the scenario's specifics concerning Delta demographics and population centers, the forecasted storm was severe enough to ensure it would have to be addressed across multiple infrastructures (the ICIS level). On the other hand, it was not so severe as to be impossible to better prepare for within the forecast period, especially in terms of efforts to reduce or mitigate risk arising because the infrastructures are interconnected.

Prior to the SOC meeting, we developed map services based on gas, electrical power and water conveyance infrastructures. At the meeting these were projected on two large screens visible to all participants. We turned layers off and on and panned in and out to follow the conversations. The effect was to remove location ambiguity for participants and broadened their consideration to all the infrastructures displayed on the maps.

Our experience from the Sherman Island and SOC workshops confirms the value of GIS as an aid to the situational awareness of infrastructure operators and emergency responders when faced with a major scenario affecting key infrastructures. Many technical and social factors, however, challenge these GIS systems. A high level of GIS, modeling and engineering expertise is needed by participants to prepare the appropriate map services. Identification of the map services needed and when they are to be created or shared is complex, having case-by-case features. Graphic standards are needed to aid in the effective interpretation of the maps. In some cases core data must be shared for more advanced modeling. We see this in the example discussed in the following section (the modeling of flooding, road closure, access time, and route reconfiguration), where data might best be stored and maintained on separate servers. However, these challenges for developing a "common operating picture" through emergency management GISs are being addressed by Esri and others [10].

3. Assessing First Responder Access Via the Road Transportation Network: Flood Simulations and Accessibility

3.1 Background

The Delta road transportation network is owned and managed by many public entities that spatially overlap and operationally interconnect. This certainly holds for Sherman Island, where the impacts of levee failure and island inundation on Hwy 160 and the wider network of which it is part could be significant, extreme, and long term. These consequences of levee failure can be quantified as negative impacts on a transportation network's ability to function under adverse conditions [11], that is, its resilience.

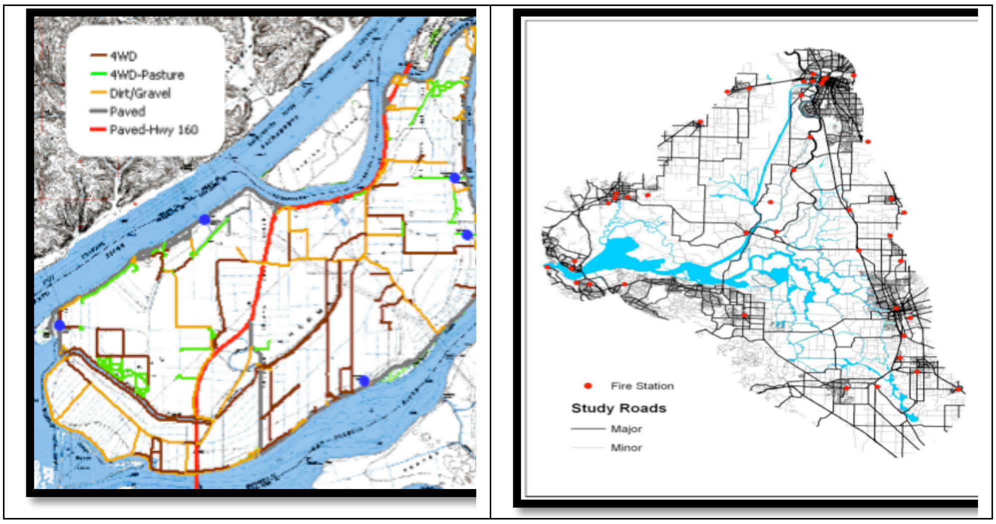
There is growing interest in policies, engineered designs and management strategies that ensure reliable and sustainable transportation systems and networks [12]. Although much of this literature examines and models flow and movement under normal growth scenarios [13], emerging research is examining impacts of catastrophic environmental events on network reliability and evacuation strategies [14-17]. Metrics have been identified to quantify the reliability of networks subject to adverse events and consequences [18]. Santos et al [11] outline four types of reliability metrics: connectivity, travel-time, capacity and vulnerability. The last measures how susceptible a network's accessibility is to the loss of a small number of links that cause the largest reduction in network performance. Studies have quantified consequences of flooding on interurban transportation network accessibility ranging from using small scale (county-based data) to relatively large scale for identifying critical transportation links [14]. However, data resolution remains somewhat aggregate, which necessarily introduces uncertainties when it comes to modeling that are not always fully recognized or acknowledged.

We adopted a strategy employing simulated levee failures and island flooding to model and quantify the consequences of accessibility loss for first responders to all citizens living in the inundated region. In one activity we model the large spatial scale (neighborhood) consequences and results from a levee storm failure on Sherman Island. In another activity we model over the Delta region the changes in the probability of citizen access to first responders given the failure of entire islands. Reported results are preliminary: We continue to adjust the inundation flood model simulations on Sherman Island, as we iteratively flood islands in the Delta region and calculate probability of access to first responders in our scenarios.

3.2 Methods

As indicated in section 2, we embed our modeling in the RESIN GIS. For our Sherman Island model we integrated high-resolution, digital ortho-photography (from US Geological Survey), with the latest available road network (2010 Tele-Atlas – mapped in Figure 2a) and high resolution LIDAR surface data (from the California DWR). We enhanced the Tele-Atlas data and field-verified using GPS (Global Positioning System) to develop an accurate Sherman Island transportation network (Figure 2b) with segmented road navigation characteristics (in this instance, speed capacity).

Figure 2 Sherman Island roads: field classified (left, 2a)—major and minor roads, and first responder locations (right, 2b)



<u>Sherman Island model</u>. A Sherman Island levee breach simulation was developed in light of the storm scenario to enable us to flood, measure and map the consequences to

road network accessibility on Sherman Island. Our initial execution of the model used a “bathtub” flood simulation approach that filled the entire island from lowest to highest elevations. Through key informant interviews we identified staging areas and access points of first responders. We modeled accessibility by first responders within the first hour, to all points on Sherman Island both before and after a flooding event begins.

Delta model. Suddeth et al [19] used historic data and generated risk of inundation for all Delta islands. We employ their predictions to generate island candidates for flooding and removal of road infrastructure elements. When removed, we calculated the impact on the probability of citizen access to first responders and mapped the change. Following Radke and Mu [20] we generated the probability of all citizen households being served by each first response unit. We measure this for the first 30-minutes, a reasonable response time for first responders. For each service area, the number of households is calculated based on the density of households in the corresponding 2000 Decennial Census block groups. We then modeled two inundation scenarios, one for Sherman Island and the other for Bouldin Island. [For further documentation see 20.]

3.3 Preliminary Results from Sherman Island and Challenges

Figure 3a maps the baseline accessibility for Sherman Island first responders in the first hour, while Figure 3c maps the altered accessibility surface during a levee breach scenario where the water level has reached -14 feet Mean Sea Level in that first hour. (Figure 3b shows the flooded areas at -14MSL, where main island roads become inundated). Green shaded areas in Figures 3a and 3c are by and large accessible within 20 minutes of travel time while red areas require closer to 1 hour to reach. As the water rises to -14MSL, accessibility to the island’s south-central section is quickly reduced, isolating its citizens from first responders within the critical first hour. Eventually the island floods to approximately MSL with only the tops of the levees remaining above water.

