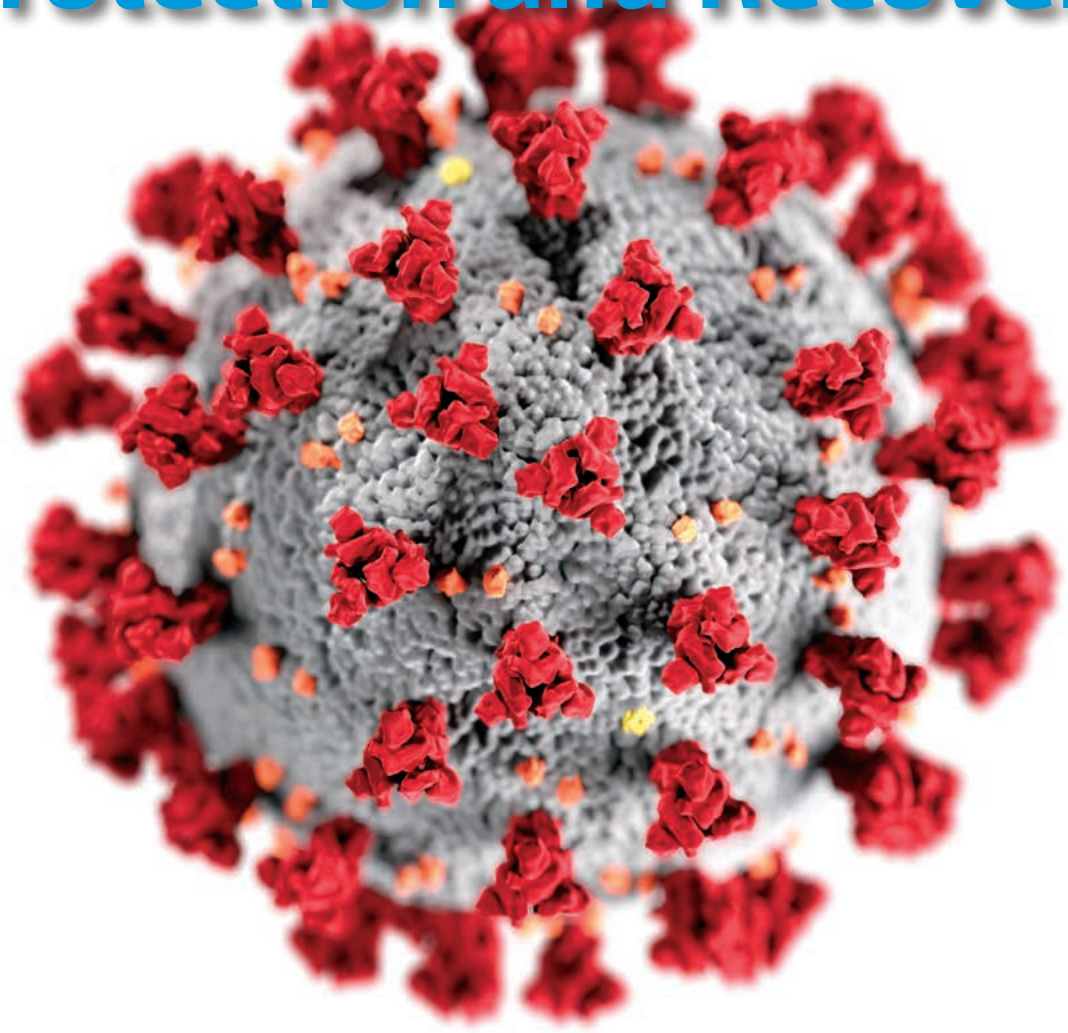
INSIGHT

This Issue's Feature:

Critical Infrastructure Protection and Recovery



JUNE 2020
VOLUME 23 / ISSUE 2

LOCKHEED MARTIN

This issue is sponsored by the Lockheed Martin Corporation.

INCOSE®

A PUBLICATION OF THE INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING

30th Annual INCOSE international symposium

Virtual Event
July 20 - 22, 2020

Join us for the 30th Annual INCOSE International Symposium and the 1st Virtual Edition

SYSTEMS ENGINEERING FOR EARTH'S FUTURE

Uniting Technology and Grand Challenges through Systems Engineering

The Premier International Systems Engineering Conference

3 Days, 3 Tracks, 3 Keynotes, 70+ Presentations, Panels, and More!

- **over 70** Papers, Presentations on Systems Engineering — Monday - Wednesday
- **3** Inspiring Keynote Speakers
  - **Bernie Fanaroff** - Former Director Square Kilometer Array (SKA) Project Office
  - **Dr. Ronnie S. McKenzie** - Managing Director, WRP
  - **Jakob van Zyl** - Hydrosat, Inc.
- **25** Countries Represented — **Argentina - Australia - Brazil - Canada - China - Finland - France - Germany - India - Ireland - Israel - Italy - Japan - Lithuania - Netherlands New Zealand - Norway - Singapore - South Africa - Sweden - Switzerland Thailand - Turkey - United Kingdom - United States**
- **19** Application Domains — **Top Domains: Enterprise Systems Engineering - Defense - Aerospace - Academia - IT/Telecom - Environmental Systems - Automotive - Energy - Autonomous Systems - City Planning - Infrastructure**
- **38** Topics Represented — **Top Topics: Systems Thinking - System Arch/Design Definition - MBSE - Needs and Req Definition - Processes - Systems of Systems - Complexity - Systems Science**
- **4** Panels — Monday - Wednesday

Including Topics Like These Discussed With Global Leaders in Systems Engineering
Aerospace - Systems Thinking - Defense - Diversity - System Security Teaching and Training - Cybernetics

SPONSOR INCOSE IS 2020!

1. Unique brand of recognition and visibility for your organization
2. Access to the latest thinking relevant to the practice of Systems Engineering
3. Put a spotlight on your organization's competency in Systems Engineering
4. Be associated with the highest culture of professionalism and innovation
5. Demonstrate organizational support to INCOSE's mission
6. Develop sustainable business relationships

Lots of possibilities to interact with systems engineering communities

Visit **www.incose.org/symp2020** and contact us **TODAY** - The IS2020 Organizing Team

INSIGHT

A PUBLICATION OF THE INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING

JUNE 2020 VOLUME 23 / ISSUE 2

Inside this issue

About This Publication

INFORMATION ABOUT INCOSE

INCOSE's membership extends to over 18,000 individual members and more than 100 corporations, government entities, and academic institutions. Its mission is to share, promote, and advance the best of systems engineering from across the globe for the benefit of humanity and the planet. INCOSE charters chapters worldwide, includes a corporate advisory board, and is led by elected officers and directors.

For more information, click here:
The International Council on Systems Engineering
(www.incose.org)

OVERVIEW

INSIGHT is the magazine of the International Council on Systems Engineering. It is published four times per year and features informative articles dedicated to advancing the state of practice in systems engineering and to close the gap with the state of the art. ***INSIGHT*** delivers practical information on current hot topics, implementations, and best practices, written in applications-driven style. There is an emphasis on practical applications, tutorials, guides, and case studies that result in successful outcomes. Explicitly identified opinion pieces, book reviews, and technology roadmapping complement articles to stimulate advancing the state of practice. ***INSIGHT*** is dedicated to advancing the INCOSE objectives of impactful products and accelerating the transformation of systems engineering to a model-based discipline.
Topics to be covered include resilient systems, model-based systems engineering, commercial-driven transformational systems engineering, natural systems, agile security, systems of systems, and cyber-physical systems across disciplines and domains of interest to the constituent groups in the systems engineering community: industry, government, and academia. Advances in practice often come from lateral connections of information dissemination across disciplines and domains. ***INSIGHT*** will track advances in the state of the art with follow-up, practically written articles to more rapidly disseminate knowledge to stimulate practice throughout the community.

ARTICLE SUBMISSION

INSIGHT@incose.org

Publication Schedule. ***INSIGHT*** is published four times per year. Issue and article submission deadlines are as follows:

- March 2020 issue – 2 January
- June 2020 issue – 2 April
- September 2020 issue – 1 July
- December 2020 issue – 1 October

For further information on submissions and issue themes, visit the INCOSE website: www.incose.org

ISSN 2156-485X; (print) ISSN 2156-4868 (online)

ADVERTISE

Readership
INSIGHT reaches over 18,000 individual members and uncounted employees and students of more than 100 CAB organizations worldwide. Readership includes engineers, manufacturers/purchasers, scientists, research & development processionals, presidents and CEOs, students and other professionals in systems engineering.

Issuance	Circulation
2020, Vol 23, 4 Issues	100% Paid

Contact us for Advertising and Corporate Sales Services
We have a complete range of advertising and publishing solutions professionally managed within our global team. From traditional print-based solutions to cutting-edge online technology the Wiley-Blackwell corporate sales service is your connection to minds that matter. For an overview of all our services please browse our site which is located under the Resources section. Contact our corporate sales team today to discuss the range of services available:

- Print advertising for non-US journals
- Email Table of Contents Sponsorship
- Reprints
- Supplement and sponsorship opportunities
- Books
- Custom Projects
- Online advertising

Click on the option below to email your enquiry to your nearest office:

- Asia & Australia corporatesalesaustralia@wiley.com
- Europe, Middle East & Africa (EMEA) corporatesaleseurope@wiley.com
- Japan corporatesalesjapan@wiley.com
- Korea corporatesaleskorea@wiley.com

USA (also Canada, and South/Central America):

- Healthcare Advertising corporatesalesusa@wiley.com
- Science Advertising Ads_sciences@wiley.com
- Reprints Commercialreprints@wiley.com
- Supplements, Sponsorship, Books and Custom Projects busdev@wiley.com

Or please contact:
Dan Nicholas, Associate Director – Sciences, Corporate Sales
Wiley
PHONE: +1 716-587-2181
E-MAIL: dnicholas@wiley.com

CONTACT

Questions or comments concerning:

Submissions, Editorial Policy, or Publication Management
Please contact: William Miller, Editor-in-Chief
insight@incose.org

Advertising—*please contact:*
Dan Nicholas, Associate Director
Sciences, Corporate Sales
PHONE: +1 716-587-2181
E-MAIL: dnicholas@wiley.com

Member Services – *please contact:* info@incose.org

ADVERTISER INDEX

INSIGHT volume 23, no. 2 is sponsored by the Lockheed Martin Corporation. LOCKHEED MARTIN

CORPORATE ADVISORY BOARD — MEMBER COMPANIES

321 Gang, Inc.
Aerospace Corporation, The
Airbus
Airbus Defense and Space
AM General LLC
Analog Devices, Inc.
Analytic Services
Aras Corp
Australian Department of Defence
Aviation Industry Corporation of China, Ltd
BAE Systems
Bechtel
Boeing Company, The
Bombardier Transportation
Booz Allen Hamilton Inc.
C.S. Draper Laboratory, Inc.
CACI International, Inc.
Carnegie Mellon University Software Engineering Institute
Change Vision, Inc
Colorado State University
Cornell University
Cranfield University
Cubic Corporation
Cummins, Inc.
CYBERNET MBSE
Defense Acquisition University
DENSO Create, Inc.
Drexel University
Eindhoven University of Technology
Embraer S.A.
ENAC
Federal Aviation Administration (U.S.)
Ford Motor Company
Fundacao Ezute
General Dynamics
General Motors
George Mason University
Georgia Institute of Technology
IBM
Idaho National Laboratory
ISAE SUPAERO
ISDEFE
ISID Engineering, LTD
iTiD Consulting, Ltd
Jacobs Engineering
Jama Software
Jet Propulsion Laboratory
John Deere & Company
Johns Hopkins University
KBR, Inc.
KEIO University
L3 Harris
Leidos
Lockheed Martin Corporation
Los Alamos National Laboratory
ManTech International Corporation
Maplesoft
Massachusetts Institute of Technology
MBDA (UK) Ltd.
Missouri University of Science & Technology
MITRE Corporation, The
Mitsubishi Aircraft Corporation (Mitsubishi Heavy Induftries Group)
National Aeronautics and Space Administration
National Security Agency - Enterprise
Naval Postgraduate School
Nissan Motor Co, Ltd
No Magic/Dassault Systems
Noblis
Northrop Grumman Corporation
Penn State University
Perspecta (formerly Vencore)
Prime Solutions Group, Inc.
Project Performance International
Raytheon Corporation
Roche Diagnostics
Rolls-Royce
Saab AB
Safran Electronics and Defence
SAIC
Sandia National Laboratories
Shell
Siemens
Sierra Nevada Corporation
Singapore Institute of Technology
Skoltech
SPEC Innovations
Stellar Solutions
Stevens Institute of Technology
Strategic Technical Services
Swedish Defence Materiel Administration
Systems Engineering Directorate
Systems Planning and Analysis
Thales
TNO
Trane Technologies
Tsinghua University
TUS Solution LLC
UK MoD
United Technologies Corporation
University of Arkansas
University of California San Diego
University of Connecticut
University of Maryland
University of Maryland, Baltimore County
University of Michigan, Ann Arbor
University of New South Wales, The, Canberra
University of Southern California
University of Texas at Dallas
University of Texas at El Paso, The
US Department of Defense, Deputy Assistant Secretary of Defense for Systems Engineering,
Veoneer, Inc
Vitech Corporation
Volvo Construction Equipment
Woodward Inc
Worcester Polytechnic Institute- WPI
Zuken, Inc

JUNE 2020
VOLUME 23/ ISSUE 2

FROM THE EDITOR-IN-CHIEF

William Miller, insight@incose.org

INSIGHT's mission is to provide informative articles on advancing the state of the practice of systems engineering. The intent is to accelerate the dissemination of knowledge to close the gap between the state of practice and the state of research as captured in *Systems Engineering*, the Journal of INCOSE, also published by Wiley. INCOSE thanks corporate advisory board (CAB) member Lockheed Martin for sponsoring *INSIGHT* in 2020 and welcomes additional sponsors, who may contact the INCOSE director for marketing and communications at marcom@incose.org.

The June 2020 issue of *INSIGHT* is a follow-up to our December 2016 publication, addressing *Critical Infrastructure Protection and Recovery*. The authors committed to this topic over a year ago and the publication now is unintentionally timely as we are amid a global pandemic from the novel coronavirus COV-19 that has demonstrated the fragility of our closely coupled global infrastructure. We thank theme editor Mitchell Kerman and the authors for sharing their contributions with our larger community. The theme of this issue represents the work of the INCOSE Critical Infrastructure Protection and Recovery (CIPR) Working Group with chair Daniel Eisenberg and co-chairs John Juhasz and Anthony Adebonojo. The purpose of the working group is to provide a forum for the application, development and dissemination of systems engineering principles, practices and solutions relating to critical infrastructure protection and recovery against manmade and natural events causing physical infrastructure system disruption for periods of a month or more. Critical infrastructures provide essential services underpinning modern societies. These infrastructures are networks forming a tightly coupled complex system cutting across multiple domains. They affect one another even if not physically connected. They are vulnerable to manufactured and natural events that can cause disruption for extended periods, resulting in societal disruptions and loss of life. The inability of critical infrastructures to withstand and recover from catastrophic events is a well-documented global issue. This is a complex systems problem needing immediate coordinated attention across traditional domain and governmental boundaries.

We lead with a prescient article, "Toward Building a Failsafe Hospital: The Impending Drug Resistant Pandemic," by Josh Sparber, written before the current pandemic. Josh writes that an adverse circumstance with immense potential for harm is the growing scourge of pandemics, specifically, those caused by drug-resistant microbial organisms. Systems engineers can use lean agile methods, incorporating the concept of antifragility to design systems responsive to reducing pandemic threats.

"Systems Theory Principles and Complex Systems Engineering Concepts for Protection and Resilience in Critical Infrastructure: Lessons from the Nuclear Sector" by Adam Williams presents US Sandia National Labs research exploring the safety, safeguards, and security risks and their mitigation for three different nuclear sector-related activities—spent nuclear fuel transportation, small modular reactors, and portable nuclear power reactors. The research shows that a systems-theoretic approach can better identify interdependencies, conflicts, gaps, and leverage points across traditional safety, security, and safeguards hazard mitigation strategies in the nuclear reactors, materials, and waste sector.

"Use of SysML to Generate Failure Modes and Effects Analyses for Microgrid Control Systems" by Myron Hecht presents a method for producing a failure modes and effects analysis (FMEA) from SysML together with an application to an electrical power microgrid control system. The significance of the method is the modeling of failure propagation which enables not only an automated approach but also additional results that systems engineers can use to support resiliency, safety, and cybersecurity.

"Microgrids—A Watershed Moment" by George Baker addresses the susceptibility of microgrid networks to cyberattacks and accidental or intentional electromagnetic interference-caused debilitation. Distributed microgrid energy sources are gaining momentum in displacing bulk electric power. We must ensure that we incorporate combined physical security, cybersecurity, and EMP protection engineering into the initial designs of microgrids to avoid increasing the vulnerability of our electric power networks.

"Defining Critical Communications Networks: Modelling Networks as Systems" by Thomas Manley, Susan Ronning, and William Scheible explains what critical communications networks are, where these networks fit within a systems-of-systems context, and what other systems must also be resilient, redundant, and reliable to ensure communication networks can continue to operate as designed. Short duration network outages can result in chaos within public transport systems, disrupt financial systems, and reduce business productivity. Short duration outages have the potential for loss of life of field utility workers, law enforcement field personnel, and alerting the public through emergency notification systems. The authors introduce systems engineering principles, techniques, and approaches that we can use to aid in the design of critical wireless and wireline

JUNE 2020
VOLUME 23/ ISSUE 2

communications networks for normal day-to-day operations, and for the protection and recovery of those networks during service disruptions caused by man-made and natural events.

"Emergency Systems and Power Outage Restoration Due to Infrastructure Damage from Major Floods and Disasters" by Romney Duffey examines extreme events where one major consequence is damage to infrastructure causing failures and loss of electrical power to vital systems, and restoration may take several days to weeks. This coupled system engineering problem involves the restoration of the initial outages depending on the damage caused and the reliability of emergency power and backup systems. The author reviews prior work and provides a detailed analysis of the probability of emergency system restoration and determine the needed response time and reliability requirements, with comparisons to the Fukushima Daiichi Nuclear Power Station events that resulted from unprecedented flooding due to an unexpected tsunami from a major earthquake, and with (b) the analogous extended loss of pumping power due to the massive flooding of New Orleans, US-LA by Hurricane Katrina. This new analysis quantifies the chance of restoration using systems engineering and emergency measures and replaces the frequently used qualitative system resilience terminology for coping with severe events.

"Loss of Offsite Power Recovery Modeling in United States Nuclear Power Plants" by Zhegang Ma, Curtis Smith, and Nancy Johnson addresses loss of offsite power (LOOP) that can have a major, adverse impact on a nuclear power plant's (NPP) ability to achieve and maintain safe shutdown conditions. The time required for subsequent restoration of offsite power after a LOOP event occurred and the probabilities of LOOP events exceeding various durations (or LOOP non-recovery probabilities) are important inputs to NPP probabilistic risk assessments (PRA). The authors review the analysis of LOOP events at United States commercial NPPs conducted by Idaho National Laboratory (INL) for the US Nuclear Regulatory Commission (NRC). They present the current LOOP recovery modeling that estimates probabilities of LOOP events exceeding various durations (or LOOP non-recovery probabilities) based on operating experience. NPPs use these LOOP results in PRA models for various risk-informed activities. Finally, the authors provide the LOOP non-recovery probability results for the four LOOP categories: plant-centered, switchyard-centered, grid-related, and weather-related with LOOP recovery data from 1988 to 2018.

We hope you find *INSIGHT*, the practitioners' magazine for systems engineers, informative and relevant. Feedback from readers is critical to the quality of *INSIGHT*. We encourage letters to the editor at insight@incose.org. Please include "letter to the editor" in the subject line. *INSIGHT* also continues to solicit contributions for special features, standalone articles, book reviews, and op-eds. For information about *INSIGHT*, including upcoming issues, see https://www.incose.org/products-and-publications/periodicals#INSIGHT. ■

Image credit for front cover: US CDC

Toward Building a Failsafe Hospital: The Impending Drug Resistant Pandemic

Josh Sparber, jsparbear5@gmail.com

■ **ABSTRACT**
Of late and during the last century, hospitals around the world and within the US have withstood war, floods, bad weather, bad actors, and other adverse circumstances. An adverse circumstance with great potential for harm is the growing scourge of pandemics, specifically, those caused by drug-resistant microbial organisms. Systems engineers can use lean agile methods, incorporating the concept of antifragility to design systems responsive to reducing pandemic threats. They can also integrate modeling concepts into this schema. System dynamics can describe the extant highly nonlinear and complex resource paradigms within SysML parametric blocks.

■ **KEYWORDS:** SAFe, superbugs, pandemic, antifragility, SysML, parametric, fractal, system dynamics, QSAR

INTRODUCTION: HOSPITAL SURVIVAL AROUND THE WORLD

Why I Wrote This Paper

Systems engineers are tackling wicked problems. One of these intense areas of concern is whether hospitals, a critical infrastructure, can extend their survival well past the existing expectation of a 72-hour exposure to a major existential threat. While power outages are often touted as the route toward ruin, hospital analysts themselves quote many other areas wherein ruin could emerge. Pandemics are one route.

Regarding the threat of pandemics, the Society for Disaster Medicine and Public Health states that its Citizen Ready® Program standardizes "disaster health education…[to] help attain national all-hazards preparedness goals by providing critical medical and mental health information to enable individual citizens to play a more effective role in local disaster planning and response, and ensure their integration into the overall emergency response system (2018)." In parallel to this, I seek a predesigned network that can proactively fend off impending pandemic doom.

UNCOMMON PROBLEMS, COMMON SOLUTIONS: HOSPITALS UNDER DURESS

Fairfield Medical Center in Lancaster, US-OH named five problems that dog the modern medical establishment in various degrees. These are delay in transfer of patients to other facilities, a lack of integration of physician services, communities where there are unaddressed pressing and immediate health issues, a communication gap between specialists, and a shortage of personnel trained at the physician level (Becker's Hospital Review 2011).

To some extent, we can trace a lack of resilience to a dearth of integrated services and business coordination and the need to train new cohorts for updated skills. To address the lack of communication, the Lancaster center created a new position, clinical nurse leaders (CNL) (Becker's Hospital Review 2011). Like case managers, the CNLs conjoin specialists together to target patient care (Becker's Hospital Review 2011). They address two other concerns through education.

The center addressed the shortage of physicians by establishing medical colleges in the local facilities (Becker's Hospital Review 2011). They remediated the community healthcare concerns with a healthcare commons to educate and help better the community, for example, bicycle paths to address some obesity issues (Becker's Hospital Review 2011). They addressed an approach to optimizing bed usage, a good practical metric for hospitals, by coordinating services and checking physician transfer performance (Becker's Hospital Review 2011). A common drug

registry prevented physicians from double prescribing opiates (Becker's Hospital Review 2011).

GLOBAL HEALTHCARE: A STATE OF SIEGE

The World Health Organization (WHO) states that the 10 major threats to healthcare overall (and this could be synonymous with hospital survival) have multiple causes (2019). The first five leading causes, beginning with the greatest contributors are: (1) continued fossil fuel burning leading to pollution and infection, (2) unhealthy lifestyle, (3) a resurge in influenza (flu), (4) 22% of the world population living with famine, conflict, and mass emigration, and (5) antibiotic resistance (WHO 2019). The remainder are (6) high threat pathogens: Ebola, Zika and SARS, (7) weak primary care systems or those drawn out by over focus on a local problem, (8) patients challenging the need for vaccinations, (9) mosquito-borne dengue, and (10) HIV-vulnerable individuals being excluded from intervention: sex workers, transgenders, male to male sex performers, and prisoners (WHO 2019). The word pandemic would encompass at least six out of these 10 threats, with the flu occupying the position of largest pandemic contributor.

The Center for Disease Control and Prevention developed a flu modeling program "called FluSurge to help hospitals plan…some pretty sobering scenarios…. In a bad pandemic, hospitals might have four times more people in need of a ventilator than they have ventilators, and far too few intensive care beds for the seriously ill" (Branwell 2018). In 2018, Dr. Jeffrey Duchin, head of infectious diseases for the Seattle and King County Public Health Department states, "Even before flu season struck here, our hospitals were struggling to cope…hospitals have large numbers of patients living in the hallways routinely… Flu season comes and it all gets worse" (Branwell 2018). Flu pandemics seem to strike unpredictably. There was a 40-year stretch between the flu pandemics of 1918 and 1957, then 11 years to the 1968 pandemic, followed by a 41-year hiatus until 2009 (Branwell 2018). "There is virtually no way to tell when the next will occur (Branwell 2018)."

More recent approaches may provide these institutions some hysteresis, some possible elasticity, to extend their resilience or enable an "operate through" window past the date of an accelerating damage trend. We can use multiple casualty incidents (MCI) as a measure of how much to invest in expanding adaptive capacity (Cristian 2018). The Pan American Health Organization (PAHO) monitors global threats and uses a hospital safety index rating system to discern hospital vulnerabilities (PAHO n.d.). "Due to the increased frequency and impact of disasters, including natural disasters, pandemics, and terrorism, the concept of disaster resilience is accepted as being of increasing importance (Cristian 2018)." Albanese et al. (2008) declare resilience and safety to include, among others, "institutional capacity building, education and training, …*information sharing, networking, and knowledge management* [emphasis is author's], and the provision of subject matter expertise. . . . [for] a community-wide disaster response." Having life-supporting resources like food, water, electricity, air conditioning, and accurate information make hospitals centers of support in extended crises (Albanese et al. 2008).

Nassim Taleb (2014, 88-92) calls large, human-controlled systems fragile. Large bureaucracies and monolithic business organizations cleave toward great stability and then suffer unintended drastic collapse when the reality of larger scale impinges upon their modus operandi . The shared assumption that things will go as planned is part of what Taleb calls "the overestimation of the reach of scientific knowledge" (2014, 10). The alacrity with which we need to apply real world solutions to these fragile enterprises calls for a special strategy.

ROLE OF LEAN AGILE: DOES LEAN + AGILE = LEAN AGILE?

Scott Jackson, co-chair of INCOSE's Resilience Working Group, has defined resilience in *Architecting Resilient Systems* (2010, 12), as risk avoidance, survival, and recovery. At least for complicated systems, of which hospitals seem a good example, the ability to recover from unavoidable damage would be key (Jackson 2010, 12). Jackson cites Hardman et al. (2015, 15). Hardman et al. state that systems of men and machines need to use a minimalist approach to problems in which "all necessary information is available, supplementary information is retrievable, and tasks are simplified to retrieve user memory load" (Jackson 2010, 170). This is the very description of a design approach known as agile.

According to Dr. Rick Hefner in a recent class at the California Institute of Technology, the design environment is changing to "individuals and interactions over processes and tools, working software over comprehensive documentation, customer collaboration over contract negotiation, and responding to change over following a plan" (Hefner and Crews 2018). From a systems point of view, agile is a good practice for complicated systems; wherein, cause and effect can be quite obscure and is an emergent practice for complex systems; wherein, cause and effect can only be traced in retrospect (Hefner and Crews 2018). Hospitals are at least complicated enterprises due to problems of scale, and complex due to the demanding level of expertise and interaction needed at various levels for these enterprises to function effectively.

The *Systems Engineering Handbook 4th ed.* states, "In complex systems…interactions between the parts exhibit self-organization, where local interactions give rise to novel, nonlocal, emergent patterns (Walden et al. 2015, 9)." The handbook defines complicated as "interactions between the many parts are governed by fixed relationships…. This allows reasonably reliable prediction of technical, time, and cost issues (Walden et al. 2015, 9)." We could use this definition to describe the hospital itself, as a complicated system consisting of a system of complex systems.

Lean introduces another dimension to agile based on curtailing process waste through a host of methods. Examples of lean methods are plan/do/check/act, five whys, continuous flow, cellular manufacturing, five S, total productive maintenance, takt time, standardized work, mistake proofing, and leveling the workload (Lynn 2019). The Scaled Agile Framework (SAFe) principles are a group guiding lean techniques applied to agile (SAFe 2019).

For those looking for a relatively quick adaptation to potential threats that will not compromise the scale of a large complicated system, or the essential complexities needed to run each individual department, SAFe could be a guiding force. Of the nine principles espoused by SAFe, "systems thinking…[and] basing milestones on objective evaluation of working systems" occupy spots two and five (2019). These would enable SAFe, with an enterprise success story building mission, to knit together complex resources according to an evolving enterprise level plan. This plan could accelerate sufficiently large-scale buy-in and sufficiently large-scale participation to encourage the use of SAFe methods. The efficiencies achieved by using lean agile could result in reduced risk and possibly an overall reduction in insurance costs as well. That would benefit everybody.

LEAN AGILE SUCCESS STORIES IN THE MEDICAL REALM

Several exemplars exist of SAFe success in the medical institutional realm. Eleckta is a Swedish human care group addressing cancer and brain disorders. The use of SAFe was key to uniting several agile

teams, dispersed across an enterprise of 3,800 people on three continents, and located in 30 countries (SAFe 2019). SAFe usage "has delivered significant gains and improvements in several areas, provided valuable lessons learned, as well as a roadmap to refine their value stream" (SAFe 2019). While engendering 20 development teams and four agile release trains (ARTs), SAFe development across Eleckta has refined developmental tooling, clarified reporting timelines, and introduced a common enterprise level software, Rally (SAFe 2019).

Phillips has instituted SAFe across its medical technology development group. According to Sundaresan Jagadeesan, program manager at Philips Electronic India Limited, "The Scaled Agile Framework (SAFe), with its non-linear approach and adaptability, is the way of the future" (SAFe 2019). He stated the following results: "average release cycle time down from 18 months to 6 months; feature cycle time reduced from [approximately] 240 to [less than] 100 days; sprint and program increment deliveries on time, leading to 'release on demand;' quality improvements—zero regressions in some business units; 5 major releases per train per year on demand" (SAFe 2019).

AstraZeneca, a pharmacology company, sites improved results of "significantly faster time to value delivery (40-60%), reduced team sizes (cost reduction of 25-40%), and improved quality (SAFe 2019)." AstraZeneca, using SAFe, united 20 diverse teams of a total 1,000 people, with each "train" now delivering five major releases per year (SAFe 2019). To the employees, the agile process now feels "personal and organic (SAFe 2019)."

COMBATING AN EXAMPLE PANDEMIC: THE THREAT OF DRUG-RESISTANT BACTERIA

Matt McCarthy, in *Superbugs*, describes a potential crisis of global concern impacting both the third world and a neglectful commercial sector in the developed world (2019, 107). Fleischmann et al. revealed through the accumulation of global data based on 45 studies and the application of estimating techniques for countries where data is poorly recorded, "worldwide, 5.3 million deaths occur annually due to antibiotic-resistant infections (2016)."

The current high cost of doing research on antibiotics and lack of investment due to early antibiotic success in the 1950s has blinded the large pharmaceutical companies to the need to confront the superbug pandemics arising from a panoply of cure-resistant organisms: bacteria, fungi, and molds (McCarthy 2019, 11, 106-108, 118, 176).