Figure 3 Results for the Sherman Island flood transportation analyses

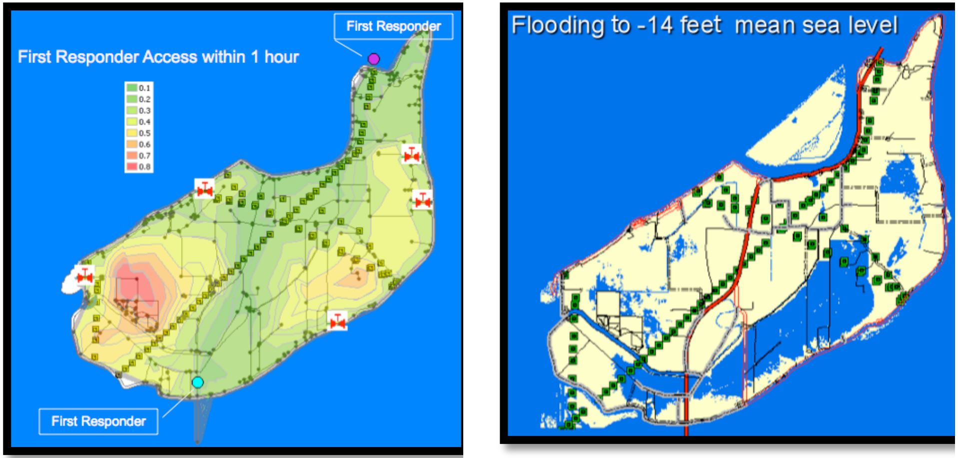


Figure 3a: First responder acces in the first hour

Figure 3b: Flood simulation to -14 feet MSL

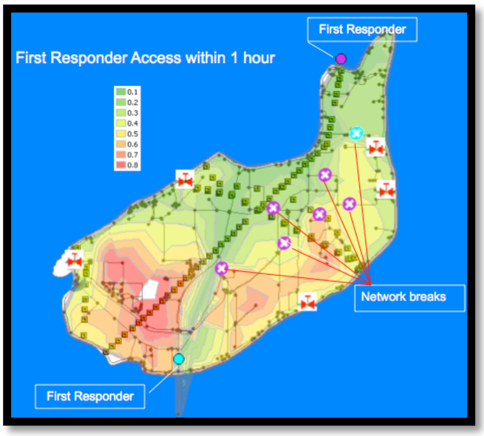
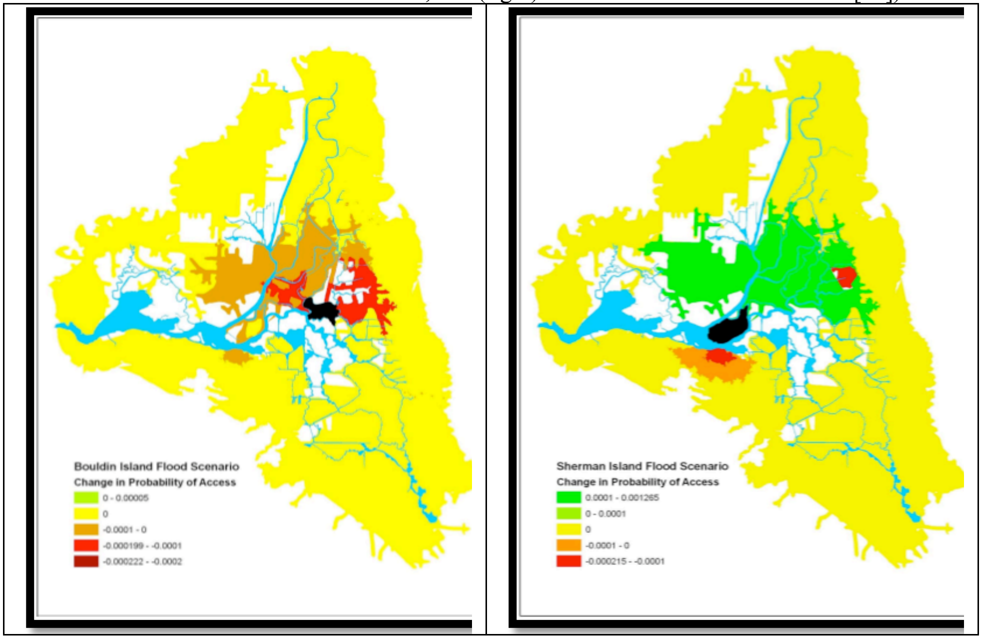


Figure 3c: First Responder Access in first hour (flooded to -14 feet MSL)

Figures 4a and 4b show results of simulated changes in the probability of first responder service for two island inundation scenarios (Bouldin and Sherman) compared to a no-flood scenario. Red areas map a decrease in accessibility; green areas depict increased accessibility. Yellow areas represent no change. Green areas with increased accessibility occur as citizens in that region have less competition to access of first responders, since their before-flooding competition has now been isolated due to flooded road segments.

Figure 4 Results for Delta transportation and first response analysis (Figure shows the probability of first responder access and service area extent between no flooding scenario and: (left) a Bouldin Island Flood Scenario, and (right) Sherman Island Flood Scenario [21])



3.4 Discussion and Further Work

The Sherman Island inundation maps reveal infrastructure elements quickly become affected during a flood event. As can be seen, levee breaches on different islands have different consequences for those elements related to the road network in and around the Delta. In order to model scenarios at a large scale, more aerial photo interpretation would be needed along with solid field verification in order to reduce modeling uncertainties.

It is nonetheless clear from our transportation analyses, the tabletop exercises and key informant discussions to this point that different crisis scenarios—e.g., a major storm versus an earthquake—entail different infrastructure consequences. Not only do different scenarios affect different infrastructure elements (e.g., different islands have different structures), but in doing so they also entail different interinfrastructural interactions (e.g., our five-day storm forecast clearly gave control operators and emergency responders more time to prepare than would be the case with a major earthquake affecting the Delta).

Also analyzing Sherman Island within a Delta context underscores the limitations of treating Sherman Island on its own, as the infrastructure systems involved extend well beyond the island. For example, Figures 3a-c show the "bath tub" flooding of water into Sherman Island, demonstrating how road elements on the island are affected over time. It would be an altogether different simulation to show how the same levee breach would over the same interval affect the deepwater shipping channel that shares the structure being breached. In fact, we did not try to simulate channel and water transportation, as that would add considerable modeling uncertainty to the analysis.

We are currently testing the flood forecasting SOBEK simulation model by Deltares [22] to fine tune the inundation process and map out more realistic scenarios. To assess the vulnerability of the wider transportation network we continue to simulate flooding and assessing other islands, thereby calculating the potential impact within the Delta.

4. RAM Methods for Characterizing the Likelihood of Levee Failure Affecting Interconnected Critical Infrastructures

4.1 Background

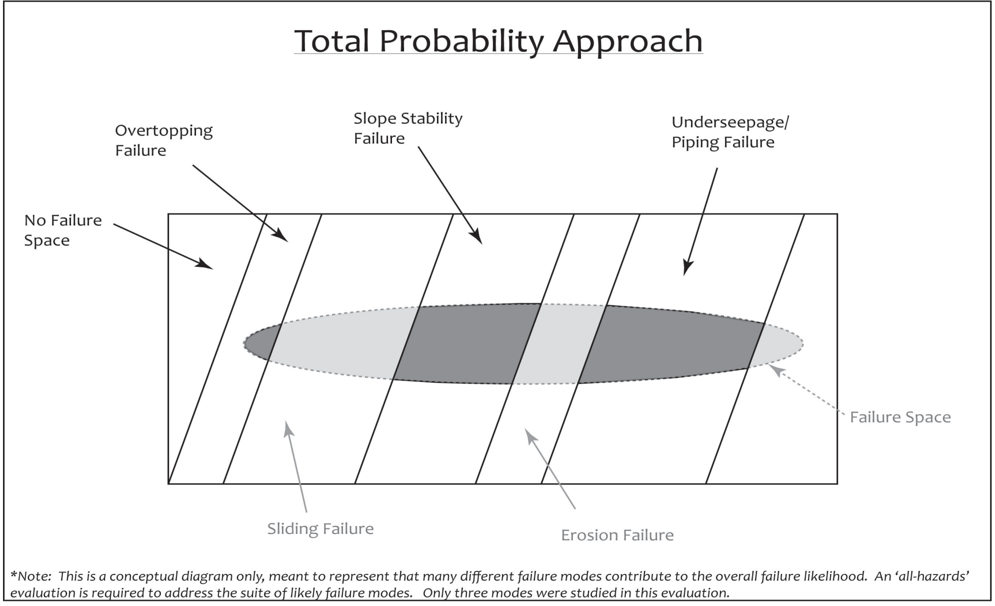
This activity develops, validates, and documents a probabilistic RAM method that explicitly addresses levee resilience and sustainability, using a case example from Sherman Island. In doing so, the activity examines performance now (2010) and projected future performance (2100) under a various water-level conditions, including forecasted variations in regional global climate change.