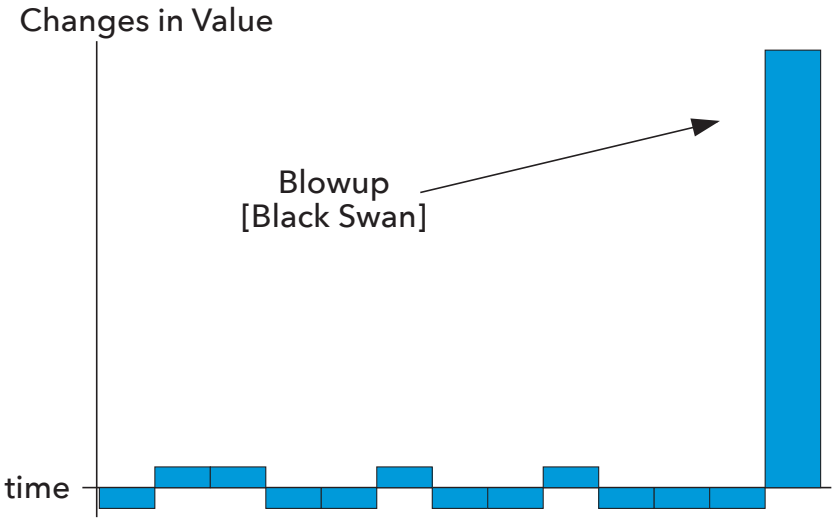


Figure 1. High positive outcome after successive failures (Taleb 2014, 436, fig. 21)

Resistant bacteria have been around since antibiotics were first discovered (McCarthy 2019, 33, 148-149). If the antibiotic main method to destroy bacterium is to deform the outer cellular skin, bacteria will simply adapt: change shape, create protective enzymes that destroy antibiotics, carry and distribute these destroying enzymes through cellular organelles known as plasmids, develop porin mutations (wall openings), or discharge antibiotics through efflux pumps (McCarthy 2019, 33, 93, 148, 186, 227). In addition, there is some proof that bacterium in nature already possesses an armamentarium of antibiotic-resistant weaponry, the great depths of which mankind has barely plumbed (McCarthy 2019, 94-95).

It is transparent that communication between research labs and antibiotic producers will be paramount in confronting a pandemic in a speedy and judicious way. Fairfield Medical Center has created an intermediating role, the CNLs—who lie at the interfaces between specialists within the departments. At hospital departmental interfaces, research watchers espying a new bug could traverse hospitals and information systems and engender a rapid and meaningful response to a potential pandemic.

Unlike doctors, earning well from prescribed procedural approaches to cures, medical researchers are knowledge workers that generate highly undervalued knowledge in experimental research and descriptive research papers (McCarthy 2019, 237). Agile programming teams could use researcher watcher customers to guide sprints toward quickly organizing this critical mass of research knowledge to effectively combat drug resistance pandemics. Such combined teams would be able to allocate capability to connect between labs and pharmaceutical packaging and delivery services, with SAFe principles as an undergirding guidance.

Opportunities are currently available for lean agile healthcare network development. For example, there is a need for more researchers and entities to speed up the development and distribution of lysins, virus-derived proteins that target each specific bacterial cell wall (McCarthy 2019, 233). No bacterial resistance exists for lysins (McCarthy 2019, 233). Lysins are derived from bacteriophages, viruses that use these biomolecules to puncture bacterial cell walls and then devour bacteria from within. Lean agile could develop a lysin informational network based on synthetic biology, a groundbreaking technique for directly synthesizing human host neutral biomolecules to target specific vectors (McCarthy 2019, 184). Using quantitative structure-activity relationships (QSARs) is a current approach, among others (Peter et al. 2019; Cherkasov et al. 2014).

A NEW METHOD OF THOUGHT CHANGES OUTCOMES: THE EFFECT OF ECONOMY OF SCALE

In *Antifragile*, Nassim Taleb describes how allowing experimentation and open-minded thought leading through low cost failures can be followed by great discoveries, mimicking the "fail early and often" mantra of Steven Jobs (2014, 181-183, fig. 6). Breaking down a complex system into small discovery units, capable of absorbing multiple doses of failure (risk) over time, happens in lean agile systems engineering. In time, the value probability curve, due to accumulating a myriad of small doses of damage initially, drifts into

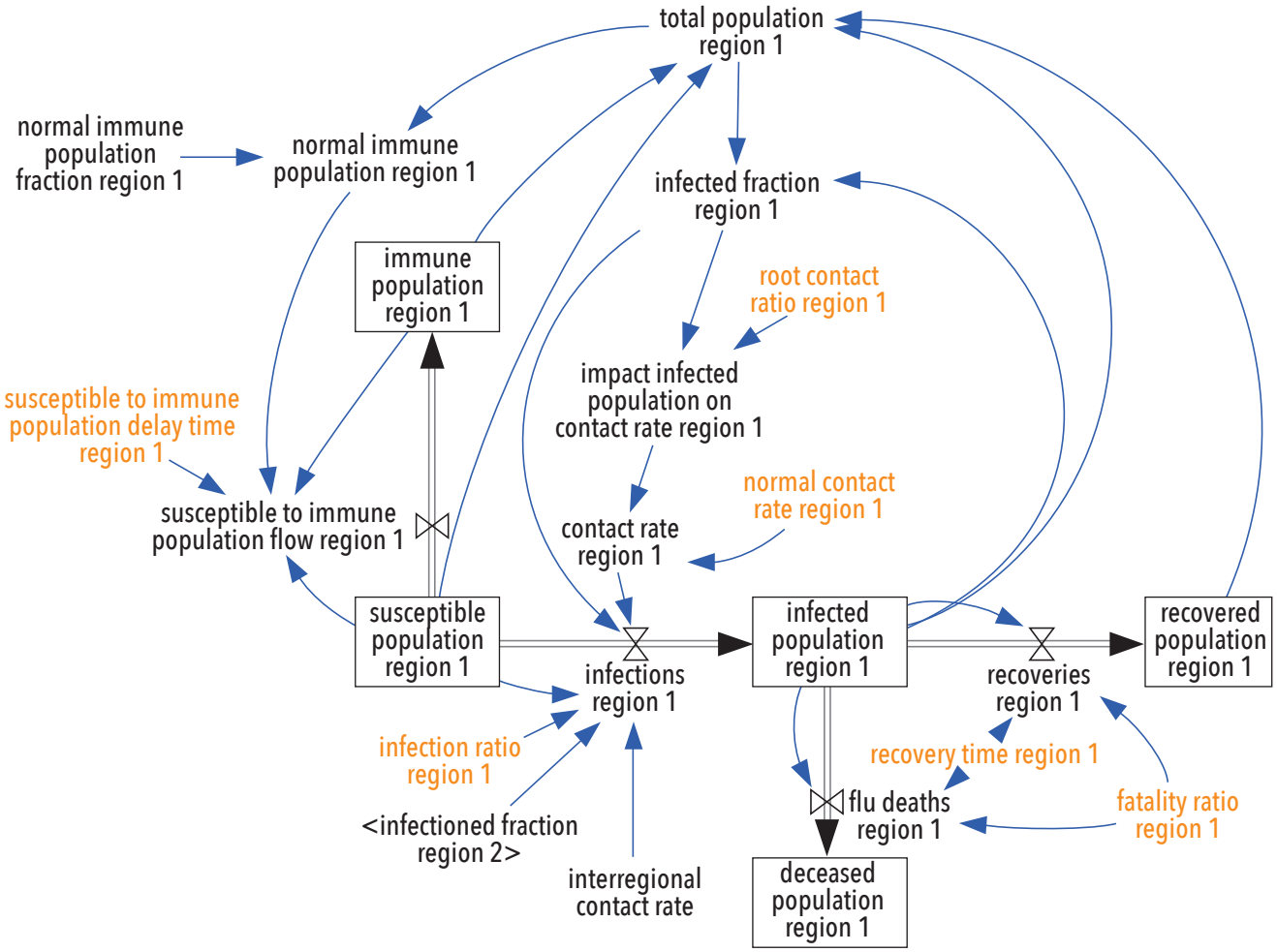


Figure 2. Exploratory system dynamics model of the flu in two regions (Pruyt and Hamarat 2010)

a positive probability area of high value discoveries (Taleb 2014, 273, fig. 13). Lean agile is an antifragile strategy.

In *Superbugs*, Matt McCarthy describes how he and director of New York-Presbyterian Hospital's infectious diseases program, Tom Walsh, open-mindedly persevere through endless small failures and institutional obstacles to the continuing research on and institutional acceptance of a miracle drug dubbed "dalba" (McCarthy 2019). Finally, they get approval to use dalba and it proves to be strikingly effective, with researchers at New York University Medical Center reporting that dalba emergency room usage lessened hospital patient stays from 26 hours to 5 hours (McCarthy 2019). New York-Presbyterian Hospital, in common with the Fairfield Medical Center, holds the optimization of hospital bed use as a valuable metric.

HOW ANTIFRAGILITY WORKS

Traffic suddenly becomes increasingly slow with a small increase in cars; passenger flight waiting times suddenly become lengthy when a slight delay occurs (Taleb 2014, 274-275, fig. 14, 278-279, 283-284). A slight increase in the deficit causes unemployment to surge numerically (Taleb 2014, 448). Taleb mentions how cost and damage can suddenly expand in a non-linear, cascading fashion as a system grows larger and more complicated, an effect Taleb labels "negative convexity bias (2014, fig. 37, 448)." While some may doubt the use of a power function to represent a new normal, one of a quickly deteriorating system, the object here is to form a preventative system, one that saves lives by successfully averting institutional degrading.

The practice of continually experimenting, as practiced by McCarthy and Walsh, strongly resembles the pattern shown in figure 3; which, if not perfectly scientific, is an acceptable description. Being open to absorbing small doses of damage: shock, stress, and failure, such as small increments of continuing damage endured by experimenters and entrepreneurs, can result in an asymmetric payoff—a large positive value empirical discovery (Taleb 2014, 158, 425). Taleb labels such a large unanticipated payoff a "black swan (Taleb 2014, 137-138, 425)." "Too big to fail" could possibly be aided by "small enough to fail productively."

To counter the tendency of large insulated bureaucracies, of which hospitals in the developed world are prime examples, a network of crises response practitioners could ready institutions to fend off a pandemic by innovating systems that would continually prepare them to expect the unexpected—a superbug attack leading to a pandemic. Further, they could catalog small hits of stress experienced through laboratory or clinical failures as lessons learned to further strengthen the existing institutions, priming them for survival, at least temporarily.

WHEN A LARGER SYSTEM MAINTAINS: THE FRACTAL ORGANIZATION

There is another approach for restructuring complicated systems. There are some instances in which larger can still stay efficient. We can see this in fractal systems, which scale down the complex portions of a complicated system proportionately. As more models

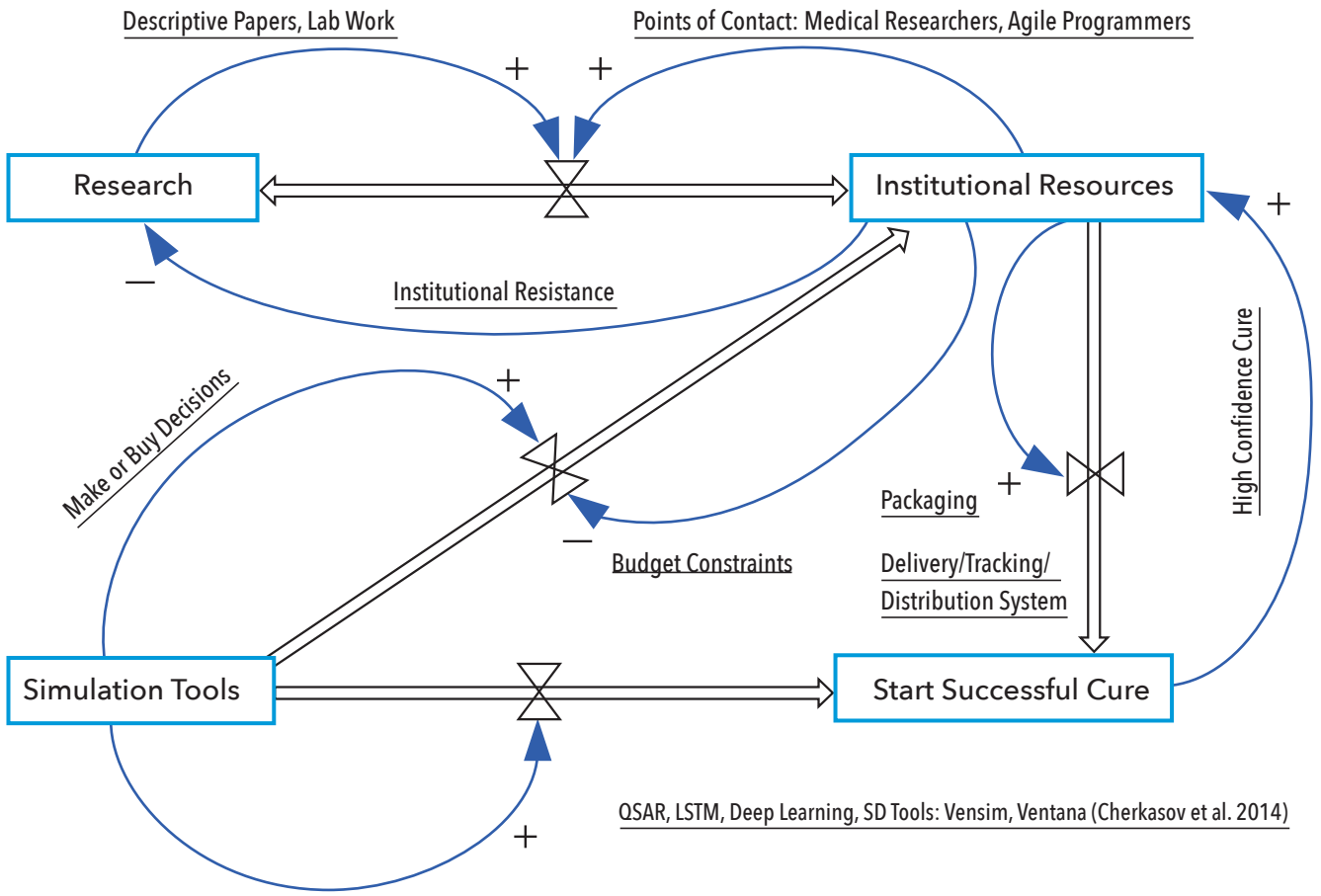


Figure 3. Napkin design for lean agile/researcher collaboration

become dynamic and agile, time to build becomes critical. Since systems built on fractals are always in a state of trading off systematic growth for effectiveness, fractal pattern thinking can expedite maintaining effective operation as a system grows large. "There is no hierarchy of command and control in a fractal system (Fryer and Luis 2004);" hence, each portion of the system maintains equal agency. In this schema, a fractal hospital could begin to incorporate and disseminate some experimental biology informatics in all its branches.

Poenaru, Dobrescu, and Merezeanu (2017, 408) give an example of a fractal social organization for healthcare information systems. They cite an "operating model [by De Florio et al.] that describes the life cycle of the service–oriented community…self–similar and factorizable into 'prime' constituents." "Simulations show that fractal organizations outperform non-fractal organizations and are able to quickly recover from changes characterizing dynamic environments (Poenaru, Dobrescu, and Merezeanu 2017, 408)."

CONCLUSION: A RELATED IDEA TO EXPLORE; SYSTEM DYNAMICS

While Taleb writes about convexity effects of doing business in enterprise domains, like large hospitals, there exists an even more definitive and revelatory method that has been superb in predicting the nonlinear effects of scale, system dynamics (Meadows, Randers, and Meadows 2004, 133-134). System dynamics (SD) can model any set of dynamic resource usages with feedback loops, sinks, sources, and delays. One starts with a 'napkin design' on paper and builds and rebuilds it until it minimally makes sense. You then build a computer simulation to reveal nonlinear adversities as well as precipitative opportunities.

According to Meadows et al. (1972, 2), "The basis of the method is the recognition that the structure of any system—the many circular, interlocking, sometimes time-delayed relationships among its components—is often just as important in determining its behavior as the individual components themselves." This presents a view of a complicated system with complex components. We can use SD for checking the impact of pandemics on healthcare resources.

Starting with the impact of influenza, Pruyt and Hamarat (2010) provide an exploratory system dynamics model of influenza spreading for the System Dynamics Society. This model is more qualitative than quantitative, but we can still use it for guidance. Next, a napkin design of a prophylactic system can be drawn.

Friedenthal, Moore, and Steiner (2009, 150) state that "Parametric diagrams are used to create systems of equations that constrain the properties of the blocks." SysML has no bundled constraint language and relies upon other applications to provide an appropriate constraint language such as OCL, Java, or MathML, to name a few (Friedenthal, Moore, and Steiner 2009, 151). We can nest SD models into SysML parametric diagrams to provide a SAFe modeler with a set of both realistic and time dynamic resource constraints.

Figure 3 is a napkin design for a lean agile/researcher team I drew. Most likely, most readers of this paper can come up with a better design. ■

REFERENCES

- Albanese, J., M. Birnbaum, C. Cannon, J. Cappiello, E. Chapman, J. Paturas, and S. Smith. 2008. "Fostering Disaster Resilient Communities Across the Globe Through the Incorporation of Safe and Resilient Hospitals for Community-Integrated Disaster Responses." *Prehospital and Disaster Medicine* 23 (5) (Sept.-Oct.): 385-390. https://dx.doi.org/10.1017/s1049023x00006105.
- Becker's Hospital Review. 2011. "5 Common Hospital Problems and How to Fix Them." https://www.beckershospitalreview.com/hospital-management-administration/5-common-hospital-problems-and-suggestions-for-how-to-fix-them.html.
- Branwell, H. 2018. "A Severe Flu Season Is Stretching Hospitals Thin: That Is a Very Bad Omen." *STAT*, 15 January. https://www.statnews.com/2018/01/15/flu-hospital-pandemics/.
- Cherkasov A., E. N. Muratov, D. Fourches, A. Varnek, I. Baskin, M. Cronin, J. Dearden, P. Gramatica, Y. C. Martin, R. Todeschini, V. Consonni, V. E. Kuz'min, R. Cramer, R. Benigni, C. Yang, J. Rathman, L. Terfloth, J. Gasteiger, A. Richard, and A. Tropsha. 2014. "QSAR Modeling: Where Have You Been? Where Are You Going To?" *Journal of Medical Chemistry* 57 (12): 4977-5010. https://dx.doi.org/10.1021/jm4004285.
- Cristian, B. "Hospital Resilience: A Recent Concept in Disaster Preparedness." 2018. *Journal of Critical Care Medicine* 4 (3): 81-82. https://dx.doi.org/10.2478/jccm-2018-0016.
- Fleischmann, C., A. Scherag, N. K. J. Adhikari, C. S. Hartog, T. Tsaganos, P. Schlattmann, D. C. Angus, and K. Reinhart; on behalf of the International Forum of Acute Care Trialists. 2016. "Assessment of Global Incidence and Mortality of Hospital-Treated Sepsis. Current Estimates and Limitations." *American Journal Respiratory Critical Care Medicine* 193 (3): 259–272. https://dx.doi:org/10.1164/rccm.201504-07810C.
- Friedenthal, S., A. Moore, and R. Steiner. 2009. *A Practical Guide to SysML: The Systems Modeling Language*. Burlington, US-MA: Morgan Kaufmann OMG Press.
- Fryer, P., and J. Ruis. 2004. "What Are Fractal Systems." http://www.fractal.org/Fractal-Systems.htm.
- Hardman, N., J. Colombi, D. Jacques, and R. Hill. 2015." What Systems Engineers Need to Know about Computer Human Interaction." *INSIGHT* 11 (2): 19-22. https://onlinelibrary.wiley.com/doi/abs10.1002/inst.200811219.
- Hefner, R., and N. Crews. 2018. "Agile Development." Lecture, California Institute of Technology, Pasadena, US-CA, 14 April.
- Jackson, S. 2010. *Architecting Resilient Systems*. Hoboken, US-NJ: Wiley.
- Lynn, R. 2019. "Useful Lean Manufacturing Tools." https://leankit.com/learn/lean/10-useful-lean-manufacturing-tools/.
- McCarthy, M. 2019. *Superbugs*. New York, US-NY: Penguin Random House.
- Meadows, D. H., D. L. Meadows, J. Randers, and W. W. Behrens III. 1972. *The Limits to Growth: A Report to the Club of Rome*. New York-US: Potomac Associates-Universe Books. https://pdfs.semanticscholar.org/99a3/41bd8ec4a4c014bab0ca8ec26aca041c8e43.pdf.
- Meadows, D. H., J. Randers, and D. Meadows. 2004. *The Limits to Growth: The 30-Year Update*. White River Junction, US-VT: Chelsea Green Publishing Co.
- Pan American Hospital Organization. n.d. "The Hospital Safety Index." Health Emergencies. https://www.paho.org/disasters/index.php?option=com_content&view=article&id=964:safety-index-&Itemid=912&lang=en.
- Peter, C. S., J. K. Dhanjal, V.Malek, N. Radhakrishnan, M. Jayakanthan, and D. Sundar. 2019. "Quantitative Structure-Activity Relationship (QSAR): Modeling Approaches to Biological Applications." *Encyclopedia of Bioinformatics and Computational Biology* 2 (2019): 661-676. https://dx.doi.org/10.1016/B-978-0-12-809633-8.20197-0.
- Poenaru, C. E., R. Dobrescu, and D. Merezeanu. 2017. "Fractal Organization in Healthcare Information Systems." Paper presented at 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, RO, 29-31 May. https://dx.doi.org/10.1109/CSCS.2017.63.
- Pruyt, E., and C. Hamarat. 2010. "The Influenza A(H1N1) v Pandemic: An Exploratory System Dynamics Approach." Paper, Delft University of Technology Faculty of Technology, Management, and Policy. https://www.systemdynamics.org/assets/conferences/2010/proceed/papers/P1253.pdf.
- SAFe. 2019. "SAFe Lean-Agile Principles." https://www.scaledagileframework.com/safe-lean-agile-principles/.
- Society for Disaster Medicine and Public Health. 2018. "Citizen Ready® Program." https://societyfordisastermedicineandpublichealthinc.wildapricot.org/Citizen-Ready-Program.
- Taleb, N. N.. 2014. *Antifragile: Things That Gain from Disorder*. New York, US-NY: Random House.
- Walden, D. D., G. J. Roedler, K. J. Forsberg, R. D. Hamelin, and T. M. Shortell, eds. 2015. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. 4th ed*. San Diego, US-CA: Wiley.
- World Health Organization. 2019. "The 10 Biggest Threats to Health Worldwide, According to WHO." https://www.advisory.com/daily-briefing/2019/01/28/global-health-risks.

ABOUT THE AUTHOR

Josh Sparber, an A+ student in high school biology, still faithfully remembers much of what he learned at that time. In 1974, he received a BS in biology from SUNY, inspired by work going on at that time in genetics. Since then, he changed course to work in the electronics industry from 1980–2000. After earning an MSEE from Cal State Fullerton in 1999, he familiarized himself with the practice of systems engineering for almost 20 years with the US Department of Defense. Mr. Sparber's current focus is on working with the Critical Infrastructure Protection Working Group of INCOSE in researching pathways to sustaining our critical infrastructures. He is now combining some of his past endeavors to pursue independent research to open new insights for protecting humanity's precious critical infrastructures.

Systems Theory Principles and Complex Systems Engineering Concepts for Protection and Resilience in Critical Infrastructure: Lessons from the Nuclear Sector

Adam D. Williams, adwilli@sandia.gov

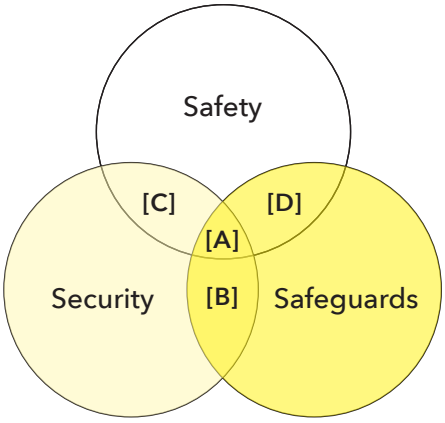
SAND2019-PEER REVIEW. *Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the US Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525*

■ **ABSTRACT**

Part of the Presidential Policy Directive 21 (PPD-21) (PPD 2013) mandate includes evaluating safety, security, and safeguards (or nonproliferation) mechanisms traditionally implemented within the nuclear reactors, materials, and waste sector of critical infrastructure—including a complex, dynamic set of risks and threats within an all-hazards approach. In response, research out of Sandia National Laboratories (Sandia) explores the ability of systems theory principles (hierarchy and emergence) and complex systems engineering concepts (multidomain interdependence) to better understand and address these risks and threats. This Sandia research explores the safety, safeguards, and security risks of three different nuclear sector-related activities—spent nuclear fuel transportation, small modular reactors, and portable nuclear power reactors—to investigate the complex and dynamic risk related to the PPD-21-mandated all-hazards approach. This research showed that a systems-theoretic approach can better identify interdependencies, conflicts, gaps, and leverage points across traditional safety, security, and safeguards hazard mitigation strategies in the nuclear reactors, materials, and waste sector. As a result, mitigation strategies from applying systems theoretic principles and complex systems engineering concepts can be (1) designed to better capture interdependencies, (2) implemented to better align with real-world operational uncertainties, and (3) evaluated as a systems-level whole to better identify, characterize, and manage PPD-21's all hazards strategies.

INTRODUCTION

Meeting the Presidential Policy Directive 21 (PPD-21) mandate that "Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards (PPD 2013)" includes evaluating safety, security, and safeguards (or nonproliferation) mechanisms traditionally implemented within the nuclear reactors, materials, and waste sector of critical infrastructure. Critical nuclear infrastructure harnesses the energy released during nuclear fission, where atomic and subatomic particles collide in a sustainable chain reaction. Related benefits include baseload quantities of electricity or significant volumes of desalinated seawater (arguably in a manner that reduces carbon emissions), as well as generating radionuclides for medical uses (cancer treatments) and advanced technological development (oil well logging). However, some nuclear fission by-products become radioactive because of unstable nuclei which dissipate excess energy by spontaneously emitting alpha, beta, and gamma rays. Uncontrolled radiation can result in particular and psychologically fear-inducing impacts on human (poisoning and latent cancers) and environmental (land contamination and agricultural spoilage) health effects. To maintain these benefits—and minimize



3S Interaction	Representative Example [Location on Venn Diagram]
Interdependency	Coordination of 3S responsibilities during emergency operations [A]
Conflict	Intrusive access control could impede evidence of peaceful uses (*increase safeguards risk*) [B]
Gap	Passive safety systems could be new targets for malicious acts (*increase security risk*) [C]
Leverage Point	Safeguards inspections could reveal a reactor vessel integrity issues (*reduce safety risk*) [D]

Figure 1. Types of interactions between safety, security, and safeguards in the critical nuclear infrastructure sector, with representative examples

these health effects—the nuclear sector applies technologies, training, policies, and protocols to meet safety (preventing unintentional radiological releases), safeguards (preventing military use of nuclear technologies), and security (protecting against intentional radiological release or theft) objectives.

Protection and recovery efforts within the nuclear domain must include addressing not only traditional concepts of security, but also the long-standing emphasis on safety and the unique need for international safeguards. From this perspective, protection and resilience for nuclear facilities each consist of a complex and dynamic set of risks that are consistent with the PPD-21 call for investigating mechanisms to "strengthen all-hazards security and resilience" for critical infrastructure (PPD 2013). In the nuclear realm, this perspective is reflected internationally in calls by the World Institute of Nuclear Security (an international non-governmental organization) for an all-hazards approach to securing nuclear materials and the facilities (2019) and domestically by a National Academy of Sciences Committee conclusion that "The NNSA should adopt…a 'total systems approach' to characterize the interactions and dependencies of security (Committee on Risk-Based Approaches for Securing the DOE Nuclear Weapons Complex 2011, 1)." More specifically, in the words of former Deputy Director-General for Safeguards at the International Atomic Energy Agency, Olli Heinonen:

> Safeguards, security, and safety are commonly seen as separate areas in nuclear governance. While there are technical and legal reasons to justify this, they also co-exist and are mutually reinforcing. Each has a synergetic effect on the other, and authorities should carve out avenues for collaboration to contribute to the effectiveness of the nuclear order. For instance, near real-time nuclear material accountancy and monitoring systems provide valuable information about the location and status of nuclear material. This in turn is useful for nuclear security measures. Similarly, such information enhances nuclear safety by contributing as input to critical controls and locations of nuclear materials (2017).

Thus, to meet the primary PPD-21 objective of being able to "withstand and rapidly recover from all hazards" for the nuclear sector, strategies for the protection and resilience of nuclear materials and facilities must adequately address safety, safeguards, and security (3S) challenges—and the interactions between them (figure 1). In response, Sandia has explored the ability of systems theory principles and complex systems engineering concepts to better understand the complexities of the interactions between traditional safety, safeguards, and security mitigations in the nuclear sector. By investigating the complexity and dynamism in international spent nuclear fuel transportation, small modular reactors, and portable nuclear power reactors, this Sandia research identified key commonalities and unique outliers necessary to support a PPD-21-mandated all-hazards approach to protection and resilience for critical infrastructure.

SYSTEMS THEORY AND COMPLEX SYSTEMS ENGINEERING FOR PROTECTION AND RESILIENCE

Sandia's studies began by asserting that systems theory principles and complex systems engineering concepts provided a useful framing for characterizing the complexity in—and interactions between—nuclear safety, safeguards, and security in real-world operations. One such systems theory principle is hierarchy; wherein we articulate functional descriptions in terms of levels of complexity within a system. Systems theory argues that hierarchy is a useful framework for understanding, defining, and evaluating the characteristics that generate, separate, and connect these levels of complexity. By extension, this logic of hierarchy also asserts that higher ranking components/influences constrain the range of possible behaviors of components at lower levels. For example, the research indicated that the size (power output) of a given nuclear reactor constrains the types of safety, safeguards, and security mitigations implemented—and, thus, influences levels of protection and resilience for the nuclear activity.

The principle of hierarchy is directly related to the observed phenomena by which behaviors at a given level of complexity are irreducible to (and thus, inexplicable by) the behavior or design of its component parts. Called emergence, this concept describes how interactions among components within a system (or with environmental influences) drive system-level behaviors. Going beyond the ability for individually selected technologies, policies, and behaviors to achieve component-level goals, the logic of emergence captures the importance of the interactions between such components on achieving system-level objectives. Recent Sandia research concluded that considering nuclear activities as complex systems afforded the benefit of evaluating safety, safeguards, and security as emergent properties—which matches the complexity observed when implemented in international or transboundary environments.

Given the importance of emergence, there is a need to better understand how interactions between components and with environmental influences impact the ability of systems to achieve their desired

objectives. This is the principle of interdependence and describes how actions (or outcomes) in one component impact actions (or outcomes) in another. The principle of interdependence also addresses the concept of feedback—where output from component A's interaction(s) with other components (or environmental influences) influences the next set of inputs back into component A actions. In this research, the team evaluated safety, safeguards, and security for nuclear sector activities in terms of how each impacted—and was impacted by—both technical and non-technical (or, socio-political) components.

Current efforts in systems engineering aim to better combine these systems theory principles to design and operate ever increasingly complex systems. As systems increase in complexity, according to Keating, et al. (2003, 38), "it is naïve to think that problem definitions and requirements will be isolated from shifts and pressures stemming from highly dynamic and turbulent development and operational environments." If this is true, then engineering for complex infrastructure should also be cognizant of—if not explicitly incorporate—risk mitigation processes that form part of its operational environment. This Sandia research aimed to better address the multidomain interdependencies between long-established nuclear safety practices, internationally-mandated nuclear safeguards processes, and socio-technical nuclear security systems. Complex systems engineering offers the mechanism by which to design nuclear facilities in such a way to account for these safety-safeguards-security interdependencies by expanding design options to include non-traditional influences on system performance. Thus, it seems that invoking these systems theory principles and complex systems engineering concepts provide a strong foundation on which to build all-hazards strategies and mitigations for critical nuclear infrastructure protection and resilience.

SANDIA'S SYSTEM-THEORETIC APPROACH TO NUCLEAR SAFETY, SAFEGUARDS, AND SECURITY

In several studies—summarized in the next section—Sandia researchers demonstrated that 3S risk stems from interactions between technical, human, and organizational influences within critical nuclear infrastructure as complex systems. These studies also offer several useful conclusions for evaluating 3S risk complexity for critical nuclear infrastructure. First, integrated 3S approaches can help identify interactions—such as interdependencies, conflicts, gaps, and leverage points—across nuclear traditional safety, security, and safeguards approaches. Second, including the interactions between safety, safeguards, and security better aligns with real-world operational uncertainties and better describes the risk complexity associated with multi-modal, multi-jurisdictional systems in which critical nuclear infrastructure must operate. Third, we can design risk mitigation strategies resulting from integrated 3S risk assessments to better account for interdependencies not included in independent S assessments.

Table 1. Summary of systems engineering design goals for each type of interaction evaluated in Sandia's systems-theoretic approach to nuclear safety, security, and safeguards

3S Interaction	Systems Engineering Design Goal
Interdependency	Identify & (possibly) decouple
Conflict	Identify, eliminate, and/or reconcile
Gap	Identify, eliminate, and/or reconcile
Leverage Point	Identify & exploit

Other efforts in the nuclear sector have taken a range of approaches to explore 3S integration. One endeavor identified overlaps in regulations, procedures, and instrumentation to offer "3S-by-design" as a potential resource savings for nuclear utilities (using shared video surveillance data between safety, safeguards, and security) (Stein and Morichi 2012). Another used traditional risk management approaches to highlight analytical consistencies between these domains—namely by pairing the traditional security-related issue of sabotage with safety and traditional security-related issue of theft with safeguards (Cipollaro and Lomonaco 2016). In contrast, the Sandia grounded their studies in systems theory and complex systems engineering to illustrate interactions (Table 1) between risks and mitigations (interdependencies), characterize oppositional forces in operational risks (conflicts), identify missed operational risks (gaps), and capture natural redundancies or compensatory effects to mitigate risks (leverage points).

For this research, interdependencies refer to aspects of expected individual S operations whose operations are directly impacted by the behavior from operations in another S. Such relationships could include, but are not limited to, technical components that are collocated and/or use the same infrastructure; temporal processes that must be completed sequentially; or organizational policies that are predicated on specific technological capabilities. Sandia's 3S analysis sought to identify any interactions within the evaluated nuclear infrastructure sector that impacted—either positively or negatively—expected safety, safeguards, or security behaviors. For example, one interdependence for critical nuclear infrastructure relates to desired responses to a fire alarm. For safety, the primary goal is to evacuate facility personnel as quickly as possible. Yet, for security, the emphasis is on ensuring that the alarm is not a diversion for a malicious act (an adversary using the chaos as an escape mechanism). From this perspective, the interdependent need for security to verify the location of all personnel from sensitive areas of the nuclear facility while also meeting the safety need for timely evacuation presents a complex systems engineering design problem.

Often, integration-based analyses focus on identifying—and mitigating—conflicts. For this research, conflicts refer to aspects or objectives of expected individual S operations that negatively overlap with expected behaviors from a different S. Systems engineers commonly capture conflicts using various forms of trade space analysis within systems engineering by tracing their origins to either implementation, design, or requirements decisions. This research sought to expand on this tradition to identify negative interdependencies between safety, safeguards, and security—particularly where an improvement in the operations of one S resulted in a deleterious effect on behaviors in another S. For example, one conflict in critical nuclear infrastructure are common practices related to transporting hazardous materials. For security of nuclear transportation, one point of emphasis is "need to know," or limiting who is informed about the transportation details (route and timelines). Yet, national safety regulations often require clear (and distinct) markings indicating that a given vehicle is carrying nuclear materials. So, an improvement in hazardous material marking for first responders directly impedes implementing "need to know" to meet security obligations. From this perspective, we could address this conflict by invoking

Table 2. Representative set of enhanced mitigation design goals identified from interdependencies, conflicts, gaps, and leverage points in safety, security, & safeguards activities

Case	Safety	Security	Safeguards	[3S Interaction Type] Systems Engineering Design Goal
SNF Transport	Better SNF access can help prevent unplanned radiological release	Focus on preventing unauthorized access during SNF transport	Fewer people with SNF access can enhance continuity of knowledge during transport	**[Leverage Point** Identify and exploit multiple benefits of focusing on preventing unauthorized access
Small Modular Reactors	Strict access controls challenge emergency operations	Strict access control procedures to offset fewer onsite security personnel	Strict access controls can provide assurance to safeguards inspectors	**[Conflict]** Identify, eliminate, or reconcile impact of access controls on emergency operations
Reactors	Scuttling as a last-ditch response to an accident	Scuttling raises questions on protection responsibilities	Scuttling raises questions on reporting and accountancy responsibilities	**[Gap]** Identify, eliminate, or reconcile benefits of scuttling on security and safeguards responsibilities

systems theory principles into technical or procedural redesign.

In addition to conflicts, integrating across safety, safeguards, and security behaviors can identify operations or behaviors that we have not yet identified. For this research, gaps refer to aspects or objectives of expected individual S operations that we have not captured, mitigated, or otherwise addressed. Yet, this perspective also demonstrates that gaps can be positive and represent missed opportunities to improve system behaviors. For example, one gap common across critical nuclear infrastructure is coordination during emergencies involving nuclear materials. Much like emergencies with other hazardous materials, the safety (protect the public from undue harm) and security (protect the materials from malicious use) are well known. One unique (and often missing) aspect of critical nuclear infrastructure emergencies are the safeguards—which, from this perspective, is a gap that represents an opportunity for enhanced emergency operations. More specifically, coordinating completion of safeguards actions (maintaining continuity of knowledge of the location and amounts of nuclear materials) can improve safety and security operations by streamlining hazardous clean-up efforts and clarifying who has had access to the nuclear materials, respectively.

Lastly, in this research, leverage points refer to aspects or objectives of expected individual S operations that positively overlap with expected behaviors from a different S. In contrast to conflicts, leverage points are force multipliers between safety, safeguards, and security when an improvement in one S results in a simultaneous improvement in expected behaviors in another S. This research purposefully sought such relationships to demonstrate the concept that there are situations in which interdependence is desired. For example, consider the multiple responsibilities involved when nuclear material is in transit and must cross a national (or international) border. Because of the importance of adhering to all safety, safeguards, and security responsibilities along the entire transportation route, border crossings represent a transition in risk mitigation responsibility that can stretch traditional (isolated) inspection approaches. From this perspective, we could assign aspects of safeguards inspections to safety inspectors to take advantage of the larger number of qualified safety inspectors worldwide. Thus, already existing safety operations augment the need to meet continuity of knowledge of nuclear material responsibilities by designing jurisdictional transition inspections to leverage data commonly collected for safety purposes to meet safeguards obligations.

LESSONS FROM ACROSS THE NUCLEAR INFRASTRUCTURE SECTOR

Evaluating the risk complexity for different pieces of nuclear infrastructure demonstrated the applicability of this research to meeting the PDD-21 mandate for critical infrastructure. This section summarizes the technical evaluations of an integrated 3S approach to risks for three different nuclear infrastructure sector-related activities—spent nuclear fuel (SNF) transportation, small modular reactors, and portable nuclear power reactors. A representative set of how identifying interdependencies, conflicts, gaps, and leverage points can enhance 3S risk mitigation strategies is summarized in Table 2. In addition, these studies illustrate how using systems theory principles and complex systems engineering concepts can meet the PPD-21 call for an all-hazards approach.

Case 1: International Transportation of Spent Nuclear Fuel

Recent interest in new nuclear programs (United Arab Emirates and Vietnam) and the increasingly popular fuel take back agreements from existing nuclear power programs (Russia) indicate an expected increase in the amount of spent nuclear fuel (SNF) transported across the globe, including transfers of SNF casks between transportation modes (road to rail to water) and across geopolitical or maritime borders. SNF is nuclear material that has undergone fission within a reactor vessel and is now significantly radioactive. Risk mitigation for the international SNF transportation is challenging because of the likelihood that related mitigation resources and regulations along approved routes will be inconsistent. To investigate the resulting complexity in achieving 3S objectives, this study (Williams et al. 2017b) used a hypothetical SNF transportation across fictitious borders and between multiple conveyances. (For details on the hypothetical case description, see Williams et al. 2017a)

Results from this study demonstrated that different analysis techniques, albeit in different ways, incorporated systems theory principles and complex systems engineering concepts to identify interdependencies, conflicts, gaps, and leverage points for risk mitigation. One interdependency identified how the negative health effects of the radiological release from exposure to SNF—an important factor in designing adequate security responses to SNF transportation accidents–would directly

impact security responders' effectiveness. Consider advanced notification of SNF transportation details to local first responders as an example of a conflict. While the timeline for advanced notice can both shorten response and public evacuation times, it can also increase the possibility for and adversary to obtain route information. Two new states of increased risk—uncoordinated implementation of both standard operating procedures and operational emergency plans—emerged from several gaps identified in expected SNF transportation behaviors which evaluating safety, safeguards, and security individually missed. Other results identified leverage points for better mitigating the risks of SNF transportation, including how improved prevention of unauthorized access to the cask (for the security goal of preventing theft) also results in better mitigation of unplanned radiological releases (from a safety accident) and enhanced continuity of knowledge of material location (a safeguards issue).

Though representative of the larger study, these results highlight how hierarchy (constraining end-to-end SNF transportation risk), emergence (ensuring that inspections meet objectives), and interdependence (accounting for the impact of security protocols on security performance), as systems theory principles, better capture the real-world risk facing international SNF transportation. Similarly, identifying gaps (the potential for there to be no shipment oversight entity), interdependencies (the need to coordinate between security and emergency personnel after a notional train derailment), conflicts (inspectors may have contradictory safety and safeguards responsibilities), and leverage points (using security procedures to maintain continuity of knowledge for safeguards) provides the opportunity to use complex systems engineering to design better risk mitigation strategies. Using these insights resulted in a systems-based all-hazards approach for managing risk complexity in multimodal and multijurisdictional international SNF transportation.

Case 2: Small Modular Reactors

By design, small modular reactors (SMRs) will have a smaller operational footprint and generate substantially less energy than the current nuclear power plants (NPPs), thereby offering a significant relative cost reduction to current-generation nuclear reactors—increasing their appeal around the globe. In addition, SMRs offer a variety of passive (no additional energy is necessary for initiation) safety features intended to provide adequate core cooling to delay (or prevent) core damage in the event of a short-term station blackout. When combined with the small core size and lower power density design characteristics, the passive safety systems may provide an inherent degree of resilience to beyond design basis events not typically seen in traditional NPPs. Yet, this shift in focus from engineered active safety systems to passive safety measures has potential implications for not only safety, but also for safeguards and security of SMRs. This study conducted a technical evaluation on a hypothetical SMR (for more technical details, please see Lewis et al. 2012) based on light water reactor-based concepts and designs across a range of safety, safeguards, and security scenarios. (For more study details, please see Williams et al. 2018). Given the novelty of SMR technologies, this study identified the need to achieve the same levels of 3S risk reduction with reduced resources and applicability of current 3S technical analysis and best practice rules of thumb to SMRs as challenges to meeting the PDD-21 all-hazards approach.

Overall, the focus on this study on interactions between technologies, processes, and procedures related to safety, safeguards, and security identified several instances where traditional assumptions of independence did not fully capture likely SMR operational realities. In one example of an interdependency, SMR passive safety systems can reduce the chances of a safety incident, but simultaneously offer new potential targets that increase the security risk. For an example of a conflict, consider the popular argument that SMRs will have very few personnel and strict access controls. While such restriction of access can increase security against both external and internal adversaries (and increase the assurance of appropriate safeguards-related access), they can also challenge the ability for emergency personnel to adequately respond to accidents at the facility. This study also identified the gap in understanding how the tradition of physically separating reactor trains to reduce common cause safety failures also increases the complexity of an NPPs layout and potentially makes it easier for an aspiring proliferant to guide inspectors around sensitive facility areas. Despite some incongruity between SMRs and best practices, this study identified the possibility for increased safeguards inspections frequency (due to the technical reactor characteristics and assumed attractiveness of the nuclear materials) would also reduce chances for an insider adversary to perpetrate a malicious act against the facility.

Though seemingly obvious, these interactions are not often accounted for individual technical analyses available in the public domain. These representative examples also illustrate how key systems theory principles like hierarchy (the role of a smaller facility footprint on traditional safety, safeguards, and security mitigations), emergence (statements regarding by-design approaches for both security and safeguards in SMRs), and interdependence (the need to adequately secure passive safety systems) can improve risk mitigation for critical nuclear infrastructure. None of the interdependencies, conflicts, or gaps, identified in the study presented significant challenges to SMRs meeting safety, safeguards, and security objectives. Yet, they did identify leverage points where we could implement complex systems engineering concepts—designing for safety-safeguards-security interdependencies as part of the operational environment, for example—to gain efficiency and effectiveness in an all-hazards approach for protection and resilience for SMRs.

Case 3: Portable Nuclear Reactors

A recent solution to siting and construction challenges of traditional NPPs are portable nuclear reactors (PNRs), or power-generating reactors that we can move between locations with sub-gigawatt electricity generation capability. Several nations are in the beginning stages of deploying and operating PNRs—including the Offshore Floating Nuclear Plant by the Massachusetts Institute of Technology, the US Army's proposed mobile very small modular reactor (vSMR), China's floating small modular reactor, and Russia's floating PNR, the Akademik Lomonosov (which, according to media reports, docked in December of 2019 and has supplied 10GWh of electricity through January 2020 [Nuclear Engineering International 2020]). While such flexible redeployment comes with many operational benefits, there remain many unanswered questions about PNRs and how their risks may differ in form from traditional land-based reactors. One of the most unique aspects is the fact that each PNR can be transported as a complete NPP, resulting in changing risk profiles as the PNR moves between territorial and international borders or as water-borne travel challenges the assumption that a PNR (and its safety systems) will remain upright for the duration of any accident. In response, this study conducted a technical evaluation on a hypothetical PNR based on the scant technical information available in the public domain. (For more study details, please see Williams et al., forthcoming)

The results of this study on PNRs highlighted the value of systems-level analysis of safety, safeguards, and security interactions in developing all-hazards strategies for critical infrastructure that differs significantly from the status quo. Take, for example, the interdependency between the need to scuttle (or, purposely sink) a floating PNR to prevent an adversary act from succeeding and the safeguards reporting and inspections obligations for the sunken nuclear material. This also represents a conflict—while scuttling a floating PNR might serve as an ultimate security risk mitigation for preventing theft and sabotage, doing so also directly impedes the safety objectives of protecting maritime environments and associated commercial interests from undue exposure to radionuclides. Other 3S conflicts for PNRs are directly related to the potential for inconsistent and different interpretations of international maritime laws. One interesting gap identified in the study relates to the implications of the potential loss of control of the entire floating PNR vessel—as this scenario may allow a non-nuclear state access to a fully functioning nuclear reactor, even if it is only for a short period of time. In contrast, one similarly interesting leverage point identified in the study relates to how we could use the anticipated increase in safety-related inspections of PNRs between use locations as opportunities for additional safeguards-related inspections and reporting.

The preliminary results from this study are a first step in identifying, mitigating, and preventing such risks from negating the tremendous opportunities—like more flexible, cost-efficient electricity generation for remote civilian areas—presented by PNRs. Overall, this technical evaluation concluded that the researchers expect no significant public health impacts, current international safeguards approaches will be challenged, and, we will need to overcome jurisdictional ambiguity (and current technological shortcomings) for adequate security. This study also illustrated how hierarchy (defining constraints by level of PNR mobility), emergence (ensuring 3S risk mitigations are adequate across all possible PNR states), and interdependence (accounting for more dynamism between 3S mitigations during PNR motion) as systems theory principles helped address the anticipated increase in complexity for PNR operations. Combining these principles with complex systems engineering concepts provides an integrated approach better capable of including operational environments into PNR designs. In so doing, it may be possible to develop general PNR performance requirements designed to ensure that systemwide, safety, safeguards, and security risk remains acceptable—a conclusion of this study that supports the PDD-21 all-hazards approach for critical infrastructure protection and resilience.

CONCLUSIONS AND IMPLICATIONS

In calling for an all-hazards approach for protecting critical infrastructure, PDD-21issued a new challenge to designing and implementing resilient systems and structures to meet societal needs among increasingly complex operational environments. Moreover, PDD-21 is a charge that implicitly points to insufficiencies in traditional approaches that seek to optimize individual domains in isolation—as exemplified by how the nuclear infrastructure sector traditionally treats safety. While seeking to optimize nuclear safety (or nuclear safeguards or nuclear security) may yield apparent improvements in risk reduction, doing so disregards key aspects of risk complexity that can significantly impact overall performance. In response, three recent Sandia studies evaluated the impacts and implications of exploring the interactions between safety, safeguards, and security risk mitigation in the nuclear infrastructure sector. Across these studies of international spent nuclear fuel transportation, small modular reactors, and portable nuclear reactors, incorporating systems theory principles (hierarchy, emergence, and interdependence) and complex systems engineering concepts (designing to include the operational context) produced higher fidelity results. These results included descriptions of risks missed by more traditional approaches and requirements for improving mitigation designs toward improved protection and resilience. Ultimately, these three studies demonstrated the utility of using systems engineering to incorporate interdependencies between safety, safeguards, and security controls for enhancing the overall performance of critical nuclear infrastructure.

Several important implications result from the conclusions of these three studies. First, risks for critical infrastructure are not necessarily independent—implying that protection and resilience efforts should address the potential for interdependency. Second, systems theory principles provide a useful mental model for describing interdependencies and complex systems engineering concepts help characterize potential solutions. More specifically, these principles and concepts help identify risks that traditional approaches miss, while simultaneously offering a wider set of potential mitigations to improve overall performance. Third, evaluating interdependencies, conflicts, gaps, and leverage points helps incorporate elements of the operational environment into system design—which has traditionally been a source of notable uncertainty in critical infrastructure risk. For example, explicitly evaluating desired safety, safeguards, and security behaviors as emergent properties in terms of these interactions directly results in opportunities to overcome traditional obstacles in risk reduction. Lastly, we enhance designing for protection and resilience in terms of all-hazards strategies when accounting for interdependence—whether between elements of risk itself or between isolated mitigations against elements of risk.

Though representative, these Sandia study results highlight opportunities to leverage interactions between critical infrastructure operations (and with operational environments) to guide desired behaviors to meet PDD-21's three strategic imperatives. Refining and clarifying functional relationships, employing systems theory principles and complex systems engineering concepts to design for leverage points and gaps/conflicts can strengthen critical infrastructure protection and resilience. Consider using SNF security inspections at a border crossing to support safeguards and clarifying security/safeguards responsibilities for floating PNRs in territorial waters, respectively. These principles and concepts can also enhance information exchange by providing a common mental model (focus on emergent behaviors in an operational environment for PNRs) and by coordinating multi-domain risk mitigations toward the same protection and resilience goals (3S coordination for SMR operations). Lastly, explicitly evaluating integration in terms of interdependencies, conflicts, gaps, and leverage points offers a wider analysis function to develop solutions in support of critical infrastructure decisions more creatively. These results from Sandia's critical nuclear infrastructure studies describe the unique position that systems engineering has in meeting PPD-21's call to "address…in an integrated, holistic manner this infrastructure's interconnectedness (PPD 2013)"—and speaks to the role systems engineers can play in developing appropriate all-hazards strategies to enhance protection and resilience of critical infrastructure. ■

REFERENCES

- AP News. 2019. "Russia's Floating Nuclear Plant Sails to Its Destination." 23 August. https://www.apnews.com/208ba688c44c4ff49de735ecb9a3963f.
- Cipollaro, A., and G. Lomonaco. 2016. "Contributing to the Nuclear 3S's Via a Methodology Aiming at Enhancing the Synergies Between Nuclear Security and Safety." *Progess on Nuclear Energy* (86): 31-39.
- Committee on Risk-Based Approaches for Securing the DOE Nuclear Weapons Complex. 2011. "Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex (Abbreviated Version)." Report, National Research Council of the National Academies. https://www.nap.edu/catalog/13108/understanding-and-managing-risk-in-security-systems-for-the-doe-nuclear-weapons-complex.
- Divison of Nuclear Security. 2015. *Nuclear Security Series Glossary, Version 1.3*. Vienna, AT: International Atomic Energy Agency.
- Heinonen, O. 2017. "Nuclear Terrorism: Renewed Thinking for a Changing Landscape." Briefing at the Open Debate of the United Nations Security Council, New York, US-NY, 13 February. https://www.belfercenter.org/sites/default/files/files/publication/21317_Olli_UN_Briefing.pdf.
- Keating, C., R. Rogers, R. Unal, D. Dryer, A. Sousa-Perez, R. Safford, W. Peterson, and G. Rabadi. 2003. "System of Systems Engineering." *Engineering Management Journal* 15 (3): 36-45.
- Lewis, T., B. Cipiti, S. Jordan, and G. Baum. 2012. "Generic Small Modular Reactor Plant Design (SAND2012-10406)." Report, Sandia National Laboratories.
- Nuclear Engineering International. 2020. "Russian Floating Nuclear Plant Supplies 10GWh of Electricity to Chukotka." *Nuclear Engineering International Magazine*, 27 January.
- PPD (Presidential Policy Directive). 2013. PPD-21. *Directive of Critical Infrastructure Security and Resilience*. Washington, US-DC: PPD, Administration of Barack Obama.
- Stein, M., and M. Morichi. 2012. "Safety, Security and Safeguards by Design: An Industrial Approach." *Nuclear Technologies* (179): 150-155.
- Williams, A., D. Osborn, J. Bland, B. Cohn, C. Faucett, L. Gilbert, S. Horowitz, and J. Rutkowski. Fourthcoming. "System Studies for Global Nuclear Assurance and Security (GNAS): 3S Risk Analysis for Portable Nuclear Reactors (Volume I)—Technical Evaluation of Safety, Safeguards, & Security (SAND2019-TBD)." Report, Sandia National Laboratories.
- Williams, A., D. Osborn, J. Bland, J. Cardoni, B. Cohn, C. Faucett, L. J. Gilbert, R. Haddal, S. Horowitz, M. Majedi, and M. K. Snell. 2018. "System Studies for Global Nuclear Assurance & Security: 3S Risk Analysis for Small Modular Reactors (Volume I)–Technical Evaluation of Safety, Safeguards, & Security (SAND2018-12447)." Report, Sandia National Laboratories.
- Williams, A., D. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, M. Thomas, M. J.Parks, E. Parks, and Amir H. Mohagheghi. 2017a. "Hypothetical Case and Scenario Description for International Transportation of Spent Nuclear Fuel (SAND2017-13661)." Report, Sandia National Laboratories.
- ——. 2017b. "System Theoretic Frameworks for Mitigating Risk Complexity in the Nuclear Fuel Cycle: Final Report (SAND2017-10243)." Report, Sandia National Laboratories.
- World Institute for Nuclear Security. 2019. "WINS 2019 Annual Report: The Golden Threat of Nuclear Security." Report, World Institute for Nuclear Security. https://wins.org/wp-content/uploads/2019/03/WIN-102-0219_WINS_Annual_Report_2019_SCR.pdf.

ABOUT THE AUTHOR

Adam D. Williams is a principal R&D systems engineer in the Nonproliferation and Cooperative Threat Reduction Center, Sandia National Laboratories. He has a BS in mechanical engineering, MA in international affairs/national security, and PhD in human and systems engineering.

Use of SysML to Generate Failure Modes and Effects Analyses for Microgrid Control Systems

Myron Hecht, myron.hecht@aero.org

■ **ABSTRACT**
In this article, I present a method for producing a failure modes and effects analysis (FMEA) from SysML together with an application to a microgrid control system. The significance of the method is the modeling of failure propagation which enables not only an automated approach but also additional results that systems engineers can use to support resiliency, safety, and cybersecurity. I discuss the analysis products and insight they provide.

SECTION 1 INTRODUCTION

Microgrids are small electrical power grids that include both electrical energy sources and loads at the distribution station level. More formally, a microgrid is a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the main power grid (US Department of Energy Microgrid Exchange Group and the CIGRE 6.22 Working Group 2019). The goal of microgrid design is to enable isolation of the local grid to protect from the main grid instabilities and to produce electrical energy for the loads within that isolated grid when necessary. However, to do so, the microgrid itself must be resilient to both non-malicious failures and cyber-attacks. As I describe in the next section, a failure modes and effects analysis (FMEA) is one of the techniques that engineers can use to enhance resiliency.

The basic elements of a microgrid include generators, storage devices, and loads that we can control in a coordinated manner either while connected to the main power network or while isolated (islanded). figure 1 shows a SysML block definition diagram (BDD) of a notional microgrid system that I will use as an application example. The system consists of the following subsystems and components:

- a generator system, consisting of fuel tanks, a diesel engine, and a conventional (rotating electromagnetic) generator
- solar arrays, consisting of a controller, solar panels, and an inverter
- wind turbines, consisting of turbine units and a controller
- a battery subsystem, consisting of a controller, inverter, cell arrays, and a mechanical supporting structure. The battery subsystem stores energy generated by the intermittently running solar cells and wind turbines and can also be charged by the generator system
- an interconnect, which detects the presence or absence of incoming power and controls the connection to the main power grid
- voltage regulators, circuit breakers (common components across multiple subsystems)
- a microgrid control subsystem which controls the entire microgrid including power generation, charging and discharging of the battery backup, and power consumption (electrical load) control. I will use the microgrid control subsystem in the example discussed in figure 1.

This article describes an approach for automated FMEA generation using the microgrid control subsystem shown in figure 1. Section 3 describes the automated FMEA approach including representation of failure modes, transformations, and propagations using a SysML profile (a data structure definition that extends SysML to this specific purpose). The profile extends SysML through additional types, stereotypes, and relationships described in figure 1. Hecht et al. define the profile in greater detail in another publication (2020). Section 4 describes how such a model can generate an FMEA automatically using a plug-in developed for this purpose. (A plug-in is a Java program written to customize and extend the SysML tool.) Section 5 describes the output from the plug-in and how engineers can use it to make design decisions during the development process. Section 6 discusses the benefits of this approach, and section 7 provides concluding remarks.

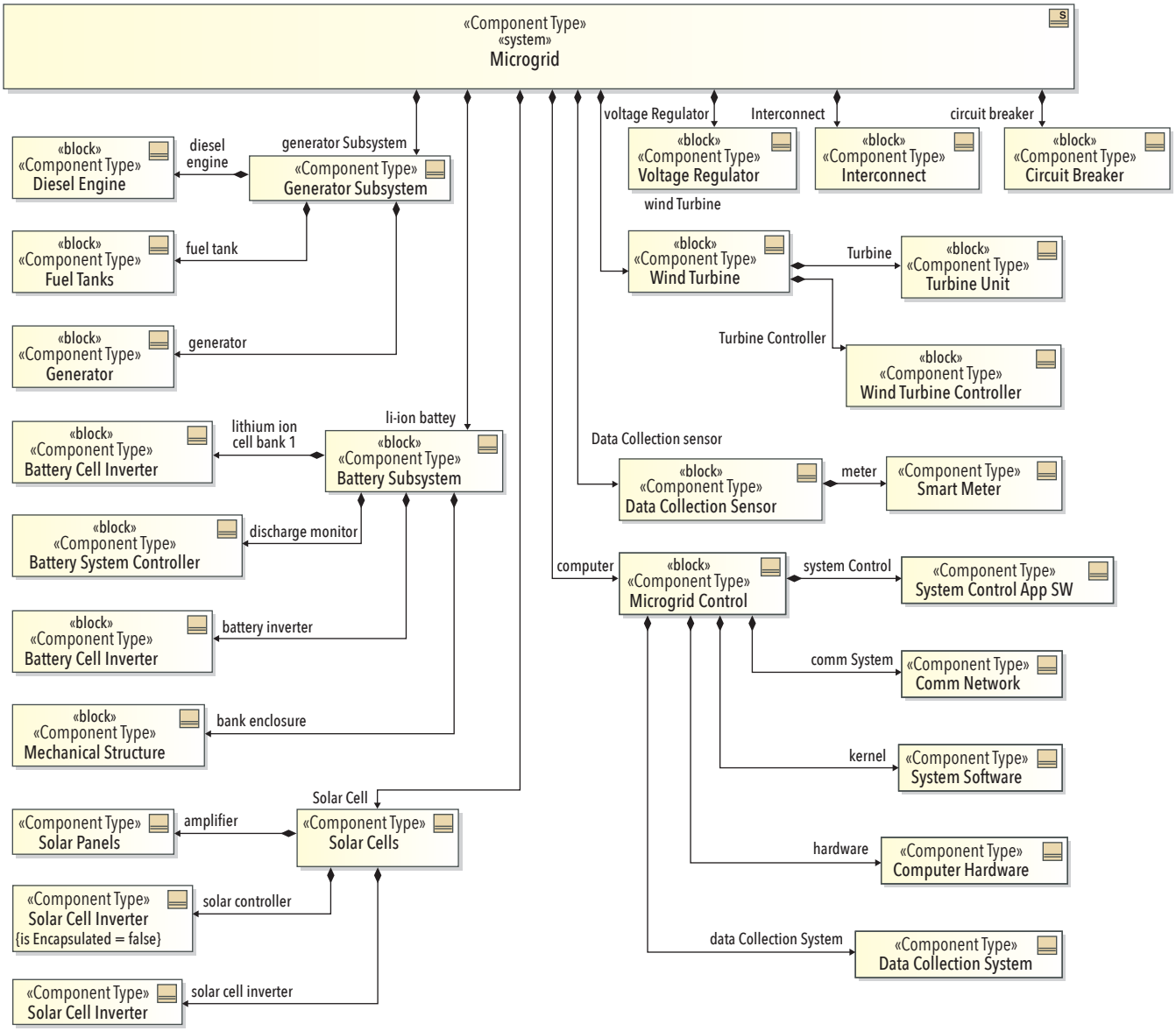


Figure 1. SysML block definition diagram of an example microgrid subsystem

SECTION 2 FAILURE MODES AND EFFECTS ANALYSES

Industries widely use FMEAs in safety- and mission-critical applications to identify the consequences of component failures, identify single points of failure, define maintenance strategies, and develop mitigations (resiliency measures). The technique examines each component and evaluates

- how that component can fail (its failure modes),
- the causes of such failures,
- the effects of each failure on the surrounding components and system,
- the severity of the failure effects,
- how the failure mode can be detected,
- what we can do to prevent or mitigate the effects of the failure, and
- what if any design changes are necessary to enhance detection and mitigation.

A variation of the FMEA, called a failure modes, effects, and criticality analysis (FMECA), adds an additional element–probability–to enable the evaluation of the risk (a product of the probability and consequence) of the failure mode. However, because the probabilities of many failure modes in microgrids are difficult to assess, the analysis described here does not consider the risk term. I discuss an alternative metric for assessing relative importance, the number of propagation paths through a component, in section 5.

Multiple domains mandate FMEAs for reliability safety including defense (US Department of Defense 1980; SAE 2014; US Department of Defense 2012); avionics (SAE 2010; SAE 1996); medical devices (ISO 2007; CDER and CBER 2006), and other industries (SAE 2012, IEC 2018).

While engineers have traditionally used FMEAs for non-malicious failures, they have also developed methods adapting them to cybersecurity analysis (Briggs et al. 2019; Wallace 2005). We can apply FMEAs to microgrids to identify where we can improve the failure detection and recovery capabilities of the design to enhance resiliency with respect to both spontaneously occurring non-malicious failures as well as those which malicious actors could introduce.

Ideally, engineers should produce FMEAs iteratively at multiple stages in the development process to identify failure detection and recovery deficiencies early so that design changes to improve resiliency are economically feasible. Unfortunately, industries do not usually follow this iterative practice because of associated costs and labor requirements. However, because of their

value, there has been significant interest in the development of automated techniques for generation of FMEAs so that iterative analyses would be feasible. One example is the work of IBM and the Grenoble Institute of Technology (Larsen et al. 2013). Other research demonstrated use of the architecture analysis and design language (AADL) error model to generate functional hazard analyses (the US Food and Drug administration uses similar FMEAs) for a medical device (Larsen et al. 2013). An Object Management Group (OMG) Working Group has created a SysML metamodel and library for the creation of FMEA tools (Biggs et al. 2019). However, the previously developed approaches are not suitable for large scale systems because they do not automatically handle failure propagation and transformation for large systems. The approach I describe here addresses this issue.