4.2 Methods

To explore the performance of the Sherman Island levees as a flood protection system, three failure modes (overtopping, seepage, and slope stability) and three annual storm return periods (i.e., 2, 50 and 100 years) are being analyzed, along with an explicit characterization of uncertainties involved: namely, those related to analytical modeling, human performance, and information development (Types 2-4, respectively). The choice of the intense storm hazard scenario and identification of the three failure modes was based on our review of the long-term history of performance of the Sherman Island and similar flood protection infrastructure systems in the California Delta and results from previous analyses of the risks associated with the Delta's levees [23]

The Total Probability Theorem [24, 25, 26] enables evaluation of individual failure modes so as to add these together to calculate the total probability of failure (Pf). For example, with respect to overtopping, we would calculate $Pf_{overtopping}$ as the probability of failure due to overtopping, given overtopping occurs. For a comprehensive understanding of Pf_{Total}, all relevant failure modes are evaluated and their individual Pfs summed to yield Pf_{Total}. In the case of an earthen levee, many failure modes are possible over the lifetime of the structure. Figure 5 illustrates this conceptually with the three failure modes of our analysis (overtopping, slope stability, and underseepage/piping). It must be stressed that up to this point, many Delta analyses of levee failure have focused on overtopping as the primary mode of failure [23]

Figure 5 Total probability approach provides framework for combed multiple failure modes



**Note: This is a conceptual diagram only, meant to represent that many different failure modes contribute to the overall failure likelihood. An 'all-hazards' evaluation is required to address the suite of likely failure modes. Only three modes were studied in this evaluation.*

4.3 Progress to Date

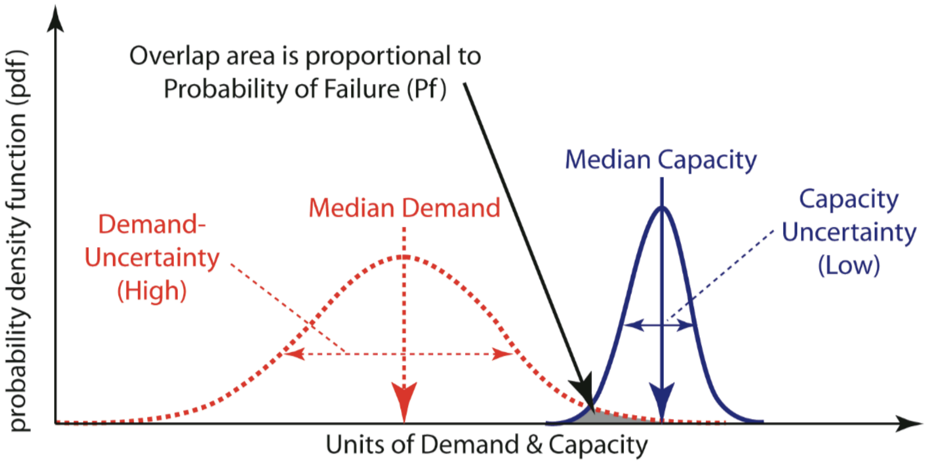
So far, the Project has addressed two major modes of failure of the Sherman Island flood protection infrastructure: seepage (levee soil hydraulic conductivity) and slope instability (level soil lateral instability). Investigation of the third failure mode, overtopping erosion, is currently being studied. As described, a primary Project objective is to address types of uncertainties not normally incorporated by engineers in their traditional risk analyses. This research activity specifically addressed Type 2 uncertainties associated with analytical models. These uncertainties are introduced into risk analyses by the imperfections that are incorporated in engineering analytical models.

These uncertainties include those associated with analytical model 'inputs', the analytical model's numerical analyses, and with the model 'outputs'.

In this research activity, the Type 2 (modeling) uncertainties were evaluated by making multiple comparisons between the results from prototype field tests and experiments and the results from analytical models that attempted to replicate or reproduce the results from these field analyses. This specification of the Type 2 uncertainties has two important effects on the estimation of the probabilities of levee failure (in this case, breaching leading to flooding of Sherman Island). The first is that they add to the total uncertainties that are addressed as part of the intrinsic uncertainties that include Type 1—natural variability—uncertainty. To the extent that the engineering risk assessor does not account for the full range of intrinsic uncertainties, the probability of failure is necessarily miscalculated. This is especially problematic when correlations with respect to the physical interrelationships between the analytical model's variables are not fully accounted for.

The second effect of Type 2 modeling uncertainties on the estimation of Pf is that they affect the central tendency and distribution characteristics of the probabilistic descriptions (probability density functions) used to define the demands and capacities for the infrastructure concerned. Basically, the probability of levee failure depends on the balance between demands imposed on the system (water levels, wind waves, seismic loading) and the capacity of the system to resist those demands (height of levees, side slopes of levees, etc.). Both demands and capacities have uncertainty associated with them. In this framework, the overlap between the demands and capacities is proportional to the probability of failure (Figure 6).

Figure 6 Overlapping demand and capacity probability density functions (pdf)

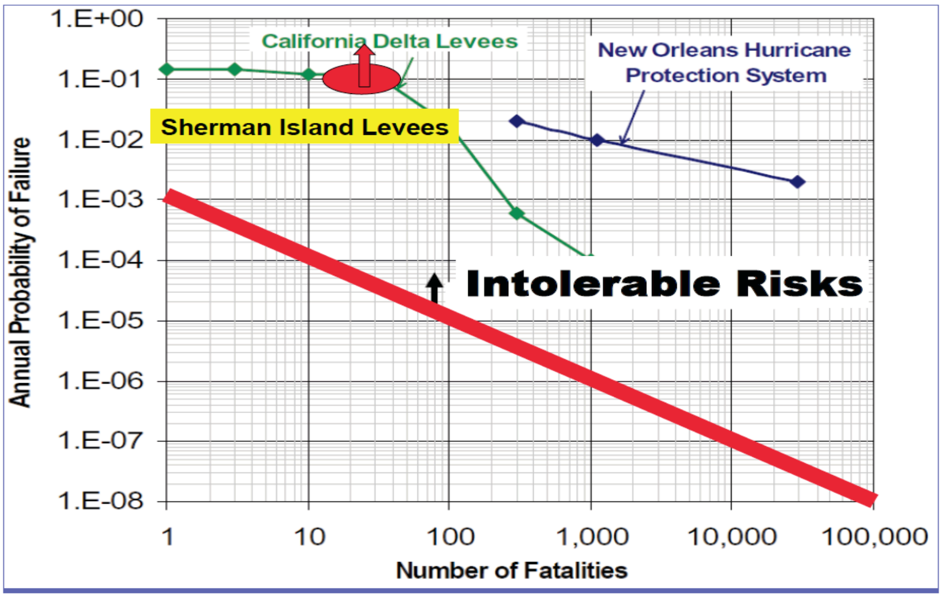


As drawn, uncertainty influences the shape of the actual demand and capacity curves. The larger the uncertainty, the wider the distributions have become, relative to their central tendencies. The more uncertainty and wider the distributions, the larger the overlap between distributions and the corresponding probability of failure, other things being equal. The more uncertain one must be with respect to demand and capacity, the greater is the estimated total value of Pf. In other words and in terms of this overlap between demands and capacities, the magnitude of uncertainty plays a major factor in the calculated total probability of failure: The more Type 2 (modeling) uncertainty, other things being equal, the greater the probability of failure.

The overall effect of including Type 2 uncertainties is thus to increase the probabilities of failure of the components that comprise the systems. This is not always the case, when the changes in the central tendencies and probabilistic distributions, through better analytic modeling, lead to reductions in the calculated probabilities of failure (the overlap in Figure 6 may decrease).