SECTION 3 AUTOMATED FMEA GENERATION APPROACH

The approach for automatically generating an FMEA I describe here is based on failure propagation and transformation calculus (FPTC) (Wallace 2005). FPTC views a system as a network of nodes and defines a notation which depicts a failure, after its origin, to be either propagated, transformed, or absorbed. We create an FMEA by logging a complete traversal of the network. We can also think of this network as a graph in which we represent the nodes as SysML blocks and represent the links as connections in an internal block diagram (IBD) as described in section 4.3. At each node, there are both incoming (sink) and outgoing (source) ports. The analysis represents specific failure modes as nested ports within the source and sink ports as shown in section 4.2. The FMEA represents propagation as a nested failure mode on the source port of a predecessor block connected to a successor failure mode of the same kind nested within the sink port of the destination block as described in section 4.3. The analysis represents transformation as a predecessor failure mode connected to a failure mode of a different kind as shown in section 4.4. Propagation paths are ordered sets of successive connections. The FMEA defines a failure propagation path by traversing connections between components until either (a) a system boundary is reached or (b) an absorbing transformation occurs within a block. A propagation path that reaches a system boundary results in a system effect. For each propagation path, the FMEA calculates a total length and identifies the locations of detection and mitigation nearest to the originating component. In addition to propagation and transformation between nodes, the FMEA can propagate

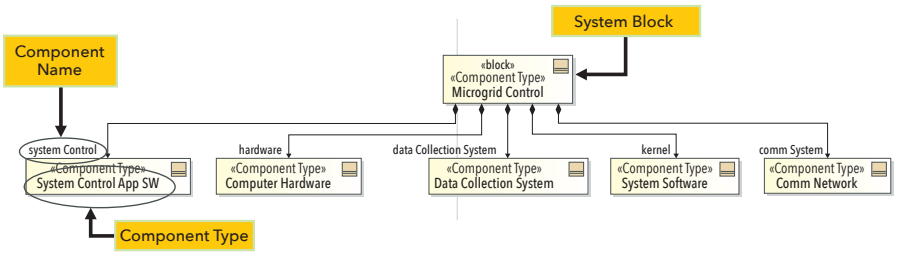


Figure 2. SysML block definition diagram of the microgrid control subsystem

or transform failure modes within a node. I describe the representations of such internal propagations and transformations in section 4.2. Once the analysis has traced all paths (including both inter-component and internal connections), it is possible to tabulate the number of components subjected to each failure mode thereby enabling prioritization. It is also possible to identify effects (such as externally observable failure symptoms) linked to each failure mode among all the propagation paths. Tabulation and summarization of such information provides greater insight into the failure behavior and vulnerabilities of the system. I describe these tabulations in section 5.

Manual approaches developed in accordance with *Procedures for Performing a Failure Mode, Effects, and Criticality Analysis* (US Department of Defense 1980), the original standard defining procedures for performing an FMEA, consider the only immediate effect, next higher-level effect, and end effects (propagations and transformations) of a failure mode thereby missing intermediate tertiary, quaternary, and higher-level effects. Because the automated approach traverses all failure propagation paths within a system, it can identify many more effects and opportunities for detection and mitigation. An example illustrating this point is a short circuit in a power supply for a database server. In a manual approach, the immediate effect of this failure mode would be a loss of output at the power supply, the next higher level is a loss of computing, and the end effect would be the loss of database services. However, there are collateral intermediate effects related to interruption of disk writing that would result in a corruption of database files. Because a conventional manual FMEA approach does not explicitly identify these collateral effects, it might not identify derived requirements for design measures to detect and mitigate such file corruption.

An advantage of comprehensively tracing propagation paths is to enable analysis not only of non-malicious failures but also of cyberattack paths. For such analyses, the approach identifies possible attack paths from a compromised processor (represented as a SysML block) and whether detections or mitigations (preventative/protective measures) exist along these paths. The approach would describe the description of the attack itself in the cause property of the FMEA profile described in (Hecht et al. 2020). The approach also enables the transformation of malicious attacks into physical failure modes and effects.

SECTION 4 AUTOMATED FMEA GENERATION PROCESS

The process for automated FMEA generation using SysML consists of five major steps:

1. System composition definition: defining the system and its components using a SysML block definition diagram
2. Component failure mode definition: defining component failure modes and internal transformations
3. Intercomponent propagation path definition: defining the failure propagations using SysML internal block diagrams
4. Failure mode propagation and transformation definition: defining the intercomponent failure propagations along each of the paths defined in the previous step using SysML association blocks and failure transformations using internal block diagrams
5. FMEA generation plug-in execution: a SysML modeling tool extension called a plug-in (a Java program integrated with the modeling tool) used for graph traversal and tabulation of results. The plug-in used in this work was implemented for Cameo Systems Modeler version 19 (3DS Catia/NoMagic 2019).

I discuss these steps in more detail in the following sections.

Section 4.1 System Composition Definition

A SysML representation (model) of the system under analysis is necessary, and if no such representation exists, the first step is to create it. This requires two diagrams: (1) a block definition diagram (BDD) to identify and define the items of which the system is composed, and (2) an internal block diagram (IBD) which describes how they are interconnected. I discuss the IBDs for automated FMEA generation in section 4.3.

Figure 2 is a BDD of the microgrid

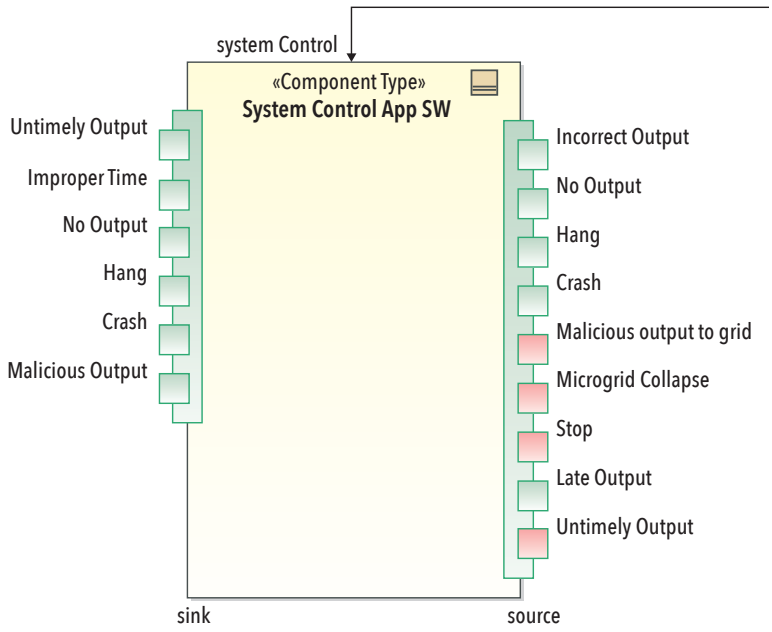
control subsystem, one of the subsystems of the microgrid shown in figure 1. The figure shows that the control subsystem is composed of five major components: system control application software, computer hardware, the data collection system, system software, and the communications networks. The BDD in figure 2 also shows the name that will identify each block in figure 4.

Section 4.2 Component Failure Mode Definition

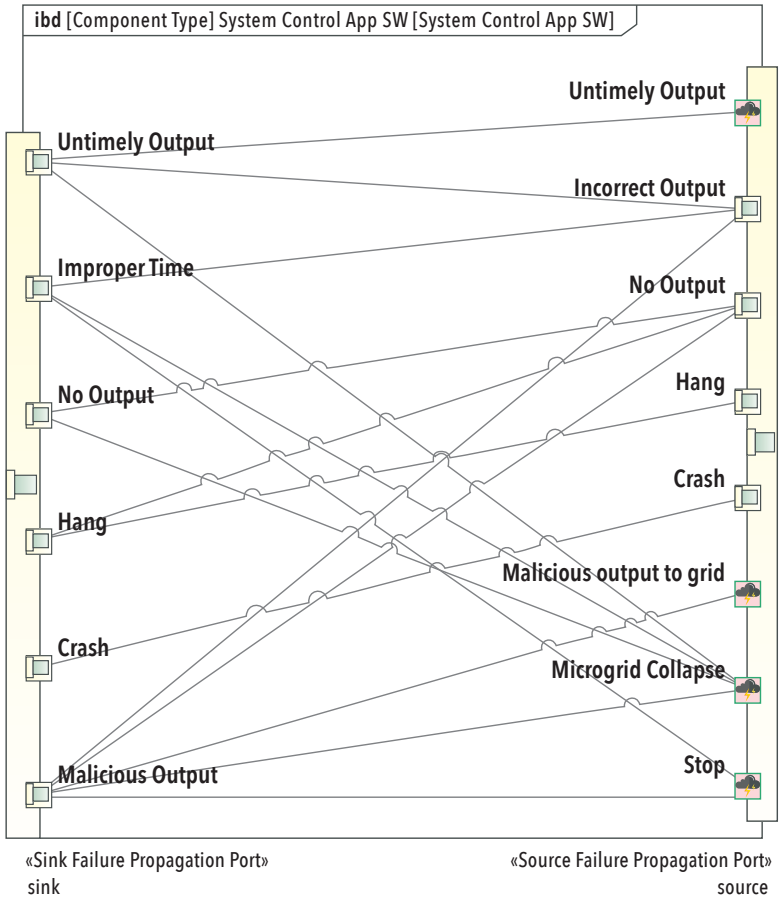
The next step is to define the failure modes, effects, and propagations within each of the components defined in step 1. Failure modes are represented as SysML ports that have properties defined in the FMEA profile (Hecht et al. 2020) mentioned in section 1. These additional properties include the failure mode name, cause, severity, detection method, mitigation method, and cybersecurity protection method (as a prevention measure against malicious failures caused by cyberattacks). Failure propagations from other components enter through the sink port. Failure originating in the component, propagating through the component, or being transformed within the component exit through the source port and spread to other components connected to the port. Figure 3(a) shows the system control application software block from the microgrid control subsystem (figure 2) with source and sink ports (outer ports) and the failure mode ports nested within them (inner ports). Some source failure modes are externally observable and are defined as system level effects. These ports are colored in light red. System level effects have an additional a property defining severity.

After we define the source and sink failure modes, it is necessary to define the intra-component failure propagations and transformations that link them. We define these internal failure propagations and transformations using a SysML IBD of the component as shown in figure 3(b). Horizontal lines connecting the input and output ports represent propagation. Diagonal lines represent transformations. In this diagram, an untimely output input failure mode can propagate into an untimely output failure mode but can also be transformed into an incorrect output or a microgrid collapse end effect in an extreme case.

I created analogous component failure mode representations (models) for the other components in figure 2. While it requires significant effort to create these models, once performed, we can preserve the work in component libraries. Thus, we can reuse both the failure modes and propagations



(a) definition of input (sink) and output (source) failure modes of a component. The pink colored ports are system effects.



(b) mapping of sink and source failure modes using a SysML internal block diagram

Figure 3. Component failure mode, propagation, and transformation definition of the system control application component within the microgrid control subsystem

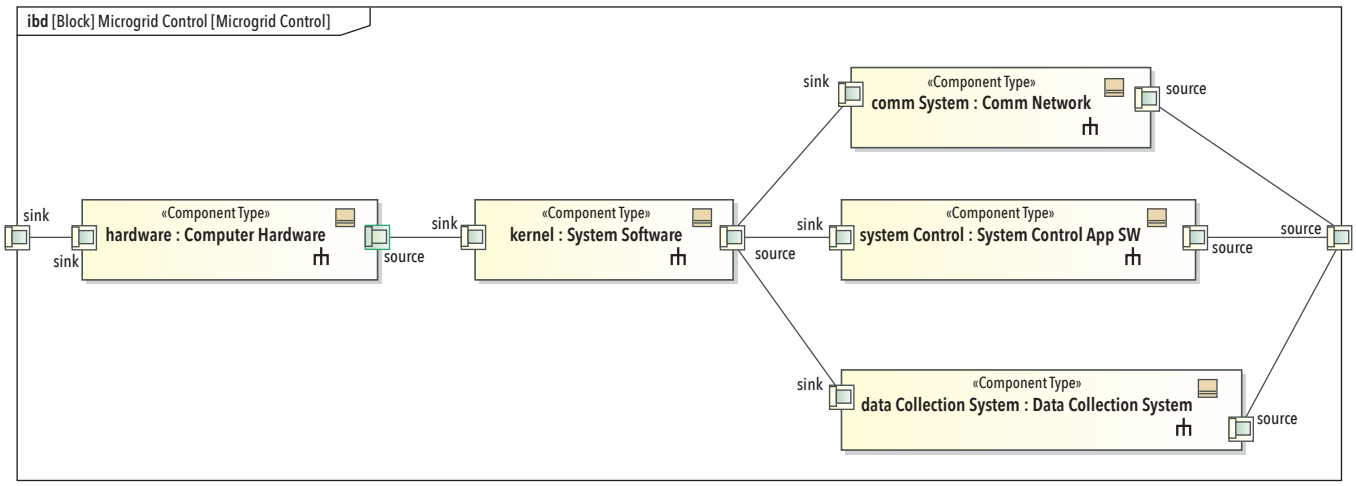


Figure 4. Intercomponent propagation path definition in the microgrid control subsystem

in future analyses thereby not only saving labor but also enabling standardization.

Section 4.3 Intercomponent Propagation Path Definition

In the third step, I describe the failure propagation paths among the components using a SysML internal block diagram (IBD). Engineers generally use SysML IBDs to show how components are connected and items (including data and power) flow through connectors and ports. However, we can also show failure propagation connections on the same primary design or architecture IBDs. On the other hand, dedicated failure propagation IBDs may be preferable because

a) the analysis should also include additional failure propagations that occur through mechanical means (overheating) that do not propagate along power or data paths, and,

b) because failures propagate through unique source and sink ports, the connections representing failure propagations are different from the other IBD connections and dedicated diagrams better represent them.

Figure 4 shows a dedicated failure propagation IBD for the subsystem shown in figure 2. Each of the blocks has failure modes, transformations, and propagations defined, as described in section 4.2. On the boundary of the diagram are a sink and source port because a microgrid control subsystem is part of the larger microgrid system. We can link such subsystem IBDs to create the complete system model. The subsystem IBD in figure 4 shows propagation of failures from hardware into the operating system (designated as system software) and then to the communication system, data collection system, and application software. However, the analysis does not define the details of failure propagation and transformation between the components until the next and last step.

Section 4.4 Intercomponent Failure Mode Propagation and Transformation Definition

The next step is defining the failure propagations and transformations between components. The IBD uses SysML association blocks, which define a connection between two blocks, for this purpose. The source port of the block from which the failure propagates is at one end of the association (the defined connection); the sink port to which the failure propagates is at the other.

Figure 5 (next page) shows how we can use SysML association blocks to represent the details of the failure propagation. Figure 5(a) shows the definition of the association between the source port of the hardware block and the skin port of the kernel block from figure 4. The name of the association is hardware-kernel. Figure 5(b) shows the connection (representing the propagation path) defined by the association block between the hardware and kernel components taken from figure 4 (the two left-most blocks) expanded to show the source and sink ports and nested failure modes. Figure 5(c) is an IBD of the connection defined in figure 5(a) shown in figure 5(b). It shows the source and sink ports at the two ends of the association as SysML participants (the term used to refer to the external connection points of the association). The IBD also shows the embedded failure mode ports. The diagram now represents the propagations and transformations between the source and sink ports of the hardware and kernel blocks using connectors in the same way that internal propagations and transformations were shown in figure 3. As was the case with the intracomponent failure propagations and transformations, the IBD represents failure propagations as horizontal lines connecting source and sink ports; it represents failure transformations as diagonal lines.

We must define the failure mode propagations and transformations between components for each connection using an association block to identify the connection and an internal block diagram to define the failure behavior within the connection. However, as was the case with the failure mode propagation and transformation definitions within a block, once created, we can reuse them if stored in library packages.

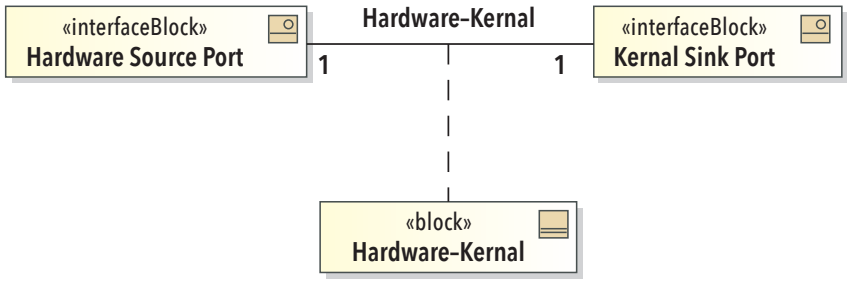
Section 4.5 FMEA Plug-in Execution

The failure modes, propagations paths, and transformations modeled in the previous steps result in a graph contained in the SysML model that we can traverse to characterize a failure propagation path from a source component to the system boundary. Each of the multiple paths for this traversal is a row in a failure modes and effects analysis. I have implemented a Java plug-in for Cameo Systems Modeler to perform this traversal and collects the data to form the primary FMEA and additional summary tables.

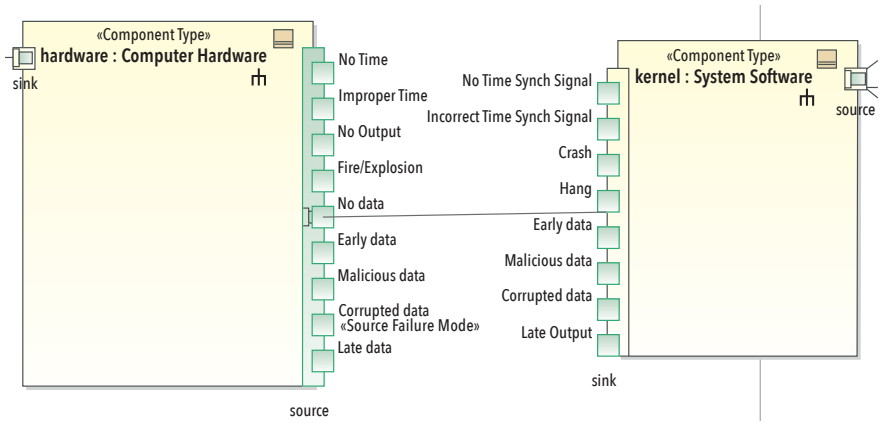
The plug-in first finds each component and searches for an originating source failure mode of that component. It performs this process of identifying propagation path origination using a depth-first search with a recursive algorithm. The traversal continues by following failure propagations until it reaches a system level effect. As it traverses each propagation path, the plug-in forms a failure propagation tree structure. When the traversal is complete, the propagation path tree structure contains all the information needed for the FMEA. A component and failure mode from a single point in a failure propagation path creates nodes in the failure propagation tree. The children of each node correspond to the components that the node's failure can affect, as well as the

effect of the failure. Nodes corresponding to system level effects do not have children since they terminate failure propagation. The recursive algorithm determines what the children are by referencing a previously created failure transformation lookup table. It recursively calls itself on the children to continue the failure propagation. Propagations stop when the plug-in reaches system effects. Once the propagation path tree is complete, the plug-in performs another depth-first search on the tree to extract each individual failure propagation path. It then outputs these paths as rows in a worksheet contained in a Microsoft Excel spreadsheet file. It performs additional analysis such as counting occurrences of specific failure patterns to create summary tables. It then outputs these summary tables as additional worksheets. I will describe the worksheet contents in section 5.

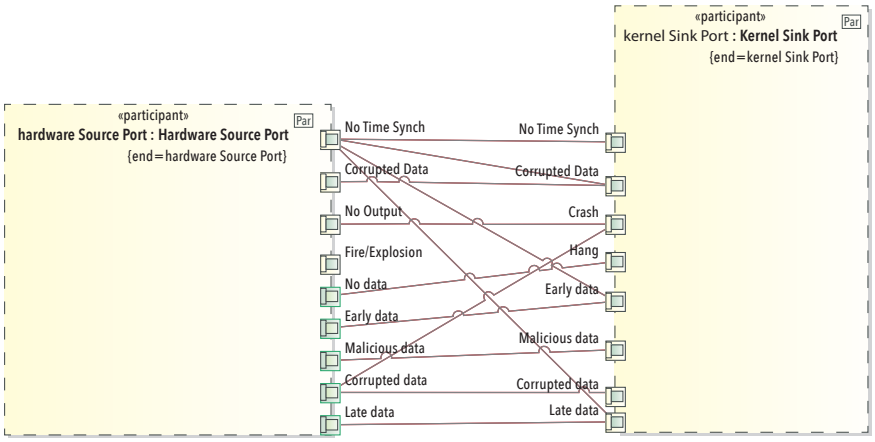
The user invokes the plug-in with a single command. The plug-in usually completes the generation process in under a minute but is dependent on the size of the model. The algorithm used in the plug-in can process any model that has originating failure modes and valid propagation paths, even if not complete (a validation function within the plug-in identifies omissions with warnings). Thus, the user can perform partial analyses at any time, thereby enabling an iterative approach for early identification of design changes that can improve resiliency.



(a) SysML association block defining the failure propagation connection between source (hardware) and sink (kernel) port



(b) Hardware source port and kernel sink port expanded on their respective blocks to show failure modes and propagation connection



(c) Internal block diagram of the association block from part (a) of this diagram showing the source and sink ports, the nested failure modes, and then failure mode propagations and transformations along the connection

Figure 5. Defining intercomponent propagations and transformations

Section 5 Analysis Output

The plug-in produces the output tables listed in Table 1. This section describes the content and use of these outputs. The output is in a Microsoft Excel file to enable subsequent reformatting for presentation and further data analysis for visualization of important failure properties of the system.

Figure 6 shows a portion of the full FMEA that the tool generates (8 of the 23 columns are shown). For the example microgrid control subsystem described here, there are 607 propagation paths with unique originating components, failure modes, causes, propagation steps, and end effects. With a conventional FMEA, which considered only the immediate, next higher level, and effects, there are only 46 rows.

The complete set of columns in the table are:

- Component level: the hierarchical level of the component (the FMEA tool can consider multiple hierarchical levels–not shown in this excerpt)
- Failed component: identification of the specific component and component type
- Failure mode: identification of the failure mode
- Internal cause: cause of the failure mode. If there are multiple causes, the FMEA lists each cause on a separate line because the protection/prevention measures would differ
- Intermediate effects: identification of each of the effects (secondary failures) as the primary failure propagates through the system until its end effect. Note that propagation description table details this propagation path further detailed.
- Intermediate causes: the causes associated with each of these intermediate effects (not shown in this excerpt)
- Intermediate detections: means of detecting the intermediate effects
- End component: the component at which the failure propagation terminates (end effect)

Table 1. FMEA generation tool output

Table	Description and Use
Full FMEA	List all FMEA information in SysML model Rows represent individual failure propagation paths
Failure modes and effects summary	Provides both qualitative and quantitative data about each failure mode and effect Enables resource prioritization by identifying system components with the highest number of failure modes, undetectable or unmitigated failure modes, and long propagation paths
System effects summary	Provides analysis of all system effects in system Useful for identifying undetected, unmitigated, or unprotected system effects
Diagnostics table	Matrix of system effects versus their causes Capable of determining probable causes of system effects
Propagation description	Rows represent individual failure propagation paths Each cell in a row lists detailed information about a single failure propagation step

- End cause: the cause of the failure at the end component (not shown in this excerpt)
- End effect: the end of effect of the failure (not shown in this excerpt)
- Severity: the severity of the end effect
- Severity comment: explanation or uncertainty in determining the severity (not shown in this excerpt)
- Detection: detection of the end effect (not shown in this excerpt)
- Mitigation: mitigation of the end effect (not shown in this excerpt)
- Protection: a protective or preventative measure to prevent the failure or cyberattack effect from occurring (not shown in this excerpt)
- Comment: explanation of the protective measure or documentation of uncertainty (not shown in this excerpt)
- # Propagations: number of components involved in the propagation from the primary failure mode to the end effect (not shown in this excerpt)
- First known detection: first component in the propagation path at which the failure can be detected (not shown in this excerpt)
- # Propagations to detection: number of components affected by the failure until it is detected (not shown in this excerpt)
- First known mitigation: first component at which a mitigation of the failure can occur
- # Propagations to mitigation: number of propagations to the mitigation
- First known protection: first protective measure along the propagation path that can prevent failure propagation from occurring (particularly relevant to cybersecurity)
- # Propagations to protection: number of components involved in the propagation until the protective measure is reached
- Intermediate detections: list of all detection mechanisms other than the primary and end effect detections along the propagation path
- Intermediate mitigations: list of all mitigations other than the primary and end effect mitigations along the propagation path
- Intermediate protections: list of all protection measures other than the primary and end effect protection measures along the propagation path
- Intermediate comments: explanation or uncertainties on the intermediate detections, mitigations, or protections.

The second output table is the failure modes and effects summary (FMES), an excerpt of which is shown in figure 7 for the microgrid control subsystem (the full FMES for this example has 56 rows and 18 columns). The FMES enables a rapid identification of the failure modes that lead to the most severe effects, components with the most failure modes, the most used detection and mitigation effects, and the distribution of failure modes by severity. In this excerpt, the hardware corrupted data failure mode has the largest number of occurrences (rows). However, the kernel

Failed Component	Failure Mode	Internal Cause	Intermediate Effects	Intermediate Detections	End Component	End Effect	Severity
kernel	No data	Hardware or software failure	data Collection : No data	data Collection : Timeout	Microgrid Control	No data	2
kernel	Early Data	Software or timing failure	data Collection System : Early data; data Collection System : Bad Data	data Collection : Reasonableness Check; data Collection : Reasonableness Check	computer	Bad data	3
kernel	Early Data	Software or timing failure	data Collection System : Early data; data Collection System : Bad Data	data Collection : Reasonableness Check; data Collection : Reasonableness Check	Microgrid Control	Bad data	3
kernel	Malicious data	Cyberattack	data Collection System : Malicious data; data Collection System : Falsified Data	data Collection : Reasonableness Check; data Collection : Reasonableness Check	computer	Falsified data	1

Figure 6. Failure modes and effects analysis (excerpt)

Component	Failure Mode	Primary Failure Mode Occurrences	Intermediate Effects and Occurrances	Unique Failure Modes and Effects Occurrences	Total Failure Modes and Effects Occurrences	Detection	Mitigation	Protection	Severity 1	Severity 2	Severity 3
hardware	Corrupted Data	62	0	1	62	Unknown Detection	Unknown Mitigation	Unknown Protection	24	10	20
hardware	No Output	22	0	1	22	Timer Expiration	Retry or substitute default	Unknown Protection	8	4	10
kernel	Crash	12	44	3	56	Reasonableness Check	Unknown Mitigation	Unknown Protection	16	10	30
kernel	No Output	10	40	5	50	Timer Expiration	Retry or substitute default	Unknown Protection	40	10	0
hardware	No data	24	0	1	24	Timer Expiration	Retry or substitute default	Unknown Protection	12	6	6
kernel	Hang	12	24	2	36	Reasonableness Check	Unknown Mitigation	Input Validation	16	8	12
comm System	Hang	2	8	3	10	Timer Expiration	Restart	Unknown	4	0	6
system Control	Hang	2	8	3	10	Timer Expiration	Restart	Unknown Protection	4	0	6
data Collection System	Hang	4	8	3	12	Timer Expiration	Restart	Unknown Protection	0	6	6
hardware	Early data	56	0	1	56	Timer Window	Reject data and	Input Validation	20	10	20

Figure 7. Failure modes and effects summary table (excerpt)

no output failure mode has both high occurrences (rows) and the highest number of severity 1 (most severe) occurrences. Therefore, its mitigation should receive the highest priority in the microgrid development effort. However, as we can see in this example, there the analysis has not defined any mitigation measures yet.

The specific columns in the FMES are:

- Component level: in an analysis that uses a hierarchical analysis, the nesting level of the component
- Component: name or identification of the component
- Component description: description of the component (taken from the SysML block documentation field)
- Failure mode: failure mode of the component (taken from the sink failure mode)
- Failure mode description: more detailed description of the failure mode (hidden in this output)
- Primary failure mode occurrences: number of times this failure mode appears as a primary (for example, left most) failure mode
- Intermediate effects occurrences: number of times this failure mode appears as an effect (like after the first failure mode)
- Unique failure modes and effects occurrences: number of unique propagation paths in which this failure mode appears
- Total failure modes and effects occurrences: sum of primary and intermediate failure mode occurrences
- Detection: means of detecting this failure mode
- Mitigation: means of recovering from or otherwise limiting the severity of the failure mode
- Protection: means of preventing this failure mode (particularly important if it cannot be detected or recovered from)
- Comment: comment containing assumptions, unknowns, or requirements associated with this failure mode
- Severities: count of propagations in which this failure mode is associated with a highest severity (severity 1) effect to the lowest (severity 5).

The third analysis product is the system effects table that shows components and counts of end effects, detections, mitigations, and protections. Figure 8 is an excerpt; there are a total of 17 rows in this table representing the end effects that the analysis identified. This enables assessment of the system's dominant externally observable failure behaviors.

The table contains the following information:

- Component: the component at the end of the propagation chain
- System effect: the end effect on the system
- Total system effect occurrences: total number of occurrences of the end effect
- First known detection, number of occurrences: the first detection measures along the propagation chain and the number of occurrences

Component	System Effect	Total System Effect Occurrances	First Dectection : Number of Occurrences	First Mitigation : Number of Occurrences	First Protection : Number of Occurrences	Severity
computer	No data	56	Authentication, reasonableness check : 11; Self announced : 1 Timing Window : 5; CRC : 3; BIT/Remote diagnostics : 1; Reasonableness Check : 10; Timer Expiration : 25;	Redundancy : 1; Retry or substitute default values : 48; Reject data and retry : 5; Restart : 2;	Unknown Protection : 11; General Code Scanner : 15; Input Validation : 19; Vulnerability analysis and mitigation : 11;	2
computer	Falsified data	9	Authentication, reasonableness check : 3; Timing Window : 1; Reasonableness Check : 3; Timer Expiration : 2;	Retry or substitute default values : 8; Reject data and retry : 1;	General Code Scanner : 3; Input Validation : 3; Vulnerability analysis and mitigation : 3;	1
computer	Bad data	15	Authentication, reasonableness check : 1; Timing Window : 3; CRC : 2;; Reasonableness Check : 3; Timer Expiration : 6;	Retry or substitute default values : 12; Reject data and retry : 3;	General Code Scanner : 3; Input Validation : 11; Vulnerability analysis and mitigation : 1;	3

Figure 8. Systems effects table (excerpt)

Observable System Effect	Components with Related Propagation Paths				
	Comm System	Data Collection System	Hardware	Kernel	System Control
Mission Terminating Result	1	1	71	21	5
Late Output	2	1	19	6	3
Mission Terminating Result	1	1	71	21	5
Late Output	2	1	19	6	3
Loss of Data	4	3	50	17	4
Loss of Data	4	3	50	17	4
Comm Failure	3	0	7	2	0
Comm Failure	3	0	7	2	0
No Data	0	6	38	12	0
No Data	0	6	38	12	0
Falsified Data	0	1	6	2	0
Falsified Data	0	1	6	2	0
Bad data	0	1	10	4	0
Bad data	0	1	10	4	0
Destroyed Computer	1	1	0	0	1
Destroyed Computer	1	1	0	0	1

Figure 9. Diagnostic table

hardware : Computer Hardware Failure Mode: No Time Synch Cause: Timing failure	kernel : System Software Failure Mode: Early data Cause: Unspecified Cause Detection: Reasonableness Check Mitigation: Unknown Mitigation Comment: Protection: Input Validation	kernel : System Software Failure Mode: Incorrect Output Cause: Unspecified Cause Detection: Reasonableness Check Mitigation: Retry or substitute default values Comment: Protection: General Code Scanner	data Collection System: Data Collection System Failure Mode: No data Cause: Unspecified Cause Detection: Timeout Mitigation: Unknown Mitigation Comment: Protection: Unknown Protection	computer : Microgrid Control Failure Mode: No data Cause: Unspecified Cause Detection: Timer Expiration Mitigation: Retry or substitute default values Comment: Protection: Unknown Protection Severity: 2 Severity Comment:
hardware : Computer Hardware Failure Mode: No Time Synch Cause: Timing failure	kernel : System Software Failure Mode: Early data Cause: Unspecified Cause Detection: Reasonableness Check Mitigation: Unknown Mitigation Comment: Protection: Input Validation	kernel : System Software Failure Mode: Incorrect Output Cause: Unspecified Cause Detection: Reasonableness Check Mitigation: Retry or substitute default values Comment: Protection: General Code Scanner	data Collection System: Data Collection System Failure Mode: No data Cause: Unspecified Cause Detection: Timeout Mitigation: Unknown Mitigation Comment: Protection: Unknown Protection	Microgrid Control : Microgrid Control Failure Mode: No data Cause: Unspecified Cause Detection: Timer Expiration Mitigation: Retry or substitute default values Comment: Protection: Unknown Protection Severity: 2 Severity Comment:

Figure 10. Propagation description table (excerpt)

- First known mitigation and protection number of occurrences: the first mitigation measures along the propagation chain and the number of occurrences
- First known protection number of occurrences: the first protection measures along the propagation chain and the number of occurrences
- Severity: severity of the system effect.