However, better modeling that reduces analytic uncertainty may find that the overlap of demand/capacity distributions is indeed large. Our work in this activity confirms that there is wide variability between tested models for seepage and lateral instability compared to what has been traditionally estimated as the probability of levee failure for Sherman Island. In fact, even without including the yet-to-be computed risk of overtopping, the results from our analyses of hydraulic conductivity—seepage—effects and from analyses of lateral stability alone indicate that for current (2010) conditions the annual probabilities of levee failure are "excessive." (The probabilities of failure are estimated to be even greater for future (2100) conditions.) To summarize, the notional probabilities of failure determined so far in the Project for both current and future conditions are clearly 'not acceptable'—they are intolerable—when compared with acceptability guidelines for other U.S. infrastructure systems (Figure 7).

Figure 7 Assessments of risks associated with failure of water protection levees in the California Delta, in the Greater New Orleans Area, and at Sherman Island for exposure to current severe storm conditions compared with example U.S. risk acceptability guidelines



4.4. Discussion

A first question is: “Are these notional probabilities of failure in Figure 7 realistic?” When these adjusted Pfs are compared to the historic—actuarial—estimates of levee failure in the Delta during extreme storms, they appear to be “excessive.” This is because “real trials” of the levees do not include Type 2 uncertainties. Analytical models have not been “tested” in any actual levee failure in the Delta, nor over the run of such failures. However, it is critically important that distribution and central tendency “corrections” with respect to Type 2 uncertainties be included, if only to result in analytical models that “on average” are able to reproduce what is observed in the field and across different scales. Experience-based estimates of Pf must be adjusted for the wide variability in modeling important failure modes that currently is under-recognized or ignored in traditional risk analyses.

The more general point here is that the full suite of uncertainties is generally omitted when estimating the probability of infrastructure failure. Omission directly affects decisionmaking and such incomplete risk analyses can do a great disservice. Without better accommodating the full suite of uncertainties, engineers may be recommending to decisionmakers investment in technologies, when that investment would be better used in correcting for the uncertainties already increasing the probability of failure.

5. Improved RAM at the Site Level: Extension of QMAS Methodology to Sherman Island

5.1 Background

Human and organizational factors play a major role in the performance of highly-engineered systems, but current RAM approaches often do not sufficiently account for them [25]. While there is a rich literature on “human error” in all stages of large technical systems, less attention has been given to how other humans operating these systems actually manage to prevent accidents waiting to happen in these increasingly under-funded infrastructures [26]. Human and organizational factors (HOF) have caused failures, but they also significantly reduce the risk of system or sub-system failure.

The challenge for engineers incorporating HOF into the design, production, management, and assessment of critical infrastructures is to adopt RAM strategies that model and accommodate increasingly interconnected and complex infrastructures throughout their life cycles. Risk estimates not only need to be updated constantly as dynamic conditions change; RAM also needs to include the expertise of those with deep operational and management familiarity with the infrastructures under such changing conditions. Without such involvement, it is difficult to see how engineers and others can design and manage for infrastructure resilience and sustainability.

Our RESIN research relies on and improves a field-developed and tested RAM method that quantifies the probability of failure of an infrastructure element or specific system in terms of its HOF (the extrinsic factors contributing to failure) and consolidates that estimate with the estimate of failure due to physical or structural properties of that element or system (the intrinsic factors contributing to failure). This tool is QMAS

(Quality Management Assessment System), originally developed and tested by Bea and colleagues in the offshore oil industry [27].

The development and extension of the tested intrainfrastructural tool for as yet untested interinfrastructural applications has been a RESIN challenge that remains a work in progress. We reformatted the QMAS tool's initial protocols, modified original areas of concern (e.g., the procedures component has to take into account the wealth of intergovernmental laws and regulations related to the operation of water and energy infrastructures), and produced a new text and associated presentations for prototyping an interinfrastructural QMAS. We describe only one product of this research activity, the application of the improved QMAS instrument to floodfighting on Sherman Island in light of the storm scenario mentioned in the preceding section and used in the other activities. As before, levee failure equates to a levee breach and the task in this activity was to calculate the probability that floodflighting would itself fail, given the factors and tasks of concern to those local experts responsible for or knowledgeable about floodfighting requirements prior to any levee breach.

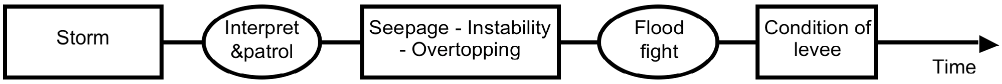
5.2 Method

QMAS has three steps: (i) system characterization; (ii) expert discussion; and (iii) Pf calculation. System characterization is to provide a detailed understanding of the system in question, generating an event tree representing first-round scenarios leading to failure. This step is based on a literature review and discussions with subject area specialists, which were undertaken prior to the exercise on Sherman Island in June 2011. The second step, expert discussion, occurred that day at the Island Reclamation District office and involved three risk assessors, the District engineer, the District supervisor, and a DWR field expert with deep familiarity of the Island and surroundings. The value of QMAS is that it is a formal tool that enables field experts to translate their experience and knowledge into structured risk assessments. The last step assembles the results of the assessment into a probability of failure calculation.

The focus in the QMAS method we were prototyping that day was on floodfighting, given its importance to levee flood protection (section 4). Criteria for choosing qualified risk assessors were developed prior to assessor selection. Our prototype does not presume that there can ever be "complete knowledge" of interinfrastructural risk, but rather that those who have operational knowledge of their respective systems can interact together in structured ways to produce more reliable Pf and Cf estimates at the ICIS level.

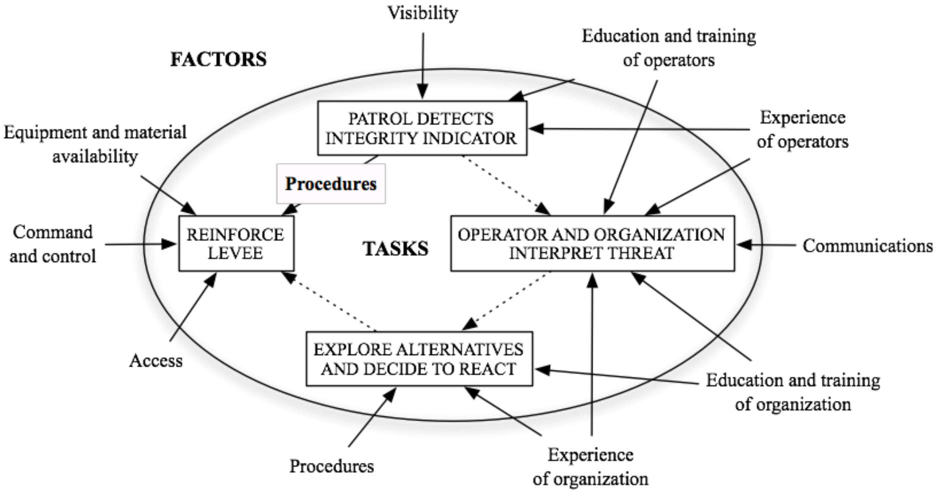
To illustrate the method, the following diagram (Figure 8) lays out the events leading to failure in floodfighting (notice the failure modes for levees remain seepage, instability and overtopping as in section 4).

Figure 8 Events leading to failure in floodfighting



The squares represent events associated with the performance of the system, be it the weather, levee or other physical feature. The circles are the actions taken by the floodfighters in response to physical conditions. The three assessors, who were expert in floodfighting processes involving Sherman Island, were first trained to use QMAS. They were then asked to identify all components of floodfighting involved in each task and to score them as described below. The QMAS components are detailed in Figure 9 and summarized as: operators, organizations, structures, procedures, environment, hardware, and interfaces between and among the other components.

Figure 9 QMAS factors and tasks in floodfighting

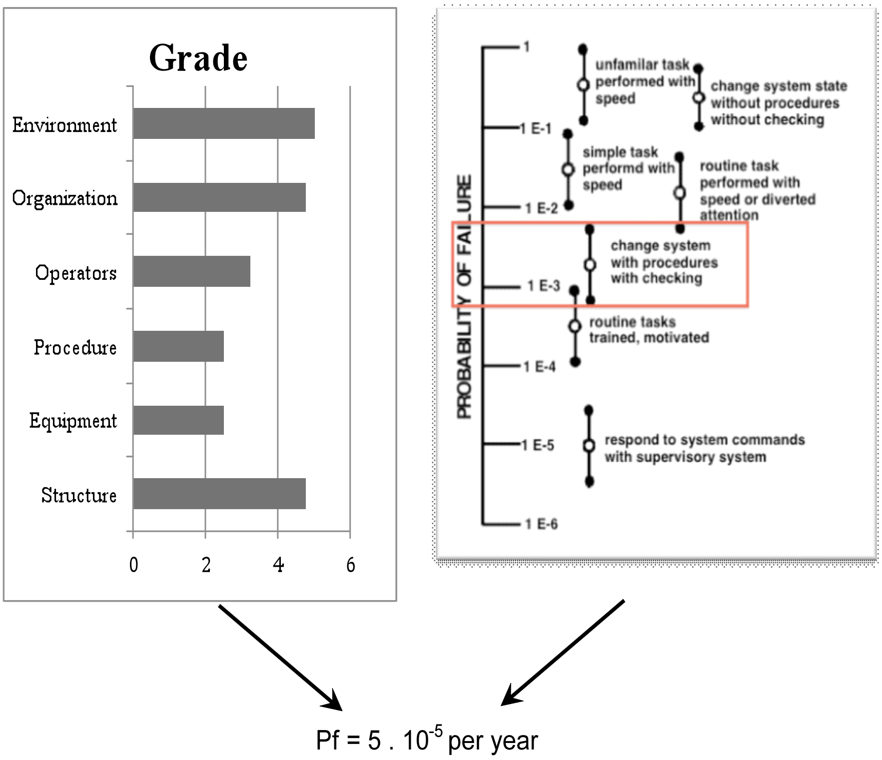


When assessors set out the components in the detail they require, they then grade each in terms of a scale that indicates their assessment of the current efficacy of each, on a scale of one (excellent/best) to seven (very poor/worst). The grading has several purposes. It allows the expert team to highlight varying degrees of concern when it comes to floodfighting. Identification of concerns through the grading protocol also enables assessors to assemble worse-case scenarios involving concatenations of the high-score concerns. Local operators and managers operating under the legal and regulatory mandates to be reliable may well have different worse-case scenarios than those who lack such local expertise.

5.3 Results and Challenges

The grades were used to quantify the probability of failure of each component being graded. For both Figure 8's 'interpret & patrol' and the 'flood fight' tasks, we determined the base probability of failure based on the literature [28]. The grades for each task component were then used to shape this base probability in order to take into account the expert knowledge of local site conditions. The data to determine the probability of failure of one of the floodfighting tasks are presented in Figure 10.

Figure 10 Floodfighting probability of failure



As a result of the exercise, a Pf was with respect to floodfighting was estimated to be in the order of magnitude of some five times ten to the minus five per year. As with all probability estimates in this article, this estimate of a low annual probability of failing in floodfighting is illustrative only. Here too readers must be aware of modeling uncertainties. While any low Pf estimated with respect to floodfighting offers some room to believe qualified expertise can mitigate the overall Pf of levee failure, section 4 underscores that the overall Pf of flood-related levee failure are already high. Fortunately, the QMAS methodology as been designed to be used in periodically updating of Pf and Cf estimates, in light of new information from field experts and others. Indeed, the probability of failure can only become more reliable as new information helps understand how the system functions.

The Sherman Island risk assessors offered other reasons during the exercise why any Pf of floodfighting may be higher than they estimated. The storm scenario was quickly identified by the assessors to be major enough to affect more than just Sherman Island, a finding also of the August 2010 tabletop exercise at CalEMA's State Operations Center (section 2). One "worse-case" scenario the three risk assessors wanted to develop further centered on the lack of available floodfighting capacity for Sherman Island due to that capacity having been allocated to floodfighting on other islands in the same storm.

6. Enhanced Risk Analysis for Interconnected Infrastructure Systems: Sherman Island and Beyond

6.1 Background

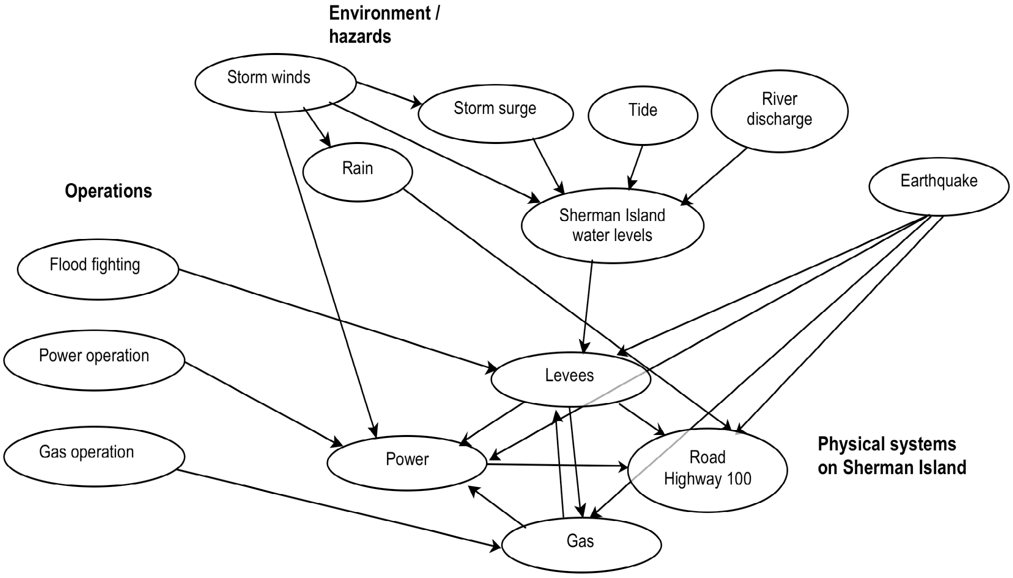
The earthquake and tsunami in Japan (March 2011) and the failure of the New Orleans levees in hurricane Katrina (2005), among many other examples, have demonstrated that such events can: (i) encompass multiple and different types of infrastructure; (ii) cascade to other infrastructures; and (iii) extend outside the area that is directly affected by the triggering event. A number of publications have assessed general aspects of risk associated with interconnected critical infrastructure systems [29-31].

This section returns to the overall goal of the RESIN research to develop and demonstrate specific methods for the (interdisciplinary and quantitative) analysis of risk in interconnected infrastructure systems. We build on preceding sections by integrating levee, transportation and human factors into risk analyses for multiple infrastructures. We draw from the body of work (e.g. [32, 33]) focusing on types of infrastructure systems typically found in highly developed and urbanized deltaic and coastal regions, starting with the Delta and extending to others, e.g., in the Netherlands, Japan and elsewhere

6.2 Risk Analysis for ICIS

For analysis purposes, risk is defined as a set of scenarios (s_i), each of which has a probability (p_i) and a consequence (x_i) [34]. To understand risk at the ICIS level, it is critical to identify scenarios that include interactions between various systems and to assess the probabilities and consequences for the interactions. This section follows Bea [27] in defining an engineered system in terms of environment (including hazards), operations (operators, organizations, procedures), and physical systems (structure and hardware). Influence diagrams are used to visualize how hazards, operations and physical systems interact. Figure 11 shows the characterization for Sherman Island.

Figure 11 Example of an influence diagram used for the risk analysis for various interconnected infrastructures for Sherman Island



A Bayesian network can be created that indicates the conditional probability of a failure event, given a set of conditions and/or failure of another system. Since RESIN methodologies for improved RAM are in the process of development the analysis here relies on previously published estimates and is illustrative only.