For the microgrid control subsystem example, this table shows that (1) falsified data is the most severe end effect but the analysis has identified mitigation, detection, and protection measures for all such effects, and (2) no data is the second most severe effect with more propagation paths than the falsified data failure mode and the analysis has also identified measures for mitigation, detection, and protection.

The fourth analysis product is the diagnostics table, shown in figure 9, which enables an assessment of what is the most likely item to have failed given the externally observable system effect. The number of rows is equal to the number of components/end effect combinations; the number of columns is the number of components (plus the adversary block). Using the top row as an example starting from the left, one failure mode from the communication system or the data collection system could lead to a mission terminating result, but that 71 failure modes from the data collection could lead to that effect. Thus, if it were to occur, hardware would be the first component the analysis would examine for a root cause. On the second row, 19 hardware failure modes could lead to a late output effect.

We can use this table as an aid in assessing the likely causes for a given symptom because it provides a measure of the relative likelihood of each component to be the root cause leading to the system end effect. Hence, it is called a diagnostics table.

The final analysis product is the propagation description table shown in figure 10. The table shows the propagation description table detailing the propagation of each failure mode. It expands the condensed propagation information in the full FMEA. Each cell represents a single step in a failure propagation path. There are the same number of rows in the propagation as in the original FMEA (1110 in this case). The cells describe the component, failure mode, cause, detection measure, mitigation measure, a comment, and protection. To support cybersecurity assessments, propagation steps with protections are shaded in green, and the end or system level effects are shaded in brown.

Analysts can make a visual assessment of the state of the design by assessing whether a green cell (indicating a mitigation or protective measure) is present on any row where there is a brown cell. In figure 10, the protective measure of a reasonableness check can protect against two failure modes of no time synch from the computer hardware. Where protection measures are absent, the analysts should examine the existing mitigation and detection measures intended to support reliability and safety and determine whether these are sufficient for cybersecurity purposes.

SECTION 6 DISCUSSION

The methodology I describe in the previous section reduces the labor and time required for systems engineers and analysts by reducing repetitive tasks required to manually create an FMEA but does not eliminate the need for expert and knowledgeable input. A knowledgeable engineer or analyst must still originate and manually enter failure modes and internal transformations for each component–but only once. In a conventional FMEA, they would be repeated on each row. Similarly, a knowledgeable individual would have to manually identify propagations and transformations, but only between components and their nearest neighbors. The propagation algorithms would automatically generate the component to system effect by traversing the paths (hence, our characterization of this tool as an automated FMEA generation technique). Finally, when design changes result in a system model change, an analyst can generate the FMEA reflecting the changes automatically. As a result, the engineer can immediately assess the impact of design changes on reliability, safety, and cybersecurity, and produce a superior system or product.

Because the analysis identifies all propagation paths completely, the outputs this FMEA approach produces contain far more information than the traditional methodology. The additional reporting formats defined in figures 7 through 10 enable a summarization of the information so that engineers can make informed decisions despite the significantly larger number of rows that the FMEA produces. For example, the distribution of failure mode severities by component in the FMES (figure 7) enables the identification of vulnerable or critical

components and helps prioritize design and analysis resources; the analyst or engineer can use the system effects table (figure 8) to identify the best placement of detection and recovery provisions. The diagnostics table (figure 9) aids the creation of maintenance manuals and troubleshooting procedures by enabling the association of an observable system with the most likely component. Users can develop their own queries as additional needs arise. For example, if a traditional FMEA with only the immediate, next higher level, and effects is required, a user can make a query to find unique records of the first two propagations and the end effects, ignoring the additional propagation that the FMEA identifies.

SECTION 7 CONCLUSIONS

This paper describes an automated FMEA generation capability using the SysML modeling language and describes its application to a simple microgrid control computer network which is typical of other critical infrastructure control systems. I also present the outputs produced by the tool (implemented as a SysML plug-in) from this analysis and show the insights into the design that the FMEA can achieve.

The fundamental innovation in this approach is the identification and enumeration of all failure propagation paths and the detailed documentation of the failure transformations, detection measures, mitigation measures, and protective measures that we can apply to these devices to prevent or mitigate the impact of the anomaly. By doing so, we can expand the traditional FMEA approach to analysis of cyberattack vectors.

Because this approach is automated, we can readily integrate it into a system development effort using model-based systems engineering (MBSE). We can readily repeat the analysis throughout the design and use it frequently to assess a system design, identify weaknesses, and take corrective actions to create a more resilient and robust system. ■

REFERENCES

- 3DS Catia/NoMagic. 2019. "Cameo Systems Modeler." https://www.nomagic.com/products/cameo-systems-modeler.
- Biggs, G., A. Armonas, T. Juknevicius, K. Post, N. Yakymets, and A. Berres. 2019. "OMG Standard for Integrating Safety and Reliability into MBSE: Core Concepts and Applications." Paper presented at the 29th Annual International Symposium of INCOSE, Orlando, US-FL, 20-25 July.
- Gorbenko, A., V. Kharchenko, O.Tarasyuk, and A. Furmanov. 2006. "F(I)MEA-Technique of Web Services Analysis and Dependability Ensuring. In Rigorous Development of Complex Fault-Tolerant Systems edited by M. Butler, C. B. Jones, A. Romanovsky, and E. Troubitsyna, 153-167. Berlin, DE: Springer.
- Hecht, M., A. Chuidian, T. Tanaka, and R. Raymond. 2020. "Automated Generation of FMEAs Using SysML for Reliability, Safety, and Cybersecurity." Paper presented at the Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling, Vancouver, CA, 20-23 August.
- IEC (International Electrotechnical Commission). 2018. IEC 68012:2018. Failure Modes and Effects Analysis (FMEA and FMECA). Geneva, CH: IEC.
- ISO (International Standards Organization). 2007. ISO 14971:2007. Medical devices—Application of Risk Management to Medical Devices. Geneva, CH: ISO.
- Larson, B., J. Hatcliff, K. Fowler, and J. Delange. 2013. "Illustrating the AADL Error Modeling Annex Using a Siumpole Safety-Critical Medical Device." Paper presented at the Association for Computing Machinery SIGAd Annual Conference on High Integrity Language Technology, Pittsburgh, US-PA, 12-14 November.
- Pierre D., V. Idasiak, and F. Kratz. 2010. "Reliability Study of Complex Physical Systems Using SysML." Reliability Engineering and System Safety 95 (4): 431–450.
- Schmittner, C., T. Gruber, P. Puschner, and E. Schoitsch. 2014. "Security Application of Failure Mode and Effect Analysis (FMEA)." Paper presented at the 33rd International SAFECOMP Conference, Florence, IT, 10-12 September.
- SAE (Society of Automotive Engineers), 1996. ARP4761. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Warrendale, US-PA: SAE.
- ——. 2002. J1739_200208. Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA). Warrendale, US-PA: SAE.
- ——. 2010. ARP4754A. Guidelines for Development of Civil Aircraft and Systems. Warrendale, US-PA: SAE.
- ——. 2012. ARP5580. Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications. Warrendale, US-PA: SAE.
- ——. 2014. GEIASTD0009. Reliability Program Standard for Systems, Design, Development, and Manufacturing. Warrendale, US-PA: SAE.
- (CDER) US Center for Drug Evaluation and Research and (CBER) Center for Biologics Evaluation and Research. 2006. Q9 Quality Risk Management. FDA-2005-D-0334. Washington, US-DC: Food and Drug Administration.
- US Department of Defense. 1980. Procedures for Performing a Failure Mode, Effects, and Criticality Analysis. MIL-STD-1629A. Washington, US-DC: Department of Defense. https://www.fmea-fmeca.com/milstd1629.pdf.
- ——. 2012. Standard Practice for System Safety. MIL-STD-882E. Washington, US-DC: Department of Defense.
- US Department of Energy Microgrid Exchange Group and the CIGRE 6.22 Working Group. 2019. "Microgrid Definitions." https://building-microgrid.lbl.gov/microgrid-definition.
- Wallace, M. 2005. "Modular Architectural Representation and Analysis of Fault Propagation and Transformation." Electronic Notes in Theoretical Computer Science 141 (3): 53-71.

ABOUT THE AUTHOR

Myron Hecht is a senior project leader at The Aerospace Corporation where he specializes in reliability, safety, and systems engineering for satellites and ground control systems. He also is a consultant to the Nuclear Regulatory Commission in reactor safety and control systems and a lecturer at the UCLA School of Engineering and Applied Sciences. His current research is on model-based system engineering and its application to reliability, availability, and safety analysis. He has previously made research contributions in the areas of integrated hardware/software reliability modeling analysis, fault tolerant computing, and real time distributed control systems. He has served on standards committees for reliability, computers in nuclear power plants, and software in avionics systems. He is an author of more than 90 refereed publications in reliability, safety, products liability, and systems engineering. Myron holds a BS in chemistry, an MS in nuclear engineering, an MBA, and a JD degree all from UCLA.

JUNE 2020
VOLUME 23/ ISSUE 2

Microgrids—A Watershed Moment

George H. Baker, bakergh@jmu.edu

■ **ABSTRACT**

Microgrids are rapidly transitioning from research and test beds into commercial markets and installations. The application of microgrids to replace significant portions of Puerto Rico's electric grid in the aftermath of 2017 hurricanes Harvey and Maria show the maturity of the technology. Microgrids offer many benefits including enhanced reliability, reduced life cycle costs, improvements in power quality and efficiency, demand reduction, reduction in fossil fuel emissions by using renewable and nuclear generation, and installation flexibility for both urban and rural applications. Experts forecast the microgrid market to reach USD 31 billion by 2027.

However, microgrids might not be a silver bullet solution for problems associated with the larger electric power "macrogrid." Because of their organic digital monitoring and control systems, microgrid networks are highly susceptible to cyberattacks and accidental or intentional electromagnetic interference-caused debilitation. Energy storage technology supporting renewable energy systems is expensive and can fail catastrophically. Furthermore, integration of microgrids into the larger existing electric power networks, without attention to protection engineering, actually increases the vulnerability of the resulting network of electric power systems. We must take care in the design and installation of microgrids because of the complexity they add to the larger electric power system including added cyberattack vectors, transient current and voltage surges engendered by rapid changes in solar and wind generation output, and microgrid component susceptibility to nuclear and directed energy electromagnetic pulse (EMP) threats. We are at a historic technological juncture with distributed microgrid energy sources gaining momentum in displacing bulk electric power. We must now ensure that we incorporate combined physical security, cybersecurity, and EMP protection engineering into the initial designs of microgrids to avoid increasing the vulnerability of our electric power networks.

INTRODUCTION

This paper is based on a session at the INCOSE EnergyTech 2018 Conference and Exhibition held at the Cleveland Expo Center in US-OH. I organized the session to make the case for designed-in protection of a growing number of microgrid installations against wide-area threats to the nation's electric power system. These threats include electromagnetic pulse (EMP), major solar storm geomagnetic disturbances (GMD), cyberattacks, and physical attacks. The session described the history of microgrid development and technology, and microgrid applications including benefits and detriments. Session panelists described the wide variety of microgrid designs distinguished by the decentralized energy sources used, namely, renewable sources, hydrocarbon generation systems, nuclear power systems, and chemical sources for both power generation and energy storage.

Panelists provided insights into microgrid threats and their consequences and illuminated specific vulnerabilities to wide-area threats. Panelists also presented established protection engineering methods. It became clear that microgrids require a two-track grid protection approach. A program to protect the national electric power grid or "macrogrid" is the ultimate goal, but this is a longer-term project due to the enormity of the system involved; the macrogrid is highly complex and includes generation, transmission, and distribution systems. We can accomplish a shorter-term program to protect local critical services using hardened microgrids.

Because we are early in the microgrid implementation process, there is major benefit to incorporating EMP, GMD, cyber, and physical protection in the initial designs of new microgrid systems. Post-installation protection retrofit costs are an order of magnitude higher than designed-in protection.

MICROGRIDS—A BRIEF HISTORY AND DEFINITION

Starting in the late 1990s, scientists and engineers in the United States and Europe began to develop decentralized solutions that could manage the integration of thousands or tens of thousands of distributed energy resources (DER) in a way that would maximize reliability and resilience in the face of natural disasters, cascading power failures, physical attacks, and cyberattacks.

Grid architectures evolved that can manage electric generation and demand locally in subsections of the grid that can also be islanded from the larger grid to provide critical services if the main grid fails. These architectures are what we call microgrids. The US Department of Energy defines a microgrid as "a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island-mode" (Ton and Smith 2012, 84).

Microgrids are now emerging from lab

benches and pilot demonstration sites into commercial markets, driven by technological improvements, cost reductions, a proven pilot program track record, and a growing recognition of their benefits. At this time, unfortunately, microgrid designs and installations have not addressed wide-area debilitating electromagnetic effects, including nuclear EMP and electromagnetic directed-energy weapons, also known as radio frequency (RF) weapons. As a result, microgrid installations, since their inception, remain vulnerable to these threats. In addition, over the same period, cyber protection has been largely ignored in microgrid installations.

Microgrids come in varied sizes and power source types driven by type and location of the system(s) they power. Power source types include (1) renewable sources (solar, wind, hydro, and geothermal energy); (2) fossil fuel (liquid and gas); (3) small nuclear power modules; and (4) chemical storage and generation devices, such as batteries and fuel cells.

Various combinations of these power source types are incorporated into microgrid architectures applied to the following, from smallest to largest:

- Buildings and facilities—homes, data and communication centers, hospitals, freshwater and wastewater facilities, government buildings, food storage sites, fueling facilities, and so on.
- Larger business enterprise and academic campuses—universities, shopping centers, residential complexes, and research facilities, such as Princeton University, St. Olaf College, and the US Centers for Disease Control and Prevention.
- Communities and military bases.

Microgrids offer many advantages that are accelerating their incorporation as primary power sources. Two primary benefits are they reduce unacceptably high risks of extended electric grid outages by incorporating organic power sources independent of local electric distribution systems, and they can provide backup power if the larger grid fails. Many microgrid installations are installed to replace unreliable and aging electric infrastructure. Microgrids can also provide reliable electricity to areas with no access to an electric power grid.

Microgrids provide a flexible framework for integrating renewable energy sources within a DER architecture. Microgrid power feeds provide enhanced power quality because they are less susceptible to transients and electrical noise common to the larger grid. Solar-, wind-, and nuclear-powered microgrids reduce particulate and gas environmental emissions. To enable optimum efficiencies in the use of intermittent solar and wind renewable sources, microgrids must use intelligent control systems linking system components. These control systems, if not properly protected, introduce system-debilitating vulnerabilities to natural and malicious electromagnetic threats.

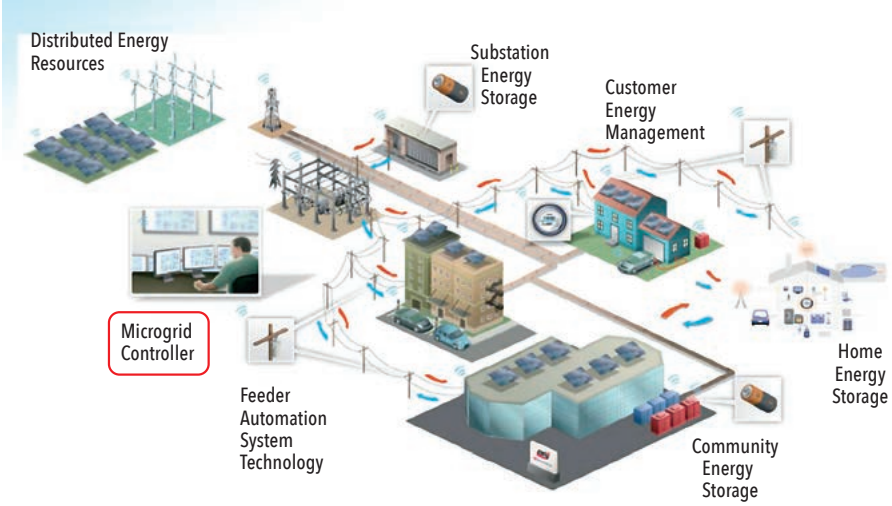


Figure 1. Microgrid architecture showing rest-of-grid (ROG) connection (Institute for Local Self-Reliance 2016a)

An important microgrid attribute, in relation to improved grid survivability and recovery, is their inherent islanding capability. Microgrid islands can continue to function during blackout contingencies and can be helpful in black starting the larger electric grid. If properly designed, we can isolate microgrids into electrical islands on command to protect connected assets from blackouts or EMP- or GMD-caused grid transients.

Other benefits include dual heating and power generation capabilities provided by solar-, geothermal-, fossil fuel-, and nuclear-powered microgrids; the ability to supply reliable electricity to areas with no access to an electric grid; and the elimination or reduction of particulate and gas environmental emissions. If properly designed, microgrids overcome reliability problems with large, regional electric power grids due to weather, cyber, physical, and EMP and GMD vulnerabilities.

Prevalent microgrid applications include data and communication centers, airports (such as Atlanta, US-GA's Hartsfield Airport), hospitals, military bases (such as Joint Base San Antonio, US-TX, Creech Air Force Base, US-NV, Port Hueneme, US-CA, and Ft. Sill, US-OK), and planned resilient communities (such as Carson City, US-CA and the Philadelphia, US-PA Navy Yard community microgrid).

Connecticut was the first US state to pass legislation in 2011 authorizing microgrids to serve community resilience. To encourage microgrid adoption, Connecticut proposed a microgrid funding program in July 2012 as a response to Hurricane Irene which gained momentum after Hurricane Sandy hit in late October 2012. Several additional states have followed Connecticut's lead, establishing programs to support microgrids. These states include California, Hawaii, Maryland, Massachusetts, New Jersey, New York, Rhode Island, and the District of Columbia. The most extensive implementation of microgrids is in Puerto Rico which, following extensive hurricane damage, is replacing its entire distribution grid with large, interconnected microgrids (Wood 2019).

The government implements its support for microgrids in several ways. These include financial incentives such as tax credits and low interest loans for energy source technologies like solar photovoltaic, wind turbine, and storage systems. One problem is that such financial devices are, by and large, not specifically focused on the integration of these assets into resilient microgrids. Other government methods for encouraging microgrid implementation include (1) direct government grants for microgrid deployments; (2) government-authorized solicitations for microgrids (often meeting specific state policy criteria); (3) mandates and targets for distributed energy resources or carbon reduction; (4) utility regulatory reforms addressing existing barriers to microgrid deployments; (5) technology commercialization plans; and (6) approval of microgrid rate bases. With government incentives, electric utilities are increasingly turning to microgrids. Dividing the grid into a patchwork of ostensibly independent microgrid islands may enable microgrids to continue to operate during outages of the larger grid (McDonald 2019).

Notwithstanding the rush to microgrids, without protection against major threats, microgrids are not a silver bullet solution for problems associated with the larger electric power macrogrid. First, microgrids have internal vulnerabilities. Electronic sensing and control systems required to balance organic microgrid generation systems and their connected load are susceptible to cyber- and electromagnetic-caused debilitation. Secondly, microgrids complicate the operation of the larger macrogrid, or rest of grid (ROG), (see figure 1). Specifically, microgrids add an additional layer of complexity to the electric grid—increasing the vulnerability of complexity. In terms of normal problems, intermittent renewable energy sources can introduce rapid load swings to ROG that have caused instances of ROG collapse. Also, ambient power backfeed from microgrids can cause disruption and safety problems in the ROG. From a system digital control perspective, physical and logical connectivity between a microgrid and a ROG control system increases the susceptibilities of the ROG to both cyber and EMP debilitation.

We are at a watershed moment in technological history. Incorporating cyber and EMP protection into microgrid design and installations will greatly enhance grid survivability. The opposite is true if we continue to ignore cyber and EMP protection. Without organic protection, we are headed for a world of grid resilience mayhem riddled with the vulnerabilities of complexity. We ignore the cyber and EMP threats to microgrids at our own peril.

GROWING THREAT VECTOR

In addition to normal accidents associated with weather and Murphy's Law, we know our adversaries are targeting our national power grid by exploiting EMP, physical, and cyberattacks. Our growing reliance on electronic control of critical infrastructures, such as process control systems (PCS), supervisory control and data acquisition (SCADA) systems, and the larger internet of things (IoT) is adding layers of vulnerability to our personal and enterprise electronic systems and system interconnection networks. Despite our growing dependence on telecommunication networks, the internet, and the indispensable supporting electric power network, EMP protection and cyber protection are spotty at best.

The President's National Security Telecommunications Advisory Committee (NSTAC) published early concerns regarding long-term outage (LTO) of the electric power grid involving interruption of electricity for months to years over large geographic regions (Edwards et al. 2006).

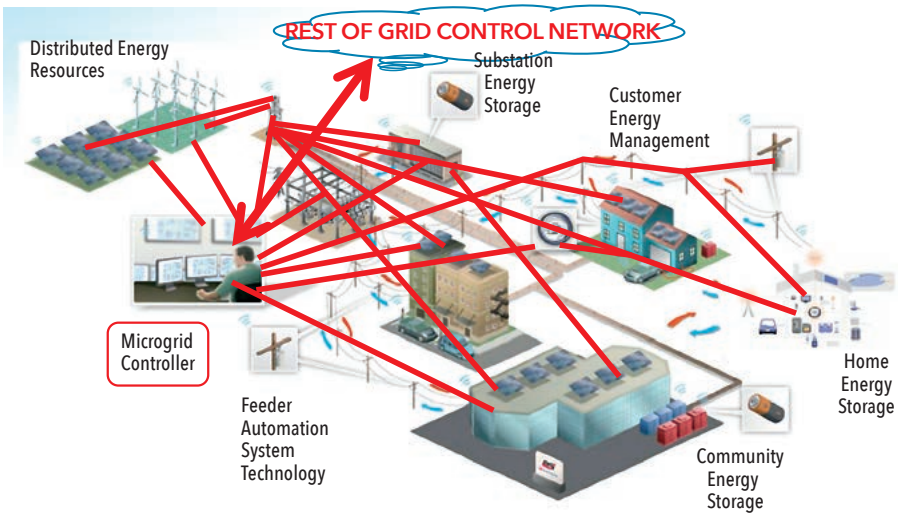


Figure 2. Notional local microgrid control network (red lines) (Institute for Local Self-Reliance. 2016b)

In a cruel irony, as society becomes increasingly reliant on uninterrupted power, the grid becomes increasingly vulnerable unless intentionally protected. The major threats to microgrids and the grid at large are highly asymmetric. These threats fall into three categories: physical, cyber, and electromagnetic.

In the physical attack domain, a small number of actors with weapons as simple as a deer rifle can shut down the North American grid for months to years. Jon Wellinghoff, then chairman of the Federal Energy Regulatory Commission (FERC), disclosed that a FERC engineering study had concluded that an attack on as few as nine transformer substations could black out the continental United States for months or years (Smith 2014). A physical attack on the Metcalf Energy Center in San Jose, US-CA nearly succeeded in depowering Silicon Valley.

Cyberattacks on grid communications and control systems occur on a continuing basis. Already inserted but unaddressed malware trojan implants could shut down large portions of grid on command. The Idaho National Laboratories' Aurora project demonstrated the ability to cause generator self-destruction using a remote control technique to open and close generator station breakers. During 2015 and 2016, Russian hackers shut down a large sector of Ukraine's power grid. And, in 2018, federal officials revealed Russians had penetrated the computers of multiple United States electric utilities gaining access privileges to digital control systems sufficient to cause power outages.

The most neglected effects on the grid are from wide-area electromagnetic effects caused by solar superstorm geomagnetic disturbances (GMDs) and nuclear EMP from high altitude nuclear bursts. Nuclear EMP engenders the highest intensity currents and voltages, with solar GMD a close second. On the threat scale, these are the ultimate common-cause catastrophes in which a single event can shut down the continental grid for long periods. The electric power grid couples the highest levels of EMP and GMD energy due to its long, elevated transmission and distribution lines. GMD effects are unavoidable: The National Oceanic and Atmospheric Administration (NOAA) projects a 10–12% annual probability of a solar superstorm GMD. While EMP probability determination is more subjective and requires Bayesian techniques, our adversaries have included EMP exploitation in their war plans and press releases. For example, North Korea has threatened to use EMP against the United States.

Because of large variations in renewable energy source output and the desire to manage energy use as loads change, microgrids come with elaborate supervisory digital monitoring and control systems. If not intentionally protected, these control systems are highly susceptible to debilitating effects from EMP and cyberattacks. Figure 2 depicts a heuristic depiction of a microgrid control network. Red lines show control connections. Each red line also constitutes a potential cyberattack point of entry or an EMP energy coupling path. Note from figure 2 that because microgrid control systems interface with monitoring and control systems for the ROG, microgrids provide attack paths into the ROG.

Use of multiple microgrids within a community, city, or region has led to the aggregation or clustering of these to take advantage of power sharing and backup

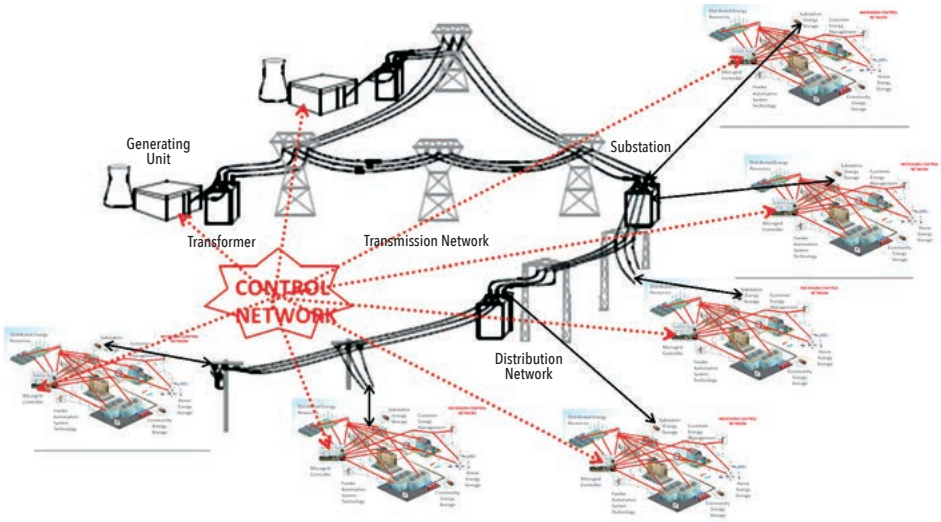


Figure 3. Multiple microgrid aggregation or cluster overlay on ROG with interconnected control networks

capabilities. Cluster control systems and power feeds are interconnected; figure 3 provides a heuristic illustration of interconnectivity. Aggregation adds additional complexity to the microgrid, and ROG control and power systems provide additional cyberattack and EMP attack vectors into the larger grid (ROG and other microgrids). Thus, the addition of unprotected microgrids can make our composite electric power system more vulnerable. Without protection, microgrid aggregation increases aggravation associated with grid failure.

PROTECTION METHODS ARE AFFORDABLE, PRACTICAL, AND BENEFIT MICROGRIDS PLUS ROG

The good news is that with designed-in protection, microgrids can be resilient against cyberattacks and EMP with the additional benefits of stabilizing and alleviating attack vectors into the grid at large. Cyber protection methods include air gaps, firewalls, and software to isolate microgrid communication and control networks from the ROG control systems and the cloud. We must devote special attention to industrial control systems (ICS) at the edges of the grid. Application of proven EMP design techniques ensures microgrid survivability. From an EMP standpoint, we can implement protection by shielding critical electronics within metal shelters, cabinets, or boxes and providing voltage or current limiters at any conducting cable penetrations. If possible, it is best to use optical fiber interconnections for all control signal lines. The small land area of microgrids and internal short line interconnects makes them virtually immune to GMD and late-time EMP (E3) threats. It is important to note that this is true only for microgrids in island mode, isolated from ROG long-lines.

We need a two-pronged protection approach. First, priority elements of the larger grid (ROG) need protection. Protection of the ROG will involve a longer-term process. In the meantime, local protection of new microgrid installations will be important to assure the resilience of local critical infrastructure services powered by microgrids.

Again, the good news is that we know how to harden. For EMP and GMD, demonstrated protection standards and guidelines exist. We can apply military and International Electrotechnical Commission (IEC) standards. For cyberattacks, existing standards apply only to the bulk power system. For microgrids, best practices are known. One important caution: industrial control system protection is different from computer network (information technology or IT) protection. Microgrids can avoid internet connections better and establish air gaps than macrogrid, but only if cyber protection is included in the microgrid design phase. Physical security benchmarks and standards include the US Department of Defense (DoD), Defense Critical Infrastructure Program (DCIP) Standards and Benchmarks. Section AP-5, (DCIP) Electric Power Standards and Benchmarks is helpful. Also, the DoD-HDBK-2000.12 H provides guidance for physical security assessments and methods.

A PLEA FOR DESIGNED-IN EMP, CYBER, AND PHYSICAL PROTECTION

As explained, the installation of unprotected microgrids harms the resilience of the existing electric grid infrastructure by increasing the vulnerability of complexity by adding layers of cyber and EMP vulnerability inherent in control systems and interconnecting data and power feed pathways. Exacerbated failure modes occur because of normal malfunctions (including mean time between failure attrition and Murphy's Law) and deliberate human acts. Microgrid protection benefits the microgrid itself and the electric power grid at large.

Protection represents a small incremental cost for systems in the design phase. The DoD experience with facility and weapon-system hardening indicates designed-in protection costs are 10 times lower than retrofit protection, namely 2–5% for built-in protection versus 20–50% for retrofit.

We are at a watershed moment in technological history where we must decide between (1) seizing the initiative for designed-in protection on microgrid installations yielding a highly resilient electricity supply, or (2) proceeding in a laissez-faire manner that increases the vulnerability of local and regional electric grids. It will be important to seize the initiative for designed-in protection. Now is the time to develop and issue design guidance and government incentives for designed-in protection engineering. ■

REFERENCES

- Baker, G., T. Popik, J. Kearns, H. Cooper, and W. Harris. 2017. "High Consequence Scenarios for North Korean Atmospheric Nuclear Tests with Policy Recommendations for the US Government." *Department of Integrated Science and Technology-Faculty Scholarship* 5. https://commons.lib.jmu.edu/cgi/viewcontent.cgi?article=1007&context=isat.
- Edwards, J. et al. 2006. "People and Processes: Current State of Telecommunications and Electric Power Interdependencies." Report, The President's National Security Telecommunications Advisory Committee (NSTAC), Telecommunications and Electric Power Interdependency Task Force (TEPITF). https://transition.fcc.gov/pshs/docs/advisory/hkip/GSpeakers060418/ACT1070.pdf.
- Institute for Local Self-Reliance. 2016a. "CPUC Microgrid Diagram." https://ilsr.org/wp-content/uploads/2016/03/CPUC-microgrid-diagram.png.
- ——. 2016b. Notional Local Microgrid Control Network." https://ilsr.org/wp-content/uploads/2016/03/CPUC-microgrid-diagram.png.