A Sherman Island probability of levee failure due to high water levels during storms has been estimated to be 0.0579 per year according to DRMS study methods [35]. In light of available information on flood conditions after breaching, the likelihood of breaching near other infrastructures and the vulnerability of the other infrastructures to flooding [36], it is possible to estimate the likelihood of failure of power and gas transmission lines on Sherman Island due to flooding. This simplified analysis indicates that for the DRMS flood scenario the conditional probabilities of failure for the power and gas lines on Sherman Island are 0.094 and 0.15 respectively. Causes for failure in this example are erosion of supports of towers and gas transmission lines near breach zones. The estimated failure probabilities of gas transmission lines on Sherman Island due to flooding ($\sim 10^{-2}$ to 10^{-3} per year) are much higher than typical frequencies of failure for gas transmission lines (10^{-6} per year per km, leading to about 10^{-5} per year for the total length of pipelines on Sherman Island). Important variables affecting the results, even in this simple illustration, would be the number of breaches and their likelihood along with the number of gas and powerlines near levees and their resistance to flood effects.

The preceding approach can be utilized to analyse failure probabilities for infrastructure elements on, e.g., Sherman Island, once better estimates of the Pf are available. For a more complete analysis of the effects of levee failure on power and gas transmission systems in the Delta, the positive redundancy and management options to prevent cascading impacts would have to be assessed, a topic addressed in the following section and an area of future work. This more realistic analysis would have to include iterative assessments as conditions and performance of infrastructure systems outside the flooded island(s) could affect the probability and consequences of failure on the island.

6.3 Special Case of Interdependent Critical Infrastructures

Interdependent systems are characterized by bi- or multi-directional interactions between two or more infrastructures (elements or systems). This too implies an interactive development of the states of various systems over time. The empirical evidence gathered by Luiijf et al [31] demonstrates that disruptions and failures due to infrastructural interdependencies are fewer than those due to dependencies (failure in one infrastructure leads to failure in another infrastructure, a failure which does not feed back into changing the state of the triggering infrastructure). Nonetheless, a simple example of an interdependent system consisting of a levee, road and floodfighting operations illustrates important conceptual and practical issues (Figure 12, next page).

The ICIS concept can be further refined in useful ways [37]. Commonly, risk analysis has two states, normal operations and failure. We found that for ICIS applications it is useful to distinguish at least three states: normal operation, disruption (e.g. a levee with seepage), and failure (i.e., the levee breaches). Transitions in multiple directions could occur between the states, not only degradation to a worse state with larger damage and disruption, but also recovery to a better state.

Figure 12 Interdependence between levees, floodfighting and condition of roads on Sherman Island and example of a Markov Chain for status of levees in a hypothetical case.

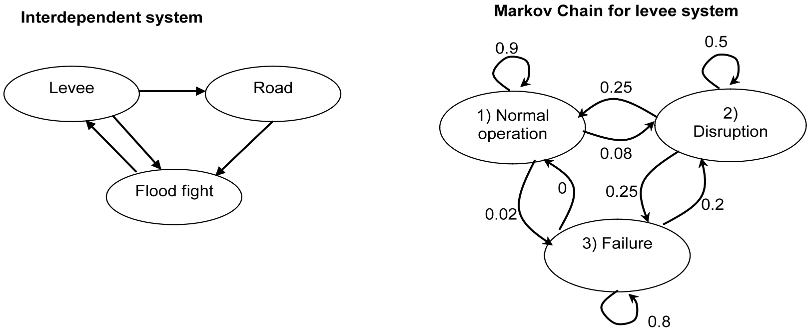


Figure 12 illustrates the relevance of distinguishing three states (including disruption) instead of two states (failure or not). Levee disruption (e.g., increased seepage) could lead to disruption and then the failure of roads and floodfighting, but it is also possible that floodfighting repairs that leakage. Markov chains can be used to analyze the development of the state(s) of such an interdependent systems over time. The right side of Figure 12 illustrates a simplified Markov chain for a single levee structure. It displays the transitions between states and the likelihood of transitions for every time step. Combinations of states of multiple infrastructures (or their elements) could be analyzed in this way, e.g. the combination of leaking levee, a flooded road and functioning floodfighting equipment. Markov chains can model the development of such interconnected infrastructure elements over time and the occurrence of various infrastructure states [38]. To do so would, however, introduces its own modeling and informational uncertainties. The size of the Markov chains grows rapidly with the number of systems (elements) and possible states and it is very challenging to find empirical information to elaborate these analyses for actual systems. Here too users and modelers face trade-offs in terms of budgets and expertise to refine the system modeling.

6.4 Discussion

Neglecting interdependencies and dependencies between failures or disruptions can lead to underestimation of the overall interinfrastructural risk. Many readers know this, but current design guidelines, management procedures and risk methodologies do not always appropriately take into account such interactions. In the Netherlands chemical facilities with very high legally required safety standards (failure probabilities smaller than 10^{-5} to 10^{-6} per year) are located in flood-prone areas behind levees with failure probabilities of 10^{-2} to 10^{-3} per year. Yet the chemical facilities are by no means designed to withstand flood conditions and the additional risk of failure of flood protection infrastructure is not taken into account by the government's guidelines for risk analysis for chemical facilities analyses [39].

One key question in analyzing the risk of interconnected infrastructure systems is the spatial scale(s) of analysis. We have seen how the physical boundaries of different infrastructures, including the areas that are affected by (natural) hazards and the regions in which the different management and disaster organizations operate, generally do not overlap nor coincide with the Delta regional boundaries.

6.5 ICIS Resilience and Sustainability

From an ICIS perspective, resilience and sustainability of any given infrastructure are *with respect to* or *conditional on* changes in the normal operations, disruptions and/or failures of the others infrastructures connected to it. Take a simplified example where the ICIS in question consists of two critical infrastructure systems, CIS1 and CIS2. Assume a change in the normal operations of CIS1 disrupts CIS2 normal operations, but only temporarily before CIS2 manages to return its normal state. In this way, normal operations in an infrastructure are *resilient* with respect to disruptions or failures in another infrastructure when the former maintains or returns to normal operations in the face of the latter. Sustainability can then be conceived as the persistence of normal operations in CIS2 relative to all stages in the loss of normal operations in CIS1. A sustainable CIS2 is one able throughout its life cycle—either by design, management, or both—to operate as if it were unconnected or only loosely coupled to CIS1.

Such distinctions matter, if only because unclear terms introduce modeling uncertainties into ICIS risk analysis and management. To pick one from many instances, conventionally wetlands in the Delta are considered part of the Delta as its own ecosystem [40]. Yet the ICIS perspective suggests that wetlands adjacent to levees and buffering wind and wave impacts on those levees should be considered as part of the levee system definition. This illustrates just one of the challenges ahead in reconciling the ICIS as a system of systems with other "system" definitions of the Deltas.

7. Importance of High Reliability Management for Infrastructures within an ICIS Context

7.1 Background

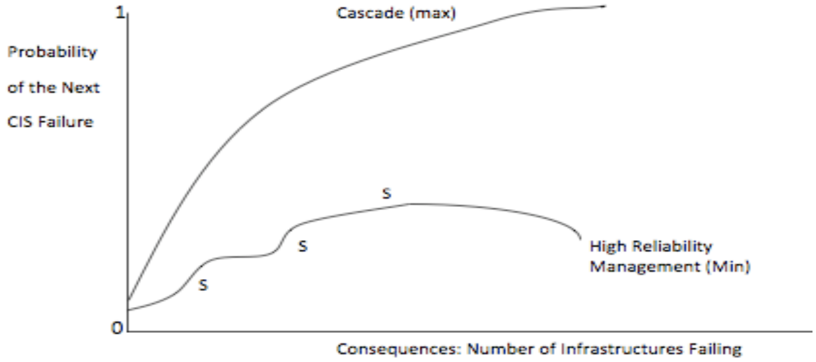
Improved RAM strategies, as with any risk analysis, are not ends on their own. They are to improve the actual reliability of critical infrastructures from design through to decommission. To that end, when it comes to adopting new risk methods and approaches, infrastructure operators must be involved and convinced about the benefits of RAM when it comes to more secure and safe operations. We know that improved RAM is being taken seriously when the infrastructure operators or emergency responders see the need and usefulness of deploying those methods to ensure the resilient/sustainable provision of the critical services. We call this willingness and ability to provide safe and continuous critical services under widely divergent conditions, high reliability management (HRM). Roe and Schulman [41] provide a review of the relevant literature, empirical evidence and findings. We see the RESIN activities described in this article as developing new tools for high reliability management.