> continued on page 42

Defining Critical Communications Networks: Modelling Networks as Systems

Thomas Manley, thomas@manley.name; **Susan Ronning,** s.ronning@adcomm911.com; and **William Scheible,** wscheible@mitre.org

■ **ABSTRACT**
As a society, we have become exceedingly dependent on our communication devices and the infrastructure networks supporting them. Even short duration network outages can result in chaos within public transport systems (air traffic control of commercial flights, traffic signaling of rail networks); disrupt financial systems (electronic payments, stock market transactions); and reduce business productivity (phone and email). It can also have the potential for loss of life: field utility workers communicating remotely with dispatch controllers to de-energize and re-energize lines for repair; law enforcement field personnel communicating needs for crowd control during riots; and alerting the public about dam breaches through emergency notification systems.

This article helps explain what critical communications networks are, where these networks fit within a systems-of-systems context, and what other systems must also be resilient, redundant, and reliable to ensure communication networks can continue to operate as designed. It also introduces systems engineering principles, techniques, and approaches that we can use to aid in the design of critical wireless and wireline communications networks for normal day-to-day operations, and for the protection and recovery of those networks during service disruptions caused by man-made and natural events.

■ **KEYWORDS:** telecommunications; wireless; telephone; 9-1-1; emergency communications; critical infrastructure; PPD-21; networks; voice; data; communications impacts; critical systems design; nodes

COMMUNICATIONS NETWORKS AS ENABLING SYSTEMS

An enterprise's core business may provide: a market for exchanging stocks (financial); electricity to business and residential customers (utilities); transportation of people or things from one place to another (railways, airplanes); or law enforcement and fire-fighting services (public safety). Communications networks underpin almost every business, government agency, and non-government organization. Networks must transport an exchange of information, be it voice or data, from one location to another to enable performance of the enterprise's core functions.

A given communications network often serves several different types of users in many different capacities. For instance, private citizens typically use the same cellular phone services for text messaging that they also use to make emergency calls to request police and fire services; ambulances may use this same cellular phone service for automated vehicle location mapping to determine the closest ambulance to a casualty (figure 1). Other multiuser examples include satellite-based voice calls made

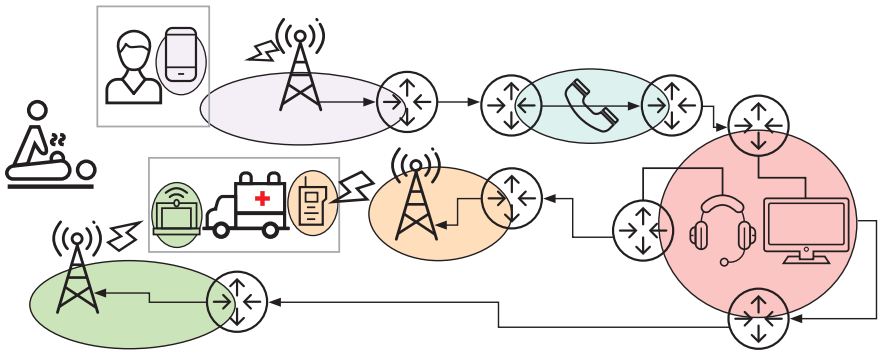


Figure 1. Emergency medical call from mobile phone service via commercial telephone system to public safety answering point to ambulance via voice radio and broadband data networks, demonstrating multibearer networks in everyday occurrence

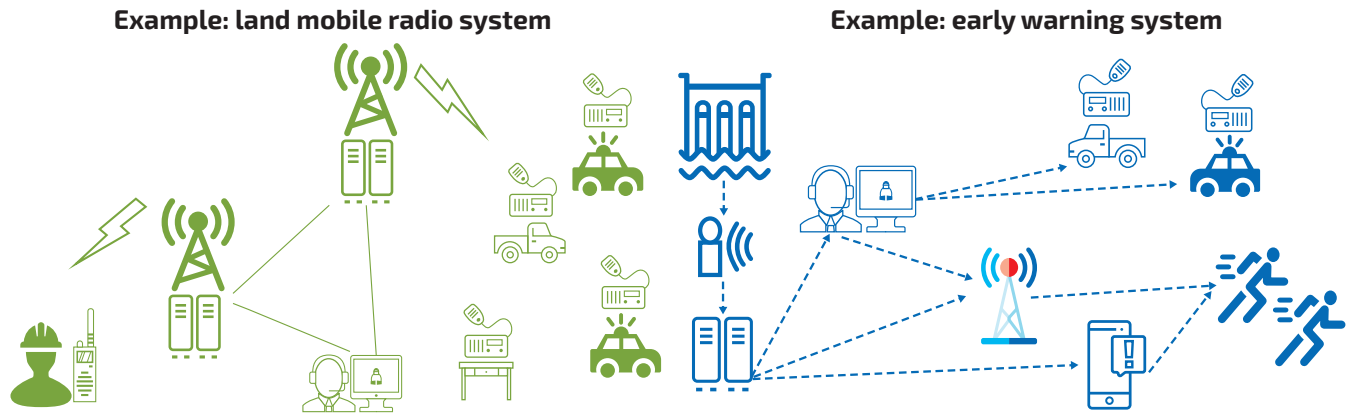


Figure 2. Two different examples of critical communications networks

from a cruise ship to the mainland, line-of-sight simplex radio transmissions between a helicopter and the ground crew guiding a pilot during landing, and a wireless access point providing data communications to multiple wireless devices in a home.

The US Department of Homeland Security's Communications Sector-Specific Plan (CSSP) (2019) states, "Since 2010, the communications sector has evolved rapidly in multiple areas, including mobile broadband, cloud computing, the Internet of Things (IoT), and software-defined networks (SDNs). Voice and data networks have continued to converge, and mobile devices, such as smartphones and tablet computers, have been widely adopted, creating enormous demand for mobile broadband communications." Although this has reduced the number of single purpose networks required, it is now more difficult to understand the criticality of the resulting networks that have replaced them.

What is a Communications Network?

A communications network may be made up of a collection of systems, integrated and interacting with one another (figure 2). The communications network system of interest may include mobile and fixed transceiver equipment. Supporting systems can include antennas and filters, primary and/or backup power, physical mounts, routers and switches, device management and alarm notification, end user interfaces, and the transport networks (or links). They can include subscriber devices like handheld cell phones and portable radios; radios installed inside vehicles, airplanes, or satellites; IoT devices; and fixed transceiver units (base stations and their antenna systems) which engineers may install inside buildings, on towers, or on satellites orbiting the earth. They can also include applications running over the network, such as email systems, video conferencing systems, and contact center systems.

All these systems must work together in concert to relay the information from one location to another. Engineers must first define, design, procure, and configure each individual system to work within their own domain, and then, when integrated with each other, support the network as a whole. And, engineers must design each–independently and together–to withstand potential failures.

APPLYING SYSTEMS ENGINEERING TO COMMUNICATIONS NETWORKS

To apply systems engineering knowledge to the design and support of communications networks, there is a need to model communications networks as systems. Yet, there is very limited guidance as to how to do this. While industries often use the terms system and network interchangeably in relation to communications networks, in practice, it can be very difficult to define system boundaries or the internal and external interfaces of communications networks as the network topology can be constantly changing. As a result, the effects of localized failures are often very difficult to predict, so performing techniques such as failure mode, effects, and criticality analysis (FMECA) can be challenging. This is increasingly the case for critical communications networks as these are often larger and more complex.

If it is possible to describe a network as a system, then we can unlock the tools in the systems engineer's toolkit to add value to both the design and support of the network. FMECA and reliability, availability, and maintainability (RAM) analysis are two such techniques that may assist engineers to assess the resiliency of a communications network qualitatively and quantitatively. Similarly, the ability to identify and label components that we may find in many places across the network, for example, switches and routers, can facilitate configuration management as well as assist in the allocation of requirements and construction of architecture descriptions. What follows is guidance on how to approach the modelling of communications networks as systems. Note that while this is focused on, and intended for, critical communications networks, it is applicable to all communications networks.

Nodes and Links

Engineers often represent communications networks graphically as a set of nodes (geographical locations where information communications technology [ICT] services are delivered) connected by links (interfaces between two or more nodes). While this approach obfuscates much of the detail of the network (for instance, it assumes a single homogeneous network where any information can potentially flow from any node to any other node), it does provide a high-level representation of the structure of the network and therefore provides a useful starting point for exploration. Note that a node can itself contain an inner network, which can be comprised of lower level nodes in much the same way a system can be comprised of subsystems. Hence nodal recursion is also possible.

Nodes can be a fixed site, such as a building or university campus. They may also consist of environmental sensors, cellular base stations, geo-stationary satellites, or automated farm gates. Nodes may also be mobile, such as vehicles that move on the ground, under the sea, in the air, or in space. They may also consist of wearable devices on people and animals, or consist of a network of unmanned autonomous vehicles (UAV) that may even include weapons in military applications.

The key is that there may be communication within nodes (intranode) and between nodes (internode) (Syed, Pong, and Hutchinson 2017). In this way, we can think of a large office housing thousands of individuals as a single node connected to other nodes via links, obfuscating the

complexity of the network within the office itself. It is in this context that they are most useful for modelling complex communications networks.

Nodal Types

We can treat each node as a distinct nodal system, with external interfaces to other nodal systems and internal interfaces between the system elements within it (see figure 3). For networks with many nodes, though (and particularly those networks with large nodes such as offices), each node would have its own unique internal design and this could quickly become difficult to manage (and support).

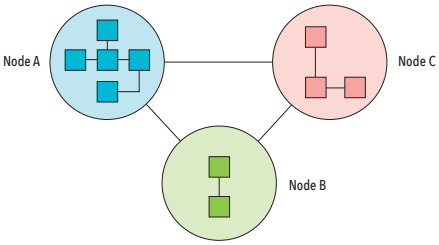


Figure 3. Example nodes showing internal and external structure with i) internode links/external interfaces and ii) intranode links/internal interfaces

The use of nodal types (where each instance of a nodal type shares a common architecture) can simplify the effort of designing and supporting each node, since this reduces the number of unique nodes and allows for the use of templates (or design patterns), as illustrated in figure 4. We can then place these patterns under configuration control to maintain consistency between each instance of each nodal type.

To create a set of nodal types, we can group nodes together in various ways. While there are many different ways to group nodes, how we group them can affect the degree of difference between nodes within a nodal type and the management effort to support them. Careful selection of the characteristics that define each nodal type is therefore important. For instance, scale is often a distinguishing characteristic, with an organization having offices configured for different office sizes based on the number of employees located there (large, medium, and small). These are candidates for nodal types. However, if the functionality (or services) that each node provides differs in more than the size (a factory may have a similar number of workers to an office, yet very different ICT needs, while a data center may have very few staff or none at all) then functionality may be a more effective characteristic to select. The following proposed principles may aid in defining a useful set of nodal types.

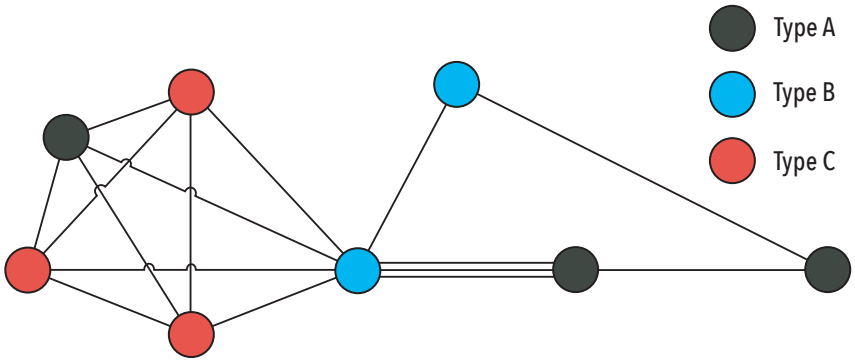


Figure 4. Node topology diagram with multiple instances of three nodal types (A, B, and C). In this case, there are three distinct links between the middle blue and black nodes.

Nodal Type Principles:

1. Functionality is more important than scale in distinguishing nodal types, that is, group nodes with common functionality into a nodal type before size;
2. Engineers should minimize the number of nodal types to reduce operational complexity and configuration management;
3. Nodal types should include sufficient granularity of services such that nodes do not provide services that are not required, such as the minimum required services;
4. Nodal type variants can be used to cater for lower level differences between nodes of the same nodal type including the modular addition (or removal) of supplementary services, for example, a manufacturer can fit the same model vehicle with manual or automatic transmission, or add roof racks.

SYSTEMS OF SYSTEMS

While systems engineering normally focus on the design of individual systems, the concept of systems of systems engineering (SOSE) was created in part to deal with the complexity arising from the existence of many independent systems interacting with each other for a common purpose, so systems engineers can usefully apply it to networks (Maier, 1998).

From the *Systems Engineering Handbook* (Walden et al. 2015, 8), systems of systems (SoS) tend to have the following characteristics which help distinguish them from ordinary systems:

- operational independence of constituent systems;
- managerial independence of constituent systems;
- geographical systems;
- emergent behavior; and
- evolutionary development processes.

The "Systems of Systems Primer" (INCOSE 2018) expands on managerial independence by positing that one of the challenges of SoS is that constituent systems "may withdraw (possibly without warning) from the SoS," implying that this is not an option available to a subsystem of an ordinary system.

We can think of communications networks as SoSs where nodes are systems that can (in theory at least) join or leave the network at will. Communications networks, however, are a special case of SoS and also tend to exhibit the following set of proposed characteristics. Additional characteristics of communications networks include:

- common purpose, that is, to facilitate communication within and between nodes;
- commonality of architecture (many nodes may be instances of the same node type and therefore share the same design);
- strong interdependence of constituent systems (certain failures within a particular node may cause other nodes to become isolated/disconnected);
- large in scale (hundreds, or even thousands of nodes); and
- a strong focus on traffic flows through a network rather than the interfaces within it.

DUAL NATURE OF SOLUTION ELEMENTS

The problem then arises when we share technology solutions between nodal types; in other words, where the engineer reuses a solution element (being simply an element of a solution) as a building block in multiple nodal type designs. How does the engineer manage these solution elements, given that they may be part of multiple nodal type designs, and changing the design for one may necessitate changing it for all other instances of it?

Another problem is that due to the deliberate logical separation of certain downstream networks, often involving encryption, different network domains may

be transported over a common wide area network (WAN). This gives rise to functional systems that engineers can overlay on top of a subset of nodes, either as:

- bearer networks (those functional systems whose main purpose is to connect nodes, for example, a WAN); or
- distributed systems (systems whose elements operate together irrespective of geographical distribution, or are at least managed as one system).

The implication is that solution elements (as building blocks of a nodal system) may simultaneously be a subsystem of a node as well as a subset of a functional system. This dual nature of a solution element is a unique property of communications networks that requires new thinking.

We demonstrate these constructs in figure 5 where section A illustrates a generic network topology of three sites (A, B, and C) that we then refine to section B through the allocation of solution elements to various bearer networks and distributed systems and the identification of nodal types (X and Y). We show the resulting simplified system block diagram in section C. Note that while there are two instances of nodal type X, only one is shown in the system block diagram.

Interestingly, nodal systems appear to meet the SoS criteria of "operational independence of the components" that Maier proposed (1998), since the network as a whole can survive the loses of some nodes; we cannot necessarily say the same for functional systems. For instance, distributed systems may be critically dependent on bearer systems. As such, we can think of nodal systems as forming SoSs, yet this may not be true for functional systems.

Links Belonging to Different Networks

Since it is possible for a node to contain multiple downstream functional systems, it is also possible for links to belong to distinct bearer networks to distinguish them from the broader network construct. A node, therefore, could connect to multiple different bearer networks using a different link for each, though the node may or may not function as a gateway between two bearer networks. That is, there may still be isolation between bearer networks, meaning that data cannot flow between them. This is often the case with commercial or military vehicles that can use multiple networks operating in different parts of the electromagnetic spectrum, for example, high frequency (HF) for beyond line of sight (BLOS), very high frequency (VHF) or ultra-high frequency (UHF) for line of sight (LOS), and satellite communication (SATCOM). While all bearer networks may be available for use at any time (assuming they are not out of range), they may not all be used at the same time. For instance, we might only use voice communications when required, since it could be difficult to listen to multiple voice networks at the same time. Geographical location and the bearer networks that the other party/parties (that the user needs to talk to) have available to them (civilian emergency services networks) may determine the selection of which bearer network to use (and when).

The implication of different links on the same node belonging to different bearer networks is that a physical node may actually be the colocation of multiple virtual nodes (where there is little or no connectivity between the virtual nodes). This is evident in figure 6 where the red and blue nodes (A) are physical nodes that

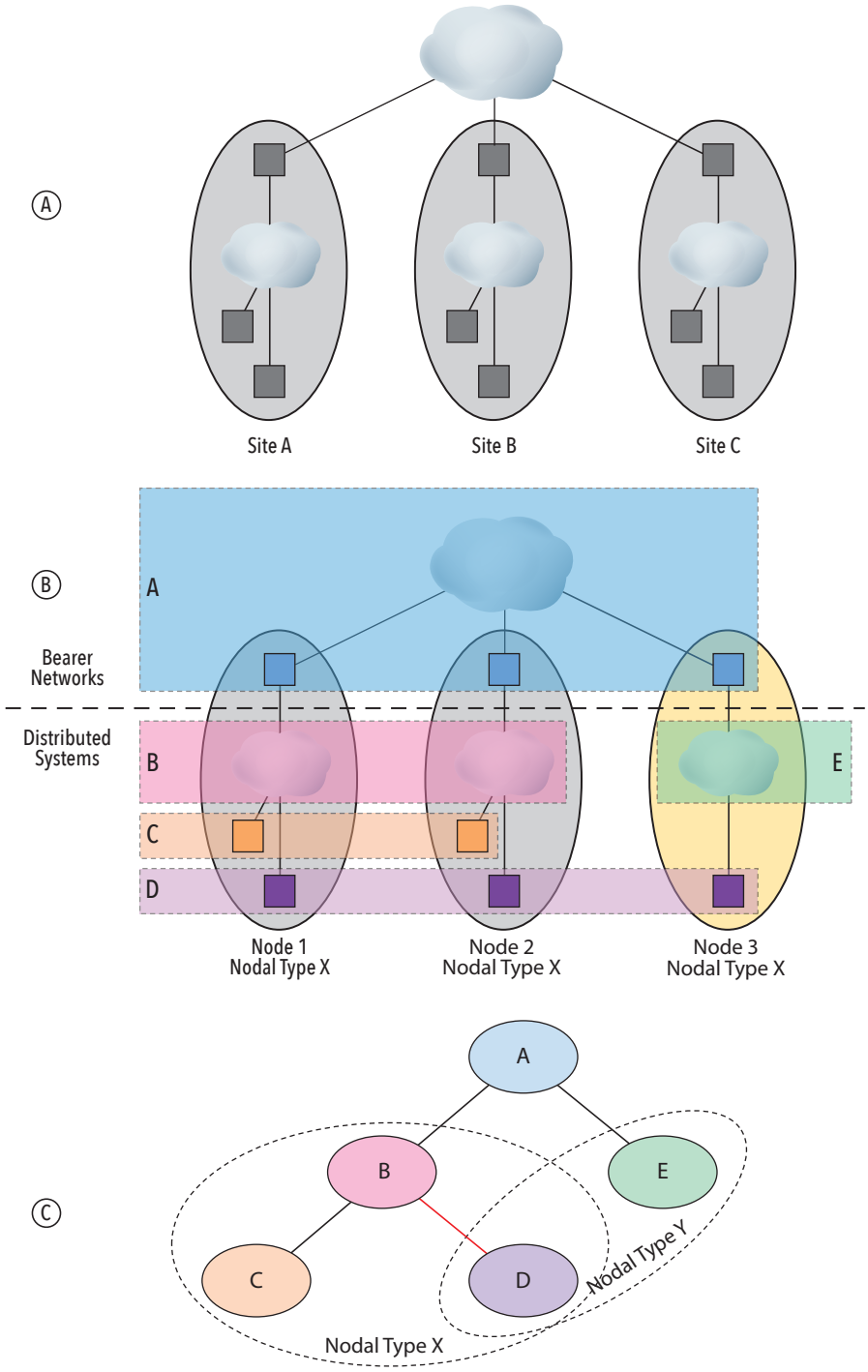


Figure 5. A) a generic network topology of three sites (A, B, and C); B) the same topology allocating components to bearer networks and distributed systems and distinguishing nodal types; and C) the resulting simplified systems block diagram

consist of four and three virtual nodes respectively (B). Because the virtual nodes do not interconnect, there are effectively four distinct networks (green, yellow, purple, and orange), and each link belongs to only one of these bearer networks (C). Traffic cannot flow between these networks without some form of interconnection, for example, a gateway.

Matrix Approach

We can treat bearer networks, nodes, and functional systems as systems each in their own right (figure 7), and they can coexist as independent conceptual constructs. However, they each have different frames of reference, and therefore we should take care when considering interfaces between them. For instance, nodes interface externally to bearer networks (and through them other nodes) whilst building blocks (solution elements of functional systems) form a part of a node. Building blocks have interfaces to other building blocks within the same node and may also have logical interfaces across nodes forming a common functional system, for example, a wireless LAN controller (WLC) on one node may control the wireless access points (WAP) at a different node.

CRITICAL OR NOT?

Today's systems engineers are well advised to consider the impact of critical

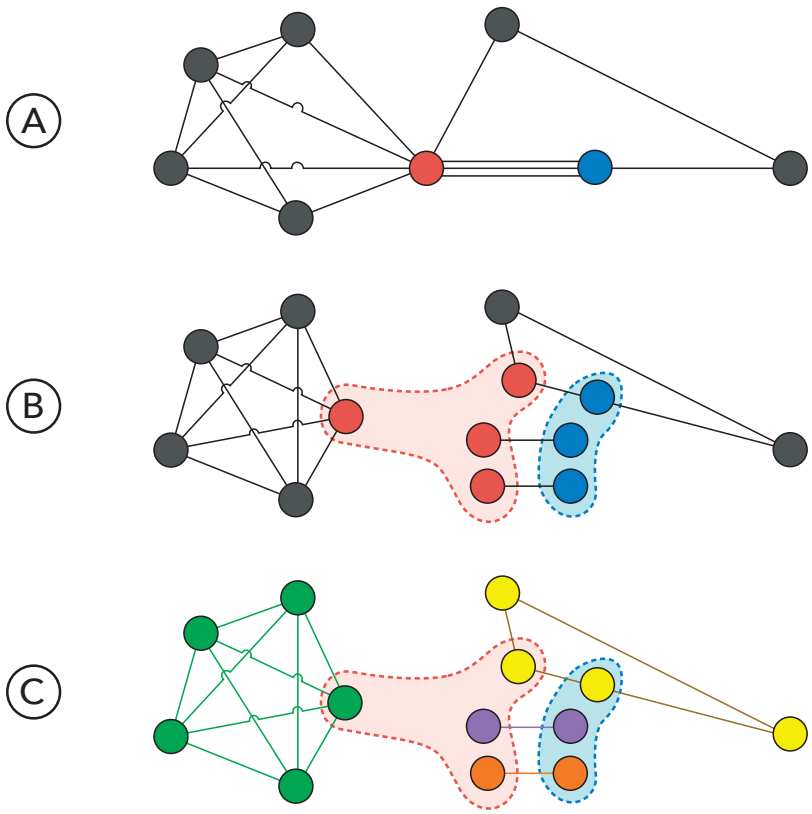


Figure 6. A) is a typical nodal topology diagram that assumes full homogeneity. B) illustrates how the red and blue nodes may be comprised of separate virtual nodes, each with their own discontinuous links. C) illustrates how the set of nodes may represent a set of discontinuous networks (yellow, green, purple, and orange)

Functional Systems (functionaliryt-based)	Nodal Systems (location-based)					
	Type A	Type B	Type C	Type D	Type E	Representative Network
Bearer Network X	√	√	√	X	√	B A A C
Bearer Network Y	X	X	X	√	√	D D D
Distributed System ∝	√	√	√	√	√	DC 2A B C 3A
Distributed System β	√	X	√	X	√	DC 2A C
Distributed System γ	√	X	X	√	√	DC 2A 3D

Figure 7. Nodal systems (location-based) versus functional systems (functionality-based). While the columns (nodal systems) are nodal types comprised of (or built from) elements from the rows, we can also consider these rows, when aggregated together, to be a functional system, either a bearer network (clouds) or a distributed system (boxes); representative network diagrams are shown on the right, where type E represents a data center (DC).

communications and the supporting communications infrastructure in their analysis, design, and support of systems.

The US Department of Homeland Security (2019) identifies "16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Presidential Policy Directive 21 specifically calls out the communications sector as critical because it provides an "enabling function" across all critical infrastructure sectors (PPD 2013).

Similarly, the Australian Government's definition of critical infrastructure (2015) is, "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security."

We define critical communications networks, with respect to this paper, to be those communications networks that:

- are themselves considered critical infrastructure in their own right (for example, networks used for public safety alerts or by the military); or that
- other critical infrastructure systems depend on for communications services (for example, air traffic control, New York Stock Exchange, utilities, and transportation systems); as well as those networks that
- are relied upon during emergencies, crises, or disasters.

Further, systems that rely on communications networks may be comprised of elements that several different organizations own and manage, preventing the underlying network from having a single owner. For instance, the Australian tsunami warning system relies on constituent elements provided by the Australian Bureau of Meteorology, Geoscience Australia, and the Department of Home Affairs as well as multiple different carriers serving each agency (Australian Government 2020). This greatly increases the complexity of these multi-organization networks.

A myriad of international and domestic vendors and companies provide today's communications infrastructure. While a communications company can promise to deliver a service, they often have little control over the infrastructures that they use (leased antennas or towers, or virtual channels on a shared fiber link). As several recent natural disasters have shown, the entire communications infrastructure of a country, state, or area can be damaged to the extent that no existing communications services are available for days or weeks.

Levels of Criticality

In the current era, the importance and criticality of having stable and always available communications is unquestioned. The importance of having and maintaining a communications infrastructure however, is seldom presented or addressed as a standalone consideration. In most government and business considerations, the criticality of communications and the need to maintain and protect the infrastructure that delivers communications services is left to the individual critical infrastructure sectors.

The US Department of Homeland Security uses four factors to determine criticality: fatalities, economic loss, mass evacuation length, and degradation of national security (Clarke, Seager, and Chester 2018). The highest level of criticality is the possibility of loss of life. A lack of communications would not directly take a life, but its impact based on the use case might. Examples may include: the inability to perform train signaling functions within a network of high-speed railways; the inability to effectively manage power distribution due to paralyzing impacts from storms or man-made events; the loss of radar managing aircraft within a Class A airspace; and the inability to communicate to field personnel during national emergencies. All such and similar events could remove or seriously degrade the efforts to coordinate responses and awareness to save lives.

What Design Criteria Should Be Incorporated Based on Level of Criticality?

The level of criticality of these networks is subject to interpretation. The Community Emergency Response Team (CERT) motto is "doing the greatest good for the greatest number of people" (Marion County, US, OR 2019). In the case of critical communications networks, there are no standard levels of design criteria, but there are design principles to support an overarching goal that any potential failure should do the least amount of damage to the least number of users, nodes, or systems. Failures occur. Wherever possible, we should identify and avoid single points of failure. The actual levels of criticality are likely to be sector (or context) specific, and therefore we only have access to general guidance.

Best practice is to evaluate nodes based on their impact with respect to the effect of failures on a localized versus system-wide basis. Data centers tend to be more critical than core/hub sites (those sites that provide connectivity to other sites); and core/hub sites tend to be more critical than edge/spur sites (those sites that do not). Edge/spur sites tend to be the least critical in the overall network architecture although they may be critical to the users in that region. In areas where communications require higher levels of availability, we may consider multiple layers of communications technology. For example, cellular services may overlap the same geographic region as a public safety land mobile radio system which line-of-sight satellite services may also serve. Or, we may consider redundant power and transport systems for network operation centers.

While each node may have its own unique criticality level, it may be simpler to assign criticality levels to nodal types. Similarly, each functional system may have its own individual criticality level since they each serve different purposes and users. Understanding who these users are and their needs is critical to developing a useful set of criticality levels. From this set of data, dependencies are easily identifiable, and we can therefore mitigate failure modes. For instance, if a nodal type with a high criticality level has a single connection to a bearer network, we may provide a second connection to remove the single point of failure. Similarly, we would ideally design a distributed system with a high criticality level with a high degree of redundancy.

Clarke, Seager, and Chester (2018) refer to the concept of minimum essential infrastructure as well as distinguishing urgent and important infrastructure. In the event of a disaster (the third category of critical communications networks, figure 2), the minimum essential infrastructure should remain operational, or be restored as quickly as possible, and we could classify this type of critical infrastructure as urgent. Outside of a disaster, though, we may require a different (perhaps expanded) set of critical infrastructure(s) to remain operational nonstop, and we could classify this type of critical infrastructure as important. On that basis, it is probable that bearer networks are more likely to be urgent, whilst some distributed systems and many bearer networks are likely to be important, and as such, the model may assist in assigning different criticality levels to different parts of a critical communications network.

SUMMARY

As described, the need, use, and understanding of critical communications is key to successful and on-going systems engineering efforts due to its impact as an enabling system to so many other critical sector systems. Acknowledging and addressing critical communications should

be part of any systems engineering effort, especially during the early understanding, requirements, and architecture definition and analysis phases.

Modelling networks as systems can be difficult because each node in the network is invariably different from all other nodes, and yet each node is comprised of common elements that together may form a functional system extending across many nodes. Without the concept of nodal and functional systems, it is difficult to efficiently identify system boundaries and interfaces, and then to place these under configuration control as configuration items.

When determining levels of criticality for critical communications networks, assigning levels of criticality separately to each nodal and functional system will assist in identifying which specific solution elements are most critical overall. This will also help provide context to the effect of failure modes and enable resiliency (including redundancy and recovery) that systems engineers need to appropriately design in to minimize the impact of failures on society.

We hope that this guidance will assist in modelling complex communications networks as systems, and in so doing, enable the application of traditional systems engineering techniques to critical communications networks. ■

ACKNOWLEDGEMENT

The authors contributed this article under the auspices of INCOSE's Telecommunications Working Group of which they are members.

REFERENCES

- Australian Government. 2015. "Critical Infrastructure Resilience Strategy: Policy Statement." https://cicentre.gov.au/document/P50S023.
- Australian Government, Bureau of Meteorology. 2020. "Australian Tsunami Warning System" http://www.bom.gov.au/tsunami/about/atws.shtml.
- Clarke, S., T. Seager, and M. Chester. 2018. "A Capabilities Approach to the Prioritization of Critical Infrastructure." *Environment Systems and Decisions*. doi:10.1007/s10669-018-9691-8.
- INCOSE. 2018. "Systems of Systems Primer." https://www.incose.org/products-and-publications/sos-primer.
- Maier, M. 1998. "Architecting Principles for Systems-of-Systems." *Systems Engineering* 1(4): 267-284. doi:10.1002/(SICI)1520-6858.
- Marion County, US, OR. 2019. "Community Emergency Response Team." https://www.co.marion.or.us/PW/Emergency-Management/CCC/Pages/cert.aspx.
- PPD (Presidential Policy Directive). 2013. PPD-21. *Directive of Critical Infrastructure Security and Resilience*. Washington, US-DC: PPD, Administration of Barack Obama.
- Syed, M., P. Pong and B. Hutchinson. 2017. "Battlespace communications network-of-networks interface modelling," 2017 Annual IEEE International Systems Conference (SysCon) 1-6. doi:10.1109/SYSCON.2017.7934706.
- US Department of Homeland Security, Cybersecurity and Ifrastructure Security Agency. 2019. "Critical Infrastructure Sectors." https://www.cisa.gov/critical-infrastructure-sectors.
- Walden, D., G. Roedler, K. Forsberg, R. Hamelin, and T. Shortell. 2015. "Systems Engineering Overview." In *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. 4th ed., 5-24. San Diego, US-CA: Wiley.

Approved for Public Release; Distribution Unlimited Case 20-0893

ABOUT THE AUTHORS

Mr. Thomas Manley is a principal consultant with Downer Defence (Braddon, AU) working in the Land Network Integration Centre (LNIC) and Land Command, Control, Communication, and Computers (C4) Program within Army Headquarters (AHQ). He is a foundation member of the SESA Telecommunications Working Group that became an INCOSE Working Group. He has 20 years' experience in telecommunications, primarily for Defence and Australian Taxation Office (ATO), working for Optus, Telstra, Boeing, and Thales.

Ms. Susan Ronning is owner and principal engineer of ADCOMM Engineering LLC (Woodinville, US-WA). She has over 20 years' experience in the telecommunications industry with a focus on critical wireless voice and data communications networks for public and private agencies in the public safety, emergency management, utility, and transportation markets. Ms. Ronning is co-chair of the INCOSE Telecommunications Working Group.

William Scheible is a principal network systems and distributed systems (Sys&Dist) engineer with the MITRE Corporation (McLean, US-VA). He has over 35 years of both commercial and government experience in all facets of network design, network operations, and systems architecture working with both wired and wireless infrastructures. He began his career with Tymshare/Tymnet in Cupertino, US-CA developing packet switching networks, followed by engagements with several financial, consulting, and networking companies before joining MITRE in 2002. He holds ESEP and CISSP certifications and is a member of the INCOSE Telecommunications Working Group. The author has provided affiliation with The MITRE Corporation for identification purposes only, and does not intended to conveyor imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.

Baker continued from page 35

- McDonald, J. 2019. "Microgrid Series." T&D World.
- Smith, R. 2014. "US Risks National Blackout from Small-Scale Attack." *The Wall Street Journal*, 12 March.
- Ton, D. T., and M. A. Smith. 2012. "The US Department of Energy's Microgrid Initiative." The Electricity Journal 25 (8): 84-94. http://dx.doi.org/10.1016/j.tej.2012.09.013.
- Wood, E. 2019. "Microgrid Policy: What Really Needs to Be Done?" *Microgrid Knowledge*. https://microgridknowledge.com/microgrid-policy-really-needs-done/.

ABOUT THE AUTHOR

George H. Baker is a professor emeritus, James Madison University and director, Foundation for Resilient Societies.

Emergency Systems and Power Outage Restoration Due to Infrastructure Damage from Major Floods and Disasters

Romney B. Duffey, duffeyrb@gmail.com

■ **ABSTRACT**

I examine extreme events where one major consequence is damage to infrastructure causing failures and loss of electrical power to vital systems, and restoration may take several days to weeks. We need to know how long it will take to restore power and design robust emergency backup that is especially important for major population centers, critical facilities, and essential industrial equipment. This coupled systems engineering problem involves the restoration of the initial outages depending on the damage caused and the reliability of emergency power and backup systems. I first review my prior work using extensive data for the prediction of power restoration probability and timing using publicly available data for severe and unexpected events. The events cover a wide spectrum of hurricanes, wildfires, ice storms, floods, cyclones, and tsunamis for multiple power distribution systems and countries, where attempts to avoid prolonged failure and ensure restoration deploy emergency crews, procedures, and extensive recovery equipment. Significant infrastructure damage, access difficulty, and societal disruption delays restoration. The resulting universal correlations show that emergency restoration probability and timing are independent of event type, depending on the degree of difficulty as restoration occurs as fast as humanly possible.

Systems design and recovery processes should all learn from these previous disasters. Because of the potential for significant delays and extended power outages, critical facilities and commercial enterprises deploy emergency or backup power systems. I provide a detailed analysis of the probability of emergency system restoration and determine the needed response time and reliability requirements. The analysis then derives integral emergency system failure rates by comparing the (a) emergency power restoration data for the Fukushima Daiichi Nuclear Power Station events that resulted from unprecedented flooding due to an unexpected tsunami from a major earthquake, and with (b) the analogous extended loss of pumping power due to the massive flooding of New Orleans, US-LA by Hurricane Katrina. This new analysis quantifies the chance of restoration using systems engineering and emergency measures and replaces the frequently used qualitative system resilience terminology for coping with severe events.

INTRODUCTION: POWER SYSTEM DAMAGE AND RESTORATION DEGREE OF DIFFICULTY

My proposition is that a common basis exists for restoring critical infrastructure system failures and for determining the overall emergency and backup systems reliability. I first review the latest results and predictions of the power restoration probability and timing using publicly available data for severe and unexpected events. For nuclear, medical, databank, chemical processing, and other industrial facilities, there are emergency procedures and coping strategies for power and cooling recovery following a loss-of-power event (Adibi and Milanicz 1999; Chow, Taylor, and Chow 1996; NRC 2016). National bodies continue to study and issue guidance, procedures, and recommendations for massive events (DHS 2017; NAS 2019). My recent paper established a fundamental theory for predicting the timing of power restoration for major disasters, storms, or disruptions (Duffey 2019a). This earlier paper demonstrated the common dynamic trends in outage restoration after damage and widespread loss of electrical power due to the dominant influence of the degree of difficulty.

Both natural and man-made disasters can cause massive damage sufficient to lose power systems for several weeks over very large urban or statewide areas, exhaust the capabilities of mutual aid and emergency response plans, and affect many millions, but still not meet the arbitrary US President's National Infrastructure Advisory Council's (NIAC) criteria of

50 million outages lasting months to qualify as a "catastrophic power outage" of national interest (2018). If we consider for a moment a major unexpected event such as Hurricane Katrina's impact on New Orleans, US-LA and the outage duration, we can only imagine the consequences of such a defined catastrophe which is beyond modern experience. In addition, these events can cripple many dependent systems: "Since communications systems rely on electricity, any incident that causes long-term power outages will create a challenging environment for telecommunications and public messaging" (DHS 2017).

The present data, analysis, and results focus on what we learn from what actually happens in real, not hypothetical, power outage events. The physics of learning, technical methodology, statistical theory, and extensive event databases fully include all human operational actions and decisions made during emergency restoration for the extremely adverse conditions prevalent in severe events and disasters. This method quantifies the chance of restoration using systems engineering and design measures and replaces the qualitative system resilience and agility and adaptability terminology for coping with damage and power outages that severe events cause (see Zio 2016 for a summary). The massive report on Hurricane Katrina highlights the need for an integrated approach to emergency systems engineering and planning: "While the pumping stations have not been considered as an integral part of the hurricane protection system, they should have been" (USACE 2006, vol. V).

The extensive power restoration data in Table 1 includes many severe events including storms, ice storms, fires, hurricanes, cyclones, and floods causing outages lasting from 24 to 800 hours over a wide range of urban, regional, and international scales (Duffey 2019a). In all cases, the affected power companies, emergency management organizations, and government agencies deployed vast numbers (sometimes many thousands) of staff, repair crews, equipment, and procedures to address power recovery, evacuate people, and repair damage. Essentially, restoration only proceeds as fast as humanly possible, limited by damage, access, and social disruption issues caused by flooding, storms, fires, wind, ice, and snow, and as the US Department of Homeland Security (DHS) states, "the restoration of the grid is generally the same across all hazards" (2018). The probability of power system non-recovery is, P(NR) = n/N0, the ratio of the outages remaining, n, at any time to the total (initial or maximum) number, N0, being the complement of the usual reliability, R(t) = 1 – P(NR).

We can also include the probability, P(EF), in any extreme event that any backup power systems (generators, batteries, and redundant supplies, to name a few) do not function in a timely manner. The overall system risk (including loss of power) expression quantifies the chance of restoration using emergency response and backup restoration measures and replaces the qualitative system resilience terminology for coping with severe emergency events. The complement is the conventional Reliability, R(t) = 1 – P(EF), which I will show is the important quantitative measure. Importantly, P(EF) is also equivalent to the probability for operators failing to restore power for nuclear plants using backup generators (Ma et al. 2018, equation 9). We now quantify both probabilities, P(NR) and P(ES), for power non-recovery and continuing backup or emergency system failure, respectively, following severe events.

Table 1. Power outage data summary

Event key: A=Alaska earthquake, B=Baseline, SS=Sandy, E=Storm Emma, F=Florence, G=Cyclone Gita, H=Harvey, HQ=Quebec ice storm, I=Irma, Ma=Matthew, MI=Michael; N=Nate, NH=New Hampshire ice storm, O=Ophelia, Q=Storm Quinn, R=Storm Riley; S=Snowstorm Grayson, T=Storm Toby, W=wildfires

City and/or region	Data source (event)	Span h	Maximum N_0
Queens, NY	NYPSC/ConEd (B)	88	25,000
New York, NY	ConEd (SS)	336	1,345,000
Florida	FDO (Ma)	240	10,234,174
Houston, TX	CPE (H)	800	109,244
Corpus Christi	AEP (H)	800	201,635
Florida South	FPL (I)	400	1,810,290
Florida NW	Duke–FL (I)	400	1,610,280
Tampa. FL	TECO (I)	400	330,103
Florida Keys	FKEPC/KES (I)	400	60,00
Florida Gulf	Gulf Duke (MI)	320	396,700
Alabama	APC–SCS (N)	60	156,000
N & S Carolina	Duke Energy (F)	190	542,780
Eire, EU	ESB (O)	240	385,000
Eire, EU	ESB (E)	60	127,000
NE, USA	Eversource (S)	50	25,796
NE, USA	Eversource (R)	90	220,378
NE, USA	Eversource (Q)	120	209,706
New Hampshire	NHPS (NH)	312	432,600
New Jersey	Jersey CP & L (T)	37	31,656
Quebec, Canada	HydroQuebec (HQ)	286	1,393,000
Taranaki, NZ	Powerco (G)	160	26,000
Napa, CA	PGE (W)	450	359,000
Ventura, CA	SCE (W)	450	8,400
Anchorage, AK	Chugach MP & L (A)	28	21,713
Totals		5,801	20,061,455

PROBABILITY OF NON-RECOVERY OF INITIAL POWER SYSTEM FAILURE

Each massive outage event is a learning experience, and "plans are based on the best information available, but no disaster follows the plan" (NAIC 2018). The probability of any individual outage being restored is random, and when we observe the probability as outcomes, we follow the well-known and established laws of statistical physics (Greiner, Neise, and Stocker 1995; Jaynes 2003; Duffey and Saull 2008). Therefore, simple exponential functions correlate the data for electric power non-restoration probability, P(NR), for all outage events well, and the degree of difficulty as characterized by the extent of infrastructure damage, social disruption, and concomitant access issues depend on and group the data (Duffey 2019).

The time scale and restoration rate difference between short timescale normal and longer extreme event restoration is illustrated in figure 1 using the data from Table 1 (Duffey 2019a). The data clearly show the two extreme groupings or categories of normal and extreme events restoration, with the normal group from figure 2 appearing on the left. Evidently, events with more extreme damage and/or access difficulty clearly have much slower restoration and longer durations, by at least a factor of 10 to 20, as my earlier results show. As opposed to traditional plots of the numbers of outages versus time for different events (see DHS 2018 for an example), the present formulation normalizes all the events and demonstrates it is not the number of outages that effects recovery rates.

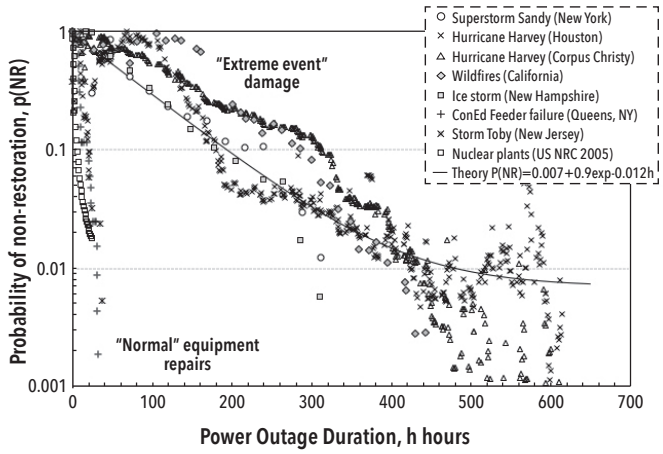


Figure 1. Power system outage probability for more "extreme" events (fires, storms, hurricanes and ice storms) compared to "normal" cases, and to the theoretical prediction and correlation from (Duffey, 2019a)

Clearly, the short-term normal restoration data (shown in figure 1) are not applicable to more severe events with additional damage, access, and social disruption issues, resulting in longer outage and restoration timeframes. The overall outage data for all types of major events and disasters follow the same fundamental trends despite their disparate origins and locations. This trend is completely independent of severe event type (hurricanes, ice storms, flooding, earthquakes, cyclones, and fires), but the rate systematically depends on the degree of difficulty or damage and is proportional to the number of remaining outages.

I originally found a typical generalized best fit (Duffey 2019a) to severe events as, with t measured in hours,

$$PNR = Pm + P0 * e - \beta h \approx 0.007 + e - 0.014h \quad (1a)$$

I have also made this fit incorporating more recently acquired data (Duffey 2019b), and with a coefficient of determination of $R^2 = 0.77$. The theoretically based fits exhibit only minor rate and probability variations for multiple independent severe events.

This analysis implies more difficulty in restoration of a failed system due to continued access, damage, and safety concerns (Duffey 2019a). The degree of difficulty parameter, β, and the minimum achievable minimum, P_m, reflects this key issue of the extent of damage.

The impact of damage to the power system and to infrastructure (bridges, roads, buildings, dams…) is evident from examining the power restoration data for the massive Hurricane Irma, devastating Florida from the 12th to about the 26th of September, 2017. It is evident that it took longer to restore power in the most heavily flooded counties (Naples/Collier) than in others (Duffey 2019a, figure 4). Figure 2 compares the Irma power non-restoration data to the other storms analyzed in figure 1 (Harvey, Florence, and Superstorm Sandy). After the initial power outage maximum, the data all have the same exponential shape, with Irma overlaying both Florence and Harvey for 200 hours. But the Naples-Collier region of more extensive flooding and damage has more difficult restoration, so the resulting probability of non-restoration, P(NR), can be up to about a factor of 2 higher during these first 200 hours.

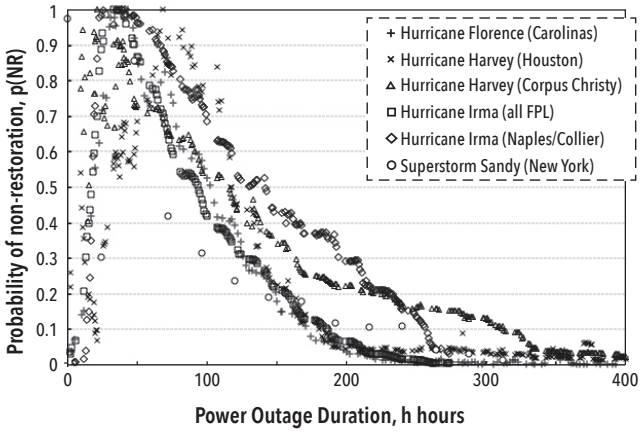


Figure 2. Influence of hurricane damage and flooding on the probability of power outage nonrestoration

CATEGORIES FOR THE DIFFICULTY OF RESTORING POWER AFTER SEVERE EVENTS AND CYBERATTACKS

The general exponential expression also fits outage non-restoration data for many other severe or rare events, from large wildfires to ice storms. The theory and the data demonstrate that it is the degree of damage to the infrastructure (in this case the power distribution system) that determines the rate of recovery (Duffey 2019a). For system design and recovery planning purposes, I define the categories as (see figure 3):

- Type 0: ordinary, which we may classify as everyday outage restorations that are relatively simple, with simpler equipment replacement, line repairs, and/or reconnection due to an effectively instantaneous outage.

- Type 1: normal baseline, β ~ 0.2, when outage numbers quickly peak due to finite but relatively limited additional infrastructure damage. Repairs are still fairly straightforward, and all outages are restored over timescales of 20 to about 200 hours.

- Type 2: delayed, β ~ 0.1 – 0.02, progressively reaching peak outages in 20 plus hours, as extensive but repairable damage causes lingering repair timescales of 200-300 hours before almost all outages are restored.

- Type 3: extended, β ~ 0.01, with perhaps 50 or more hours before outage numbers peak due to continued damage and significant loss of critical infrastructure; restoration repair timescales last for 300-500 hours or more.

- Type 4: extraordinary, β ~ 0.001 or less, for a cataclysmic event with the electric distribution system being essentially destroyed and not immediately repairable (Haiti, Costa Rica, and NAIC catastrophic outages).

I show the data for Superstorm Sandy (open circles) purely as an example, because it represents a long-term outage as specifically defined by FEMA (NAIC 2018, 32). The exponential form and trends do not change with overall duration.

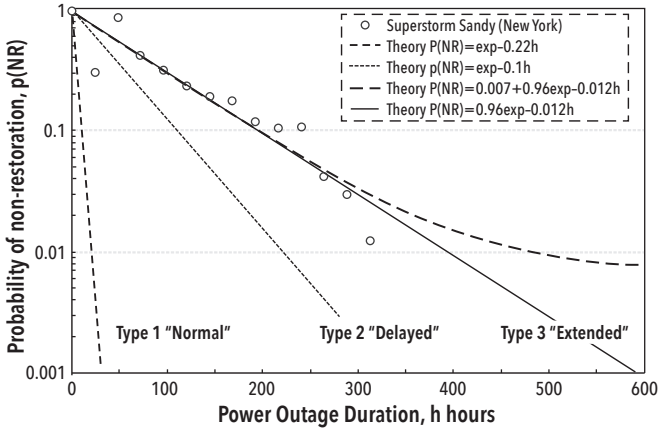


Figure 3. Simplified categories of restoration difficulty and timescales

These categories allow for a more refined emergency response and more realistic restoration planning. I further generalize the results using the following argument, presenting an extraordinary and useful fact about the damage and subsequent restoration of power systems in severe events.

This observed variation in the degree of difficulty ($0.01 < \beta < 0.2$) implies an average repair rate spread of 20 simply due to the damage extent. The irreparable fraction data range (the tail of the distribution) indicates that the chance of the damaged remaining unrestored is small but finite, $0.003 < P_m < 0.01$, even after several hundred hours. As an example, for every million outages at first, despite achieving over 99% restoration after 600 hours, several thousand could still have no power.

The DHS (2018) makes the reasonable assumption that the restoration curve for power outages or virtual damage due to cyberattacks is similar to that for known severe events, like hurricanes and ice storms. By this analogy, the DHS postulates cyberattacks causing power outages to simply increase the restoration timescales and numbers, which we would interpret as reflecting an increased degree of difficulty with β reducing further. The publicly available data (Lee, Assante, and Conway 2016; DHS 2017) shows a cyberattack caused power outages by disconnecting networks and operator control before being restored after several hours. We would now classify this event as a Type 1 normal outage, with a P(NR) range of cyber degree of difficulty, $0.1 < \beta < 0.22$, because there was no concomitant or additional access, physical damage, or societal disruption affecting recovery of the power system infrastructure and associated computing/communication networks.

Both Hurricane Harvey in Houston, US-TX, and Hurricane Florence in the US Carolinas produced rare record (historic) flooding and power outages for about 540,000 and 109,000 customers respectively, including critical medical and industrial facilities. Despite being completely different storms in entirely different locations, the dynamic probabilities of power non-restoration literally overlay, as shown in figure 4. The two events have similar peak timing (50-100 hours) and decline exponentially at the same rates over similar timeframes (500 hours). In closer detail, also evident is the human influence of the 24-hour daily cycle for the repair crews causing steps or mini-plateaus during the recovery; and is later evident as fluctuations in the later tail beyond 400 hours.

These residual outages only decreasing to the usually quoted or pre-storm 99.9% supply reliability after about 600 hours (25 days, or nearly a month) shows the overall full restoration timescale. There is some uncertainty to this end point or finishing line, as often agencies declare a small number of outages unrepairable and then excluded them from the reported numbers.

It is not correct to use the average restoration timescale or outage number as a measure of restoration effectiveness or system resilience, as both the average number of outages and the overall duration depend on the two key parameters, the characteristic e-folding rate, β, and the residual number of outages (Duffey 2019a).

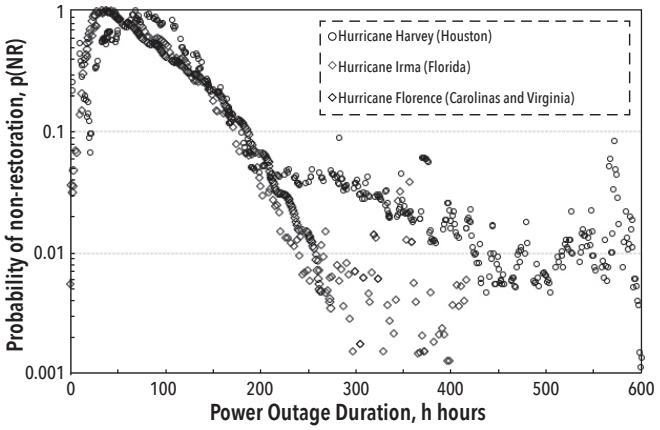


Figure 4. Similarity of the overall power restoration probability trends for three different hurricanes (Irma, Harvey and Florence) despite causing record flooding and power outages at entirely different locations

This similarity proves that the probability of outage restoration and timing due to record flooding and severe storm damage is not specific to event, location, power grid, or utility. This is true for regions with the most restoration difficulty, even if they have utilized suggested hardening of the distribution system (NAIC 2018). The overall shape is indeed quite universal (Duffey 2019; DHS 2018) according to all the known data for repairable power systems, so what happens to cause power outages at one location is similar to others, the detailed differences in the tail depending on the access difficulty. We can literally use outage recovery rates and dynamic probabilities interchangeably from one such severe event with others.

I now show that, for example in a major hurricane, the probability of flooding extent correlates with the non-restoration probability.

CHALLENGING STANDARD METHODS FOR ESTIMATING RECORD FLOOD RISK

Experts worldwide use many key references on the topic of the statistical and computer models for the frequency and magnitudes of flooding due to storms and stream flows, and on systematic changes in precipitation patterns (as a sample, see Bonnin et al.

2006; Perica et al. 2013; England et al. 2018; DeGaetana 2009; Wing et al. 2018; Shukla and Trivedi 2010; Sandoval, and Raynal-Villaseñor 2008). The best statistical fits all have essentially very similar coefficients-of-determination or goodness-of-fit parameters (for an example, see Alam et al. 2018; Langat et al. 2019); the only justification for their use is they can fit the data, even though the adjustable fitting parameters can number three, four, or more, but are not physically distinguishable. The fits are location, regionally different and specific, and require regional skewness estimators (for examples, see the excellent summaries by Bonnin et al. 2006; Perica et al. 2013; Franz and Sorooshian 2002). As Bonnin et al. (2006) also importantly state: "The current practice of precipitation (and river height and flow) frequency analysis makes the implicit assumption that past is prologue for the future. . . Furthermore, if the climate changes in the future, there is no guarantee that the characteristics extracted are suitable for representing climate during the future lifecycle of projects being designed." De Gaetano (2009) and Jorissen, Kraaij, and Tromp (2016) also attribute this fact as due to globally and locally changing climate and precipitation patterns. For coastal regions, there are similar statistical approaches and national concerns for predicting flood and storm surges (for examples, see Jorissen, Kraaij, and Tromp 2016; Matczak et al. 2016; Emanuel 2017; USACE 2006; COMRISK 2006; UK Environment Agency 2009).

As officially and clearly stated: "As a rule of thumb, statistical methods should not be used to estimate recurrence intervals in years that are more than twice the number of years of available homogeneous data" (Wright 2007).

Hence, in summary, all this extensive and detailed work shows us:

a) Distributions fitted to prior data for frequency or number of flood events are usually arbitrary and multi-parameter, and therefore only strictly applicable within the data range and may not properly include the tail of rare events;

b) The assumption that the future is just like the past historical (prior) data does not account for any systematic shifts or significant changes in weather patterns, precipitation, or climate, which have been and are observed;

c) Numerical flood depth data are generally not available for intervals longer than 50 to 100 years, and/or are incomplete, and relevant paleo/geologic data are scarce;

d) The probability of precipitation analyses and methods are orientated and tuned to daily, weekly, and multiyear weather forecasting–not to predicting one-off rare or extreme events (due to unexpected hurricanes, major storms, typhoons).

I highlight the contrast is between these rare and sudden events and the flooding due to periodic tidal and seasonal causes. In the famous case of Venice, IT (Città di Venezia 2019), repetitive seasonal and lunar tidal variations directly caused the flooding, not one-off sudden or rare events like storms, hurricanes, or tsunamis. However, as I show later, these periodic flooding events still exhibit the key similarity of randomness of occurrence which influences prediction.

We need a new approach because it is not appropriate for predicting future extreme/rare or record flood events to use statistical fits and distributions to past normal or large prior precipitation or stream flow frequency data, or for estimating the return period (or frequency) for a future record flood of a given height (magnitude). The present paper treats record floods as random outcomes or events, subject to statistical error state analysis, and takes a different approach of sampling the future to estimate the probability of a new record flood.

RARE FLOOD EVENT OCCURRENCE: RISK PREDICTION

We can simply derive the usual risk formula from knowing the probability of exceeding any flood, $p(>M_F)$, in a year called the annual exceedance probability (AEP). The probability of not having a flood in any year is, $(1-p(>M_F))$, and of not occurring y-years over, $(1-p(M_F))^y$. The probability, p_y, of having one larger than M_F in any number of years, y, is then the complement (England et al. 2018):

$$py = 1-(1-p>MF)\,y$$

Clearly, if $p(>M_F) << 1$, as for a rare event, then trivially, $p_y \sim yp(>M_F)$, simply increasing monotonically with years passing. This is a frequency estimate, since years (calendar time) are only a convenient human risk exposure measure, which natural disasters do not follow. Scientists have also used the terminology 1% AEP to distinguish and avoid using the 1-in-a-hundred-year flood terminology (see www.chiefscientist.qld.gov.au/publications/understanding-floods/chances-of-a-flood).

The key point is that the rare outcomes, namely extreme and/or record floods, do not follow standard statistical distributions, or occur at any known variance, multiple standard deviation, or moment from some average, median, or central value. As noted in "Guidelines for Determining Flood Flow Frequency" (England et al. 2018, 21): "In general, a time series of annual peak-flow estimates may be considered to be a random sample of independent, identically distributed random variables;" and we simply extend this concept to describe the occurrence of record (extraordinary) floods.

Although we learn from the more frequent outcomes, the probability or risk of a rare new record event is inherently different from what we have already experienced, so we need a new approach. As shown elsewhere (Duffey and Saull 2008), the result is embodied in formulae where a simple exponential form gives the probability distribution. For any sample of floods of magnitude, MF, in any risk exposure, prior observational or experience interval, the probability of random flood events, P_F, is (Duffey and Saull 2008; Duffey 2019a, 2019b, 2020):

$$PFMF = pm + 1 - pme - yMF$$

But scientists have already shown this form applies to millions of extreme event data and naturally includes the lowest attainable or rare event probability. For future risk, the correct time interval should be the interval of expected or probable future risk exposure.

To demonstrate how this expression applies to floods, I found the volumetric flow rate data, Q_F, for $N_0 = 115$ floods of the Tokomairiro River in New Zealand for 1961-2002 (Mohsson 2008). The river regularly threatens and has flooded the City of Milton in 2006, 2007, and 2010 (Goldsmith and Brass 2012), with local flash floods in 2017 while the government is obviously not meeting a national 50-year return period flood standard for dwellings. As is conventional, I compared the flood count, n_F, against multi-parameter generalized extreme value-type distributions, so I transcribed the flood number data from the original graph (Mohlsson 2008, figure 3). Taking the magnitude of the flood risk as equivalent to the flow, Q_F, figure 1 shows that simple exponentials fit the data well, at least based on the coefficient of determination. (Note the usual goodness of fit parameters (R^2, Fstat, moments) are not the best or most sensitive measures for fitting a few tail data points), for Q_F in m^3/s, for the total count, N = 115,

$$PFMF = 0.79e - 0.075QF \quad \text{with } R^2 = 0.973$$

$$PFMF = 0.0023 + 0.82e - 0.081QF \quad \text{with } R^2 = 0.995$$

According to TableCurve2D, of the more than 3,300 fits listed to the data, the Weibull, generalized extreme value (GEV), and Pearson VII equation types often used in stream flow analysis have $R^2 \sim 0.998$ by using four rather than three adjustable parameters. Not only do these simple exponential fits in figure 1 also align more smoothly and better than the three GEV types shown in Mohsson's figure 3, but more importantly can still capture the right tail minimum of the physical distribution caused by the rarer record floods.

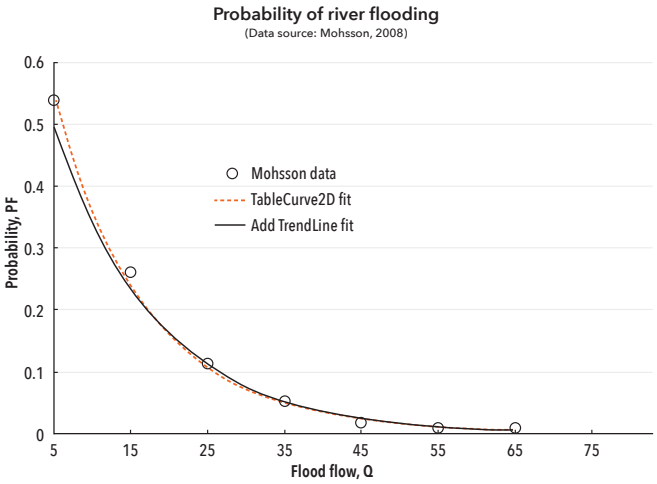


Figure 5. Probability of flood flows for a river and the theoretically based fits

The vast majority of normal data, not the few rare records at the tail, heavily influence the usual statistical goodness-of-fit methods and measures we traditionally adopt, so we therefore need a different approach.

Using a Bayesian estimate of the (unknown) probability of exceedance is (likely) a more correct probability method. This estimate is based on knowing the uncertainties and duration span of the historical record itself, or what scientists often call the prior information. We can predict the outcome probability of new record floods occurring among non-record floods in a sample of some possible total by using the classic hypergeometric sampling distribution function (see Jaynes 2003, 52-55, 68-69).

Revisiting the Tokomairiro River case discussed (see Mohsson 2008), there were 115 floods observed already, so the probability of the next flood equaling or exceeding the prior record flood of $Q = 65$ is $P_F\,(1, 1, 1, N) = 0.008695$. This result confirms the assumption of randomness as it is precisely the LaPlace-Bayes-Jaynes uniform prior value, $P_F = 1/N = 1/115$, but some 40% more than PF $(Q > 65) = 0.0062$ derived from the fitted equation.