7.2 Analytic Implications of High Reliability Management for RAM

Adding the full managerial component to the analysis of infrastructures that are functionally interconnected requires risk analysis to focus on a range between the worst outcomes of intrinsic or "natural" failures and the potentially best outcomes through "extrinsic" processes of high reliability management.

HRM can be posed as the "best case" in managing interconnectivity and establishing alternate "failure trajectories" at the other extreme from "worst case" cascade probabilities and consequences. The range between worst- and best-case probability distributions is illustrated in Figure 13.

Figure 13 ICIS risk trajectories – Maximum and minimum cases of ICIS risk



As drawn, the worst-case cascade trajectory is one without any intervening management. As each additional infrastructure fails in this scenario, it increases the probability of the next failure and so on, until all in the interconnected set have failed. In contrast, the lower trajectory reflects the best-case high reliability management in the infrastructures. Here, strategies in design and operations buffer one infrastructure failure and another by means of back-up resources, redundancies in key services, and automated protocols that when activated serve to uncouple tight interconnectivities. The increase in Pf in one infrastructure triggers management strategies to reduce what would have subsequently been higher Pfs in others. This is core to the resilience defined earlier.

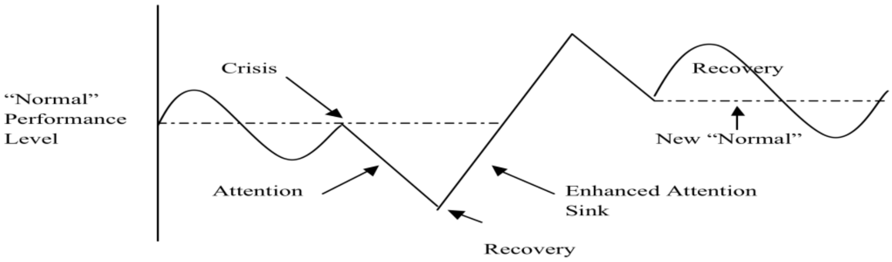
Certainly, interinfrastructural cascades can be induced or accelerated by management error. They however do not pose the same risk as do the worst-case endpoint of automatic, unmanageable cascades. Erroneously managed versus managed failure entail considerable risks, but they do not define the end points of the best and worst cases of risk. To summarize, in unmanageable situations, interconnections become tightly-coupled and compounding; in a highly managed situation, strategies are deployed to shift the nature of the interconnectivities so as to reduce their potential for failure (these shiftpoints are S in Figure 13).

The shiftpoints through managed interventions introduce slope changes in the probability trajectory of Pf in an ICIS. Some shifts involve what had been latent interconnections now becoming manifest and actual, and in so doing escalate follow-on Pfs. (Think here of the demand and capacity distributions in Figure 7 shifting in ways that increase their overlap.) Other shifts can be managed for, such as isolating a failed section of a transmission grid, or tapping floodfighters from other areas in a timely manner, thereby empirically reducing the probability of follow-on failure among infrastructures that remain operating (think here of reducing the overlap area in Figure 7).

7.3 Infrastructure Crisis Cycle, Control Variables and their Implications for Interactive RAM

Understanding managed shifts introduced by HRM in an otherwise unmanaged risk trajectory is thus critical to understanding the Pf of an ICIS. Research in control room operations of various critical infrastructures finds that operators are capable of adjusting their strategy and performance to changing conditions in the state of their infrastructures. These shifts in performance mode can define a "crisis cycle" in control room operations, as depicted schematically in Figure 14 below:

Figure 14 Crisis cycle in infrastructure management



Starting from the left side of Figure 14, control operators routinely maintain operations within bandwidths of reliable performance. They enter a crisis when they confront or anticipate conditions that threaten their skills to understand a situation through recognizing systemwide patterns and formulating localized action scenarios that they can translate into the continuance of reliable services. The time period for the crisis cycle among infrastructure operators may be advanced in every phase over managers of other infrastructures, public perceptions and even the perceptions of their leaders.

Outsiders to the infrastructure frequently think of a crisis as beginning with the "zero-point" of service, when a service, such as electricity, disappears altogether. But for the infrastructure managers and operators on the inside, the crisis may have begun earlier in the disruptions to their cognitive and management skills in ways outsiders do not see. In a similar way, recovery may well be underway earlier than the public understands or appreciates ([42] for more on the cycle).

This article has focused on three modes of operation: normal, disrupted and failed. From a crisis cycle perspective, recovery of infrastructure performance is also important and entails intense and extraordinary problem-solving activity by operators. They may be more concerned with Pf in the recovery stage than even in normal operations. Indeed, recovery is a period in which operators of interconnected infrastructures become aware that many previously latent interconnections are now very real for restoring capacity and service. Interinfrastructural restoration requirements are expressed directly in the need to coordinate control variables between and among the separate infrastructures.

Control variables are key elements or parameters, which through their management control the performance or state of a large technical system. These are the small number of manageable factors—load, generation, and frequency in the case of electrical grid operators—through which operators can exert leverage to adjust the larger state of the system. Each infrastructure has differing variables, though in some cases the variables are the same (e.g., rates of water flow can be a shared control variable, but in different ways for the state's large water supplies, shipping ports, and Coast Guard navigation service).

Assuming recovery efforts are successful, control operators return to ensuring infrastructure performance within bounded bandwidths. The end of the crisis cycle may leave operators in a "new normal" with better equipment that needed but were not able to secure beforehand, along with new response scenarios and new patterns to be used for control room situational awareness [43]. The new normal may, of course, be a more brittle state if fresh policies or regulations have been enacted that, albeit unintentionally, decrease rather than expand operator options.

What does it mean for improved engineering RAM when high reliability management is the context for to mitigating risk of failure of interconnected infrastructure systems? Minimally, we must move away from a narrow "human operator error" focus on large system failure, if only to understand how the very same humans manage to prevent system failures every day. Our first challenge is to better understand the managerial process in each infrastructure—its control variables, performance modes and options available to infrastructure managers and operators. Once that is achieved, it will be necessary to translate how changes in managerial capacity alter the probability trajectory of interconnected failure. This entails an interactive assessment of the capacity to shift away from the "natural" trajectory of concatenating failure. That interactive requirement is what makes an ongoing, updated and field-informed RAM such as QMAS attractive.

However—and this is the most important point—we must remember that high reliability management of our critical infrastructures is the best-case scenario for interconnected critical infrastructure systems. Our research to date has found key stakeholders insisting that Delta infrastructures have been negatively affected by all manner of capacity reductions (e.g., decreasing operating and capital budgets, high staff turnover) and demand increases (e.g., increasing demand for urban, agricultural, and environmental water uses).

8. Summary and Concluding Remarks

As with any research in progress, definitive conclusions and recommendations from the UC Berkeley RESIN Project would be premature. While further testing of our proposed ICIS RAM methods remains to be done, we have been focusing on methods and approaches that have proved useful within key disciplines and individual infrastructures, and initial findings have been positive.

That said, we would like to end with two unavoidable observations regarding the resilience and sustainability of the flood protection (levee) system in the Delta. First, this critically important infrastructure is clearly not sustainable for projected long-term future conditions. The current likelihoods and consequences of failure of the levee infrastructure are far too high, given current and foreseeable budget, investment and staff constraints relative to overall infrastructure demands. We have not been able to identify any realistic scenario where likelihoods and consequences of levee failure are lowered to acceptable and desirable levels, even taking into account floodfighting skills. If correct, a long term "strategic withdrawal" process from the Delta needs to be developed so that this and associated infrastructures can evolve in ways that do not compromise continuing provision of vital goods and services at sustainable levels elsewhere.

Second, findings so far must clearly lead policymakers to suppose this critically important levee infrastructure system is going to experience "on average" increased incidents of failure—breaching and flooding of Delta islands. This recognition places a high premium on development of emergency response capabilities to improve resilience of this and other critical infrastructures dependent on the flood protection system. The research team is engaged with the California Utilities Emergency Association for precisely this reason—to do what the team can do to help CUEA further develop the resilience capabilities of the California infrastructures for the Delta.

REFERENCES

[1] National Research Council (2009). *Science and Decisions: Advancing Risk Assessment*. Committee on Improving Risk Analysis Approaches Used by the U.S. EPA (from Executive Summary accessed online at http://www.nap.edu/catalog/12209.html).

[2] Hanson, J. C. (2009). *Reclamation District 341 Sherman Island Five-Year Plan* (SH 08-3.0. Five-Year Plan). California Department of Water Resources. Sacramento, CA.
[3] California Department of Water Resources, *Bulletin 132-07* accessed online at http://www.water.ca.gov/swpao/bulletin.cfm.
[4] Matella, M. (2010). "RESIN spatial cluster analysis: Preliminary results." Unpublished RESIN Research Report. UC Berkeley, Berkeley, CA.
[5] URS (2009). *Delta Risk Management Strategy: Section 4, Risk Analysis Methodology*. Prepared for California Department of Water Resources.
[6] Esri Inc. (2011), "Technical reference document: System design strategies," accessed on line at http://www.wiki.gis.com/wiki/index.php/System_Design_Strategies.
[7] Stonebraker, M. and G. Kemnitz, (1991). *The Postgres Next Generation Database Management System*. CACM 34(10), pp. 78-92 (also see http://developer.postgresql.org/pgdocs/postgres/history.html).
[8] Refractions Research, (2011) at http://postgis.refractions.net.
[9] Esri Inc. (2011b) "GIS for Homeland Security, SIG Meeting", Esri International User Conference, San Diego, CA.
[10] Esri Inc. (2011c). "Queensland floods and cyclones: How location intelligence helped in response and recovery." Esri International User Conference, San Diego, CA
[11] Santos, B., A. Antunes, and E. Miller, E. (2010). "Interurban road network planning model with accessibility and robustness objectives." *Transportation Planning Technology* 33(3), pp. 297-313.
[12] Jeon, C. and A. Amekudzi (2005). "Addressing sustainability in transportation systems". *Journal Of Infrastructure Systems* 11(1), pp. 31- 50.
[13] Hoogendoorn, S,P and P.H.L. Bovy. (2001). "State-of-the-art of vehicular traffic flow modeling." *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering June 1* 215(4), pp. 283-303.
[14] Sohn, J. (2006). "Evaluating the significance of highway network links under flood damage: An accessibility approach." *Transportation Research* 40(6), pp. 498.
[15] Kolen, B. and I, Helsloot (2009). "Evacuation, should things go wrong..." *Crisisrespone* 5(3), pp. 30 – 31.
[16] Van Zuilekom, K., E. De Romph, B. Kolen, and B. Thonus (2009). "Simulating traffic processes for practicing large scale evacuation." *Conference ICEM09*, Hague, NL.
[17] Friso, K., K.M. Zuilekom, B, van Kolen, and S. Holterman (2009). "If things do go wrong: lessons learned concerning traffic management during mass evacuation in case of possible extreme flooding in The Netherlands." *International conference on evacuation modeling and management* (*ICEM*) Delft.
[18] Miller, H. J. (1999). "Measuring space-time accessibility benefits within transportation networks: Basic theory and computational procedures." *Journal of Planning Literature, 14.1*.
[19] Suddeth, R., J. Mount, and J. Lund (2008). "Levee decisions and sustainability for the Delta." Public Policy Institute of California. *San Francisco Estuary and Watershed Science* 8(2), pp. 1-23.
[20] Radke, J. and L. Mu (2000). "Spatial decompositions, modeling and mapping service regions to predict access to social programs." *Geographic Information Sciences* 6(2), pp. 105-112.
[21] Henley, C.J. (2011). "Risk in the Sacramento-San Joaquin Delta: A study of emergency service access via the transportation network." Master of City Planning Professional Report, the Department of City and Regional Planning, UC, Berkeley.
[22] SOBEK, (2011). SOBEK Suite, accessed online at http://www.deltaressystems.com/hydro/product/108282/sobek-suite.

[23] URS (2009). *Delta Risk Management Strategy.* Multiple volumes prepared for California Department of Water Resources.
[24] Alfredo H-S, and W.H. Ang (1975). *Probability Concepts in Engineering Planning and Design - Volume I Basic Principles*. New York: John Wiley & Sons.
[25] Griffiths, G. A. (2008). *Risk Assessment in Geotechnical Engineering*. New Jersey: John Wiley & Sons.
[26] McCuen, B. M. (1997). *Probability, Statistics, and Reliability for Engineers and Scientists*, 2nd Ed. Boca Raton: CRC Press.
[27] Bea, R. (2002). "Human and organizational factors in reliability assessment and management of offshore structures." *Risk Analysis* 22(1), pp. 29-45.
[28] Williams, J. (1988). "A data-based method for assessing and reducing human error to improve operational performance." *Paper presented at Human Factors and Power Plants, 1988., Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants. June 5-9, 1988.* Monterey, California, USA.
[29] Johansson, J. and H Hassel (2010). "An approach for modelling interdependent infrastructures in the context of vulnerability analysis." *Reliability Engineering and System Safety* 95(12), pp. 1335-1344.
[30] Rinaldi, S.M. J. Peerenboom, and T.K. Kelly (2001). "Critical infrastructure Interdependencies." *IEEE Control Systems Magazine.* Issue: Dec. 2001, pp. 11-25.
[31] Luiijf, H.A.M., A.H. Nieuwenhuijs, M.H.A. Klaver, M.J.G van Eeten, and E Cruz (2010). "Empirical findings on European critical infrastructure dependencies." *Int. J. System of Systems Engineering* 2(1), pp. 3–18.
[32] Hastak, M., J.Dietz, E. Oh, and A. Deshmukh (2009). "2008 Midwest floods impact analysis on critical infrastructure, associated industries and communities.' *In: Proc. Of 2009 NSF Engineering Research and Innovation Conference, Honolulu, Hawaii.*
[33] URS (2009). *Delta Risk Management Strategy: Section 4, Risk Analysis Methodology.* Prepared for California Department of Water Resources.
[34] Kaplan, S. and B.J. Garrick (1981). 'On the quantitative definition of risk,' *Risk Analysis* 1(1), pp. 11-27.
[35] URS (2009). *Delta Risk Management Strategy: Section 13, Risk Analysis, 2005 Base Year Results.* Prepared for California Department of Water Resources.
[36] Antonioni, G., S. Bonvicini, G. Spadoni, V. Cozzani (2009). "Development of a framework for the risk assessment of Na-Tech accidental events.' *Reliability Engineering and System Safety.* 94(9), pp. 1442–1450.
[37] Nieuwenhuijs, A., H. Luiijf, and M. Klaver (2008). "Modeling Critical Infrastructure Dependencies." In IFIP International Federation for Information Processing 290, *Critical Infrastructure Protection II*, eds. M. Papa and S. Shenoi, (Boston: Springer), pp. 205-214.
[38] Sultana, S. and Z. Chen (2010). "Modeling flood induced interdependencies among hydroelectricity generating infrastructures." *Journal of Environmental Management* 90(11), pp. 3272-3282.
[39] Uijt de Haag, P. and B. Ale (2005). *Guidelines for Quantitative Risk Assessment – 'Purple Book'*. Publication CPR 18E.
[40] Healey, M.C., M.D. Dettinger, and R.B. Norgaard, eds. (2008). *The State of Bay-Delta Science, 2008*. Sacramento, CA: CALFED Science Program.
[41] Roe, E. and P. Schulman (2008). *High Reliability Management*. Stanford: Stanford University Press.
[42] Schulman, P. and E. Roe (2011). "A control room metric for evaluating success and failure in high reliability crisis management." *Policy and Society* 30(2), pp. 129-136.

[43] Garbis, C. and H. Artman (2004). “Team situational awareness as communication practice.” In *A Cognitive Approach to Situation Awareness: Theory and Application*, edited by S. Banbury and S. Tremblay; Great Britain: Ashgate Publishing, pp. 275-294.