Another typical and traditional example is in one of the US Federal Emergency Management Agency (FEMA) Academic Emergency Management and Related Courses, "Floodplain Management" (Wright 2007, figure 4.1), showing the standard probability of flowrate (discharge) Q, versus the probability, $P_F\,(> Q)$, for the Big Sandy River. Because the Pearson fitting line is extrapolated beyond the database, all we can really say about the record flow magnitude, Q_F, is that it will be greater than the last record, or more than about 28,000 cubic feet per second (cfs). Considering only the important right tail caused by three rare record floods having an average probability of $P_F\,(Q_F > 18000) = 0.025$, we compared: (a) the hypergeometric estimates; with (b) the plotted FEMA weighted Pearson Type III curve; and (c) a weighted TableCurve2D fitted exponential given by, with $R^2 = 0.997$. The comparisons in figure 6 illustrate that the real issue is fitting the three open-circle extreme points at the right tail of the distribution, not just the bulk of the black-dot data forming the peak probability (traced by the two lines). The three different estimates (a-c) have an average probability $p_F\,(Q_F > 18000) \sim 0.03$ for the three record points, a difference of 30%.

Similar case examples are from the extensive analyses of multiple distribution fits of river flows (Asquith, Kiang, and Cohn 2017, Figures 8 and 9) that I have reanalyzed elsewhere (Duffey 2020). The simple hypergeometric function is the most general sampling result but requires both the number of outcomes, nF and N, and non-outcomes, m and M, in a known or postulated sample of prior or future data points or risk interval. But there is also no advantage in endlessly debating or statistically examining which arbitrary equation is the best fit to the overall data distribution if it is only relevant to normal conditions. Rather, we should direct the efforts to determining the uncertainty in making rare record predictions. So, we need to examine more real record cases and rare event limits to gain more predictive insights, and therefore, we next consider three recent record widespread flooding examples.

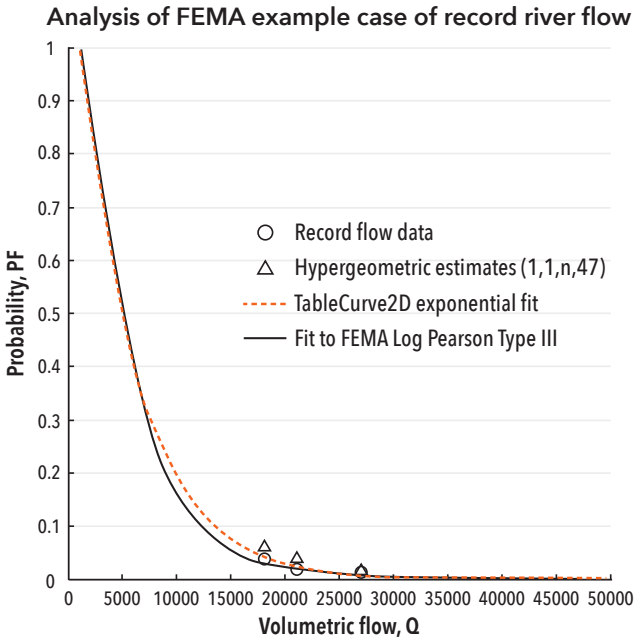


Figure 6. Illustration of alternative estimates for the probabilities for the FEMA (2019) flood risk course standard example

PREDICTED PROBABILITY OF A RECORD FLOOD

For the following Hurricane Florence and Harvey events, no one predicted the magnitude of the concomitant record flooding which significantly damaged the power system. Hurricane Florence (also Category 4) came ashore in the US North and South Carolinas and degraded to a tropical storm, but, like Harvey, stalled over land, continuing to drop torrential rain. The result was widespread flooding of many rivers, some with historically new record levels. As stated on the US National Weather Service website: "Florence analysis confirms extreme 3-day rainfall amounts exceeded 0.1% probability event expected in given year or was a 'once-in-1000-year' event."

The excellent online US Geological Survey/National Weather Service system has over 100 gauge records distributed in the region impacted by Florence, that show the whole gamut of some gauge stations with non-flood levels, some indicating floods and others having record floods. A typical gauge example (of the gauge locations with new record floods, in the spirit of this note, I chose this record history at random from among those that had a prior

NWS distribution and a listing of historic floods) for the Little River showed a new record flood where the prior historic record was for 1929-2016 (87 years). So, on a purely Bayesian approach, the new record was indeed almost the one-in-a-hundred-years flood. We would not expect such a record flood more often, except in that interval there had been eight floods above a minor flood of 18 feet, with three above a major flood of 30 feet in 2016 alone. We can derive the probability of (randomly) observing one, n_F =1, new Little River record flood in the future given the 63 non-records in the past from the hypergeometric probability P_F (1, 8, 63, N + M). Evidently, the future risk does indeed depend on the past propensity for record flooding.

Hurricane Harvey (Category 4) made landfall at Corpus Christi, Texas and then stalled after landfall over Houston, Texas, causing the worst rainstorm in US history. The precipitation rate was 10 inches (254 mm) per day causing massive concomitant local flash flooding of rivers, creeks, and bayous in Houston that entirely swamped the surrounding suburban areas and the city. I examined the data and found under prediction of flooding frequency and flood height in Houston, using the actual local online Harris County Flood Warning System (FWS). The startling observation is the factor of 10 underestimation of the frequency of occurrence for a flood depth expected and known to exceed the bank heights for the same bayous and creeks.

As a total contrast, I also compare with the flooding of Venice, IT, which has been an almost expected occurrence due to high tides, and hence provides baseline data for normal flooding due to known but still unpredictable causes. The flooding of historic Venice is an instructive counter example, having entirely different origins from that due to a sudden major storm or overflowing river. In this case, the need is to predict the probability of a new record to inform the design and operation of flood control barriers. The acqua alta data are both available and fascinating (Città di Venezia 2019), and scientists have ascribed floods to the tides coupled to variations in atmospheric pressure and winds, plus the systematic subsidence of the Venetian Lagoon (for an example, see Mel and Lionello 2014). Being tidal in nature, the peak flooding generally lasts for about three hours.

The floods are quasi-repetitive and have been extensively modeled using geographic and statistical methods (Mel and Lionello 2014), but we do not know precisely when the necessary combination of flood circumstances will occur, except for being more frequent in November. We can substantiate the random nature of the flood levels using the data for 52 years (1966-2018) in which there was a total, N = 5986, measurement of flood levels greater than 80 cm listed in 10 cm increments (or bins), n_F, up to the biggest (record) of 190 cm (Città di Venezia 2019). As shown in figure 7, the listed flood level frequency distribution, λ (M_F) = n_F / 52 per year, follows almost exactly the symmetric Gaussian or normal distribution about an average value, *MF*, with R^2 = 0.994 and for M_F > 80cm,

$$\lambda MF > 80 = 0.0293 + 0.691 - 0.0293e - 0.5MF - 127\ 2/10.33$$

Note the implied tail rate value of λm = 0.0293 per year (one in 34 years) and the mean flood level is. Since the data follow a normal distribution, this confirms the hypothesis that the flood levels are statistically random occurrences.

The probability analysis of these same 1966-2016 data gives a different perspective. figure 8 shows the probability, *PFMF=nFN*, of a flood at any level, M_F, and compared to both using hypergeometric sampling and the exponential best fit values from TableCurve2D, with R^2 = 0.9998. We can see that the hypergeometric result is exact, whereas the best exponential statistical fit again deviates slightly at the tail of lowest probabilities for the rare events.

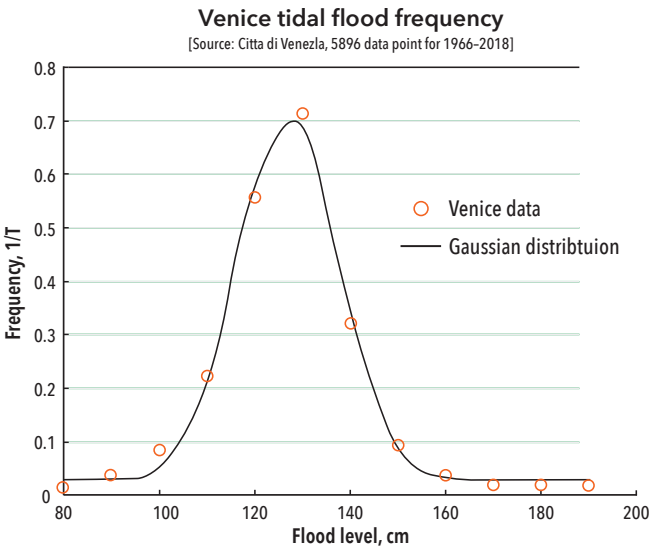


Figure 7. Normal distribution of flood heights in Venice

Naturally, the uncertainty for this rare tail, or record event, is large because of the few data points and the upper 95% confidence limit at M_F = 190cm is, P_F ~ 0.02, according to TableCurve2D, or about one in 50 floods.

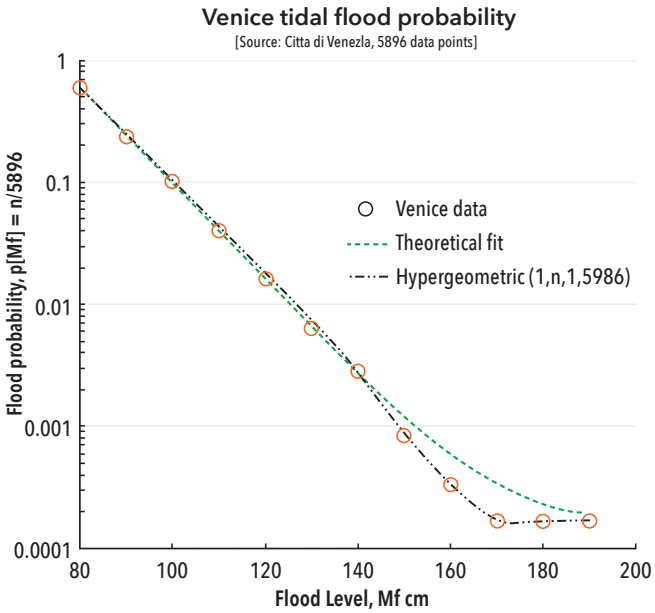


Figure 8. Probability of flood levels for Venice and theoretical fits

We may examine the effect of changing the threshold for exceeding a flood of any given height. For the new Venice Experimental Electromechanical Module, or MOdulo Sperimentale Elettromeccanico (MOSE) engineered flood prevention systems, according to the present data and allowing for a systematic future rise in the mean lagoon flood level to 167 cm, the probability is 0.029 of exceeding the MOSE flood prevention design limit of 220 cm, since they designed this new barrier to handle floods up to 3 meters (9.8 feet). The difference between the normal versus hypergeometric risk estimates is one possible measure of the uncertainty in the prediction of having a new record.

To illustrate the overall trends, figure 9 shows the flood probability estimates exceeding differing flood thresholds for

two stations in Houston, US-TX during Hurricane Harvey; one location on the US Arkansas River for the latest river flooding in 2019 following heavy rains; and comparison with the prior and quasi-repetitive Venice data.

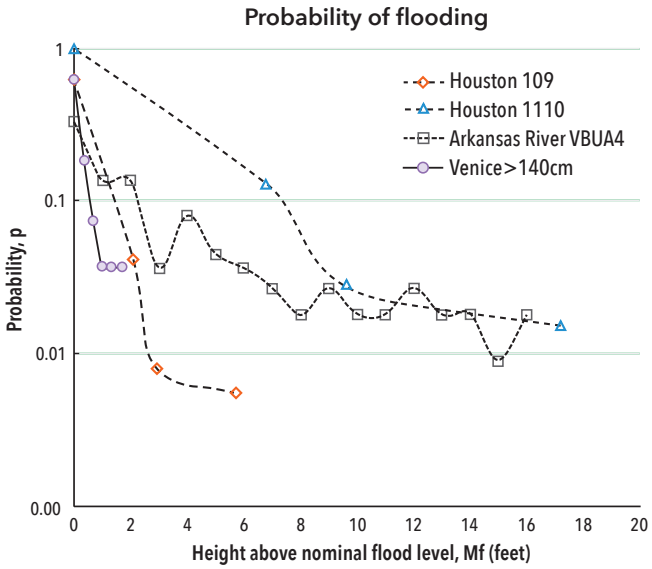


Figure 9. Typical trends for the probability of record flooding for differing locations and causes

THE SYSTEMS LINK OF POWER OUTAGE RESTORATION AND FLOODING EXTENT

I now couple the probability of record flooding to power outage onset and emergency recovery using engineered backup systems.

Most storms cause both flooding and power outages, and it is evident that power outages and flooding extent are related, but not instantaneously linked. Some part of the power system may even be above flood level or not affected by rising water, and there will be some delay before water depths affect the electric distribution, circuit connections, substations, facilities, and infrastructure. The data show that power outages (as a measure of damage) typically peak in 50-100 hours after extreme storm onset. For Venice, the degree of damage is clearly related to the percentage of the city flooded, and the past data (Città di Venezia 2019) shows a linear correlation with flood height, with $R^2 = 0.939$.

For other floods, the extensive US Geological Survey network of flood gauge readings under the surveillance of the US National Weather Service during Hurricane Florence were available on the National Weather Service website for specific locations https://water.weather.gov/ahps2/hydrograph.php?wfo=lwx&gage=abpv2). As an indirect indication of flooding extent, we define the fraction or probability of river gauges showing flooding as given by, P(g) = g/G, where g is the number of gauges showing flooding out of the total, G. Figure 4 shows the relation between this probability of flooding, P_F, and power outage non-restoration, P(NR), for storm Florence. The flooding peak occurred after some 70 hours, some 30 hours after the peak in power outages, reaching about a 30% chance before declining. Flooding persisted as drainage and recovery took longer, and some 70% of power system restoration occurred after the flooding peaked at $h = h_0$, presumably as the region progressively restored its defenses.

One plausible assumption is that the probability of power non-restoration due to flooding, P(F*), after the peak, h > h0, is conditionally dependent on and/or directly proportional to the probability of gauge flooding. For Hurricane Florence data, the

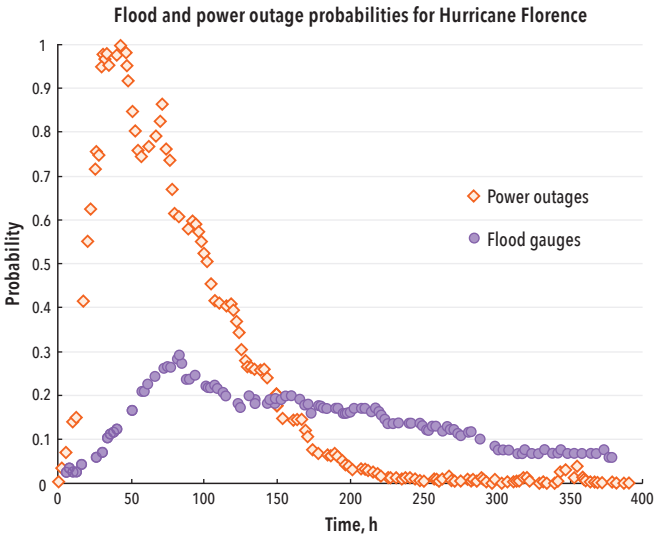


Figure 10. The relation of gauge flooding to power system outages during Hurricane Florence

best fit to the data is with an $R^2 = 0.94$,

$$PF* > 0.25e - 0.022h - h0$$

This implies of course that the difficulties the flooding caused directly resulted in a maximum of some 25% of the persistent outages. Lacking other evidence or alternative, I assumed this relation to be generally applicable to any power system susceptible to flooding. The parameter values, , are dependent on the specific factors of flood zone geography, topography, hydrology, power system design, and unique gauge locations and distribution.

I also expect that hardening of the electric distribution system against damage due to rare events should alter the peak probability, P_0*. This result agrees with the damage data from Florida Power and Light that hardening reduces the downed pole count, decreasing P_0, whereas the overall restoration rate constant, β, remained largely unaffected (Duffey 2019a), being essentially the same for Hurricane Irma as for Florence.

PROBABILITY OF EXTENDED EMERGENCY SYSTEM FAILURE AND EXTENDED POWER LOSS

I now apply the analysis to any emergency restoration of any failed critical system and quantify the chance and timescale for restoration using backup systems, emergency actions, and response measures, including black start recovery. It is important to note that the present methodology uses actual event data that fully includes all human actions and decisions, estimating: (a) the probability of restoration of a failed system; (b) the availability and reliability of alternate and backup sources; and (c) the timing and effectiveness of necessary recovery actions by humans and/or emergency crews. This methodology provides explicit and illuminating analytical solutions that we can compare against data.

Multiple engineered backup systems are available to restore power which can include batteries, diesel generators, guaranteed uninterruptible systems, alternate portable power, or black start standby or reserve systems. Consider the simple case of failures due to flooding, where workers can operate backup generators and emergency pumping systems, but these rely on hard-wired or emergency generators or batteries for motive electric power. As stated, "An availability of 90% is a reasonable figure to use for modeling future system responses assuming the stations are not

rendered inoperative due to being flooded or abandoned. This percentage has been often exceeded during hurricanes which have struck South Florida's Water Management District which is similar in size and complexity to New Orleans' pumping system" (USACE 2006, vol. VI, 47). So, a key question is how often is "often exceeded," and what is the actual reliability of the backup pumping systems in a real event when they can be inundated and stopped by record flooding, as happened due to a tsunami at the Fukushima Daiichi Nuclear Power Station in Japan, and during Hurricane Katrina in New Orleans.

The basic method, as I explain in detail in another paper (Duffey 2019b), combines the time-dependent non-restoration probability of the failed critical system, P(NR), with the dependent rate of failure to successfully deploy or actuate any or all emergency or backup systems, dP(S)/dt. Following conventional reliability analysis, I assume the probability density or rate for any emergency or backup system not successfully deployed or activated to be exponentially dependent on the overall engineered systems average or overall failure rate, λ.

Noting that $P_m << 1$, and can be neglected, I show the probability of extended failure elsewhere to be (Duffey 2019b),

$$PEF = 0tP * e - \beta t \quad \lambda\, e - \lambda t \quad dt = P * \lambda\beta + \lambda \quad 1 - e - \beta + \lambda\ t$$

The conventional reliability or chance of restoration is the complement, R(t) = 1– P(EF), which I derived as the quantitative dynamic measure of the emergency response resilience. The important failure rate ratio, $\Psi = \lambda / (\beta + \lambda)$, and the key characteristic time, or e-folding timescale, $t^* = 1 / (\beta + \lambda)$. The role of the ratio of the key failure rate parameters is now evident, with recovery timing depending on which failure rate dominates. We can generalize this result for deploying any number of independent redundant and/or diverse backup systems with differing failure rates.

The critical timing, t*, determines if an emergency system is effective or not in reducing the probability of extended loss, as $PEFt \to \infty \to \psi$. So, we need to design and determine the effectiveness of the emergency systems for limiting damage, restoring the infrastructure, and managing consequences with respect to this critical timing.

As a worked example of how to estimate the needed failure rate for critical engineered systems, the data for outage restoration following offsite power loss (In nuclear reactor risk analyses, these event sequences are traditionally termed station blackout following loss of onsite and/or offsite power (LOSP/LOOP)) for multiple US nuclear plants (Eide et al. 2005) is in figure 5. We can consider these restoration events normal or Type 1 with β ~ 0.22 without additional major damage or difficulty, as in minor ice storms, localized fires, and urban outages such as the Queens, US-NY blackout (Duffey 2018, 2019).

The probability of extended failure of the emergency diesel generators to restore power, $P(ES)_{DGR}$, Ma et al. (2018) calculated at nine hourly intervals after the onset of station blackout (SBO). Shown in figure 5, the best fit average failure rate line through the tabulated points, with $R^2 = 0.987$, is,

$$PESDGR = 0.8e - 0.087h$$

This result implies an average integral emergency diesel generator failure rate of $\lambda_{DGR} \sim 0.09$ per hour for these normal loss of power events without significant additional damage or disruption. Using this rate, the long-term probability of extended outage is $P(ES) \sim \Psi = \lambda/(\beta + \lambda) = 0.09/(0.22 + 0.09) \sim 0.29$, or nearly 30%. We must also verify and check the method and predictions against actual data for restoration in more severe events (β ~ 0.01) where multiple backup systems exist and failed.

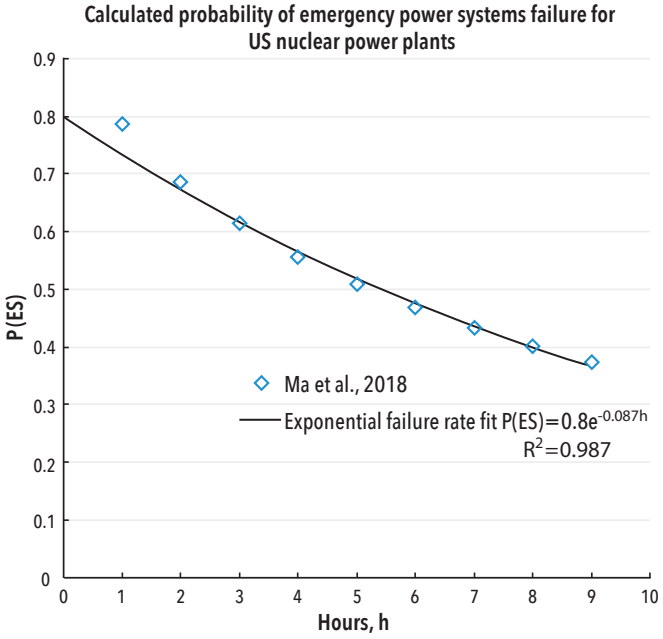


Figure 11. Reliability curve fitted to US nuclear plant emergency diesel generator failure probabilities as calculated by Ma et al (2018) during short-term (Type 1) loss of power

COMPARISONS OF THE HURRICANE KATRINA AND FUKUSHIMA NUCLEAR DISASTERS

I illustrate the detailed application of the methodology by comparing and contrasting two parallel and well-known Type 3 disaster cases of extended long outage duration of national importance and major societal impact. Besides sharing the common features of engineered emergency backup power and pumping systems failing to operate, in both cases system capability was not restored in enough time to manage or control the occurrence of major damage due to the loss of onsite and offsite power (LOSP/LOOP). The evolution of the events and integral systems data fully include all emergency responses, human actions, procedural guidance, and improvised management decisions with highly difficult and demanding conditions.

The first real-life example is the inundation of New Orleans by Hurricane Katrina in 2005, causing extensive record flooding and infrastructure damage (USACE 2006). As the US Government Accountability Office stated (2018): "Hurricane Katrina became the single largest, most destructive natural disaster in our nation's history causing over 1,800 deaths and an estimated $108 billion in damage."

By exemplifying the failure of emergency systems to successfully deploy and operate, Katrina demonstrates the high degree of difficulty in managing the consequences of a major disaster causing damage and LOSP/LOOP for critical systems. The US Army Corps of Engineers' (USACE) extensive reports (2006) show the common causes of emergency system failures were the overwhelming of the flood prevention and pumping systems, including by overtopping of levees and barriers. In fact, "The system's performance was compromised by the incompleteness of the system, the inconsistency in levels of protection, and the lack of redundancy" (USACE 2006, vol. 1). Workers distributed several hundred flood prevention pumps in various locations but many became inoperable, themselves failing due to flooding, power loss, backflows, and/or forced evacuation.

For Hurricane Katrina, we can determine the integrated systems failure rate, λ, of the engineered flood prevention systems

and the backup emergency pumps to operate. I analyzed the emergency pump outage/operability information reported daily for 28 August-21 September 2005, for the $N_p = 297$ total flood pumps located in four local regions (USACE 2006, vol. VI, Figures 12, 16, 19, and 22). I converted the published operational numbers of pumps available running, out of service, or having no data to the calculated dynamic probability of successful overall emergency pump system operation, $P(ES)_t$. As figure 6 shows, (cf figure 5), fitting these dynamic operating data, with t measured in hours, h, for the Katrina event started,

$$PESt = 0.8e - 0.003h$$

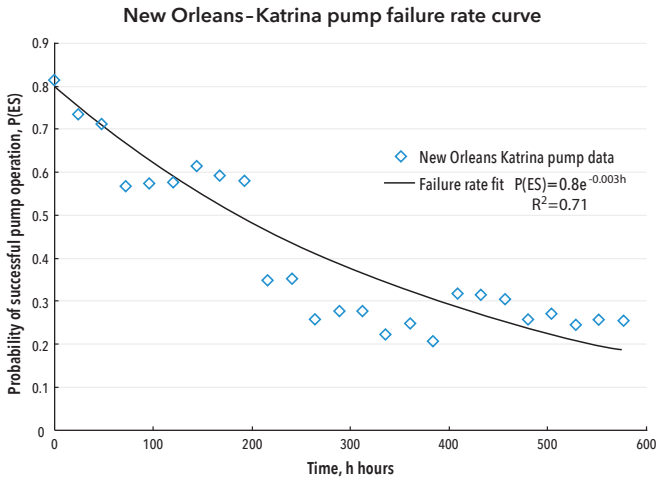


Figure 12. Reliability curve fitted to data for the emergency flood pump failures in New Orleans in the long term (Type 3) following Hurricane Katrina

Hence, for these diverse flood prevention and emergency backup pumping systems, the implied integral time-averaged failure rate is $\lambda \sim 0.003$ per hour. At the start of Katrina, at $h = 0$ hours, there is an initial operating probability of $P(ES) \sim 0.8$, or approximately 80%, which initial fraction is identical to that for the normal nuclear plant events, and only slightly lower than the USACE (2006) stated availability expectation of 90%. This high value only exists at the beginning, not throughout the event, progressively decreasing (to 20-30%) over several hundred hours as the developing damage, flooding extent, and restoration access issues worsen.

We know that the data show $\beta \sim 0.01$ per hour for humans to restore power systems as fast as possible following severe flooding, fire, hurricanes, and ice storms which cause damage and access problems, being independent of the initiating event type (see figure 1).

Taking these restoration, β, and emergency system failure, λ, rate values as typical for any severe event, the critical time, $t* = 1/(\beta + \lambda) = 1/(0.01 + 0.003) \sim 77$ hours, dominated by the restoration difficulty; while at long times, $PEFt \rightarrow \infty \rightarrow \psi = 0.0030.013 \sim 0.23$, or a 23% chance of extended systems failure or non-recovery even with ample time for emergency restoration. Hence, for major events, we should expect power and pumping outage durations lasting at least several days, even with multiple backup systems available either on- or off-site.

The second real-life example, the unprecedented nuclear plant damage caused by the Tōhoku earthquake and the resulting record tsunami, confirms this expectation. For the nine nuclear reactors at the Fukushima Daiichi Nuclear Power Station, the full reports (TEPCO 2012; ASME 2012) show the common

Table 2. Probability of extended power loss for the Fukushima nuclear plants

Fukushima Units	Power on (h)	Where	Order	P(EF) DD9	P(EF) DD11
Daiini 1, 3, 4	59	RHR	1	0.67	0.72
Daiichi 1	309	MCR	5	0.11	0.27
Daiichi 2	367	MCR-TB	6		0.18
Daiichi 3	271	Main bus	4	0.22	0.36
Daiichi 4	270	Main board	3	0.44	0.55
Daiichi 5	248	Power center	2	0.55	0.64
Daiichi 6	271	Power source	4	0.22	0.36

causes of engineered system failures were power line damage and unexpected overtopping of sea walls and flood barriers, resulting in extended loss of power, failure of emergency cooling systems, and damage to backup systems and pumps. Attempts to restore power and cooling of course happened naturally and spontaneously at Fukushima. Workers simultaneously made heroic emergency efforts to resupply grid power from offsite, provide power onsite, and use whatever backup, battery, pump, mobile, or other systems that they could deploy to enable control and cooling.

Each reactor system has reported the resulting timing and location of emergency power restoration, so we can calculate the dynamic probability of extended systems failure, P(EF) from the recovery sequence, using the two possible choices of populations/samples, N_0, of 9 and 11 plants, where 9 is the total number of Fukushima units, and 11 is the total number of plants suffering LOOP/LOSP. Therefore, we do not know which of the 9 or 11 total population choice is correct, so I have labeled the probability estimates DD9 and DD11, respectively in the column headings in Table 2, which also gives the reported power restoration times and locations.

I directly compare in figure 7 the actual severe event non-restoration or extended failure probability data for these two apparently

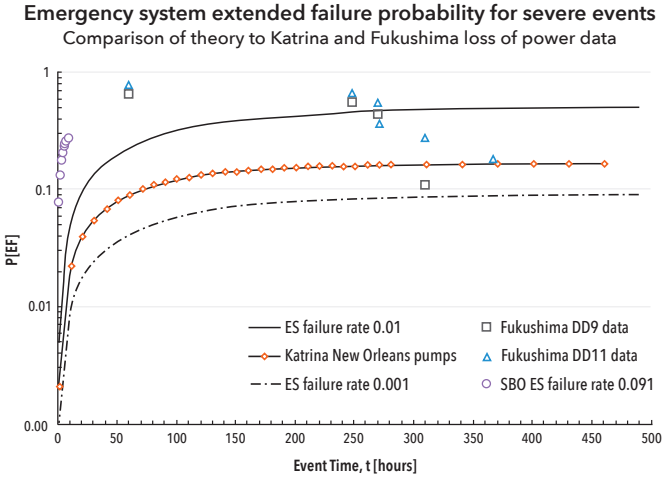


Figure 13. Probability of extended systems failure, P(EF), for assumed emergency system (ES) failure rates, and comparison to failure to restore data from the Katrina, Fukushima and calculated SBO events

disparate Type 3 events (both with $\beta \sim 0.01$ degree of damage). I compare the extended failure data for the Fukushima Daiichi and Daiini units from Table 2 (labeled by DD#) with the probability of extended systems failure, P(EF) for Hurricane Katrina using the actual emergency pump failure rate, $\lambda = 0.003$ per hour deduced from figure 6. I also show the calculated effects of a wider range of better ($\lambda = 0.001$) or worse ($\lambda = 0.01$) emergency or backup systems failure rates. For comparison, I show the shorter timescale Type 1 normal nuclear plant SBO results ($\beta = 0.22$) using the emergency systems failure rate of $\lambda \sim 0.091$ that I derived from the published calculations of Ma et al. (2018).

For the Type 3 extended events or major disasters, the emergency failure rate range encompassing that I observed is $0.001 < \lambda < 0.01$ per hour, including all engineered systems, human actions, access issues, and restoration and procedural decisions during emergency recovery and disaster response. The probability of a long or very extended outage is non-negligible and I estimate it to be of order 30% for both Type 1 and 3 events.

ENGINEERED SYSTEMS AND QUANTIFYING NATIONAL DISASTER RESILIENCE

What we have learned from these past real events has national as well as deep systems engineering implications. What is remarkable and unprecedented is that it is now possible to directly compare such disparate events and derive the range of needed failure rates for designing and implementing effective emergency backup and recovery systems. Hence, the theory and data show how emergency systems reliability, effective deployment timescale, and severe event non- restoration rate are intrinsically linked together. This is an important result, as it illustrates the influence of the failure rates at both the macroscopic engineered system and the detailed emergency response and restoration levels.

In a topical and almost philosophical terminology, many high-level reports (NAIC 2018; DHS 2018; NAS 2019) now stress the desirability of systems having some unquantified resilience or agility. Experts are even describing it as being some "capacity to resist, capacity to absorb, and the capacity to adapt" (Hegger Driessen, and Bakker 2016); or "the ability of a system to respond to, absorb, and recover from perturbations" (Fisher 2013). These are all surely desirable attributes and tautological policies, but Fang and Zio (2019) have proposed a far more precise definition and measure for real system resilience as follows.

For some k^{th} critical infrastructure network, a quantitative expression, where the dynamic resilience, R^k, to a natural hazard is the ratio of the cumulative performance under disruption and restoration over the period, P_{real}, to the target cumulative performance with no disruption, P_{target}. In the present important case for power losses in a critical power system network, the performance parameter is the dynamic probability of restoration, 1 – P(NR), with the target performance being, P(NR) = 0, attaining complete or perfect restoration at long times. By implication, since the reliability, R(t), is the complement of the probability of failure to restore, the resilience is the conventional reliability, so straightforwardly,

$$R_k(NR) = P_{real} P_{target} \equiv R \quad t=1-P \quad NR$$

Systems engineers and risk analysts know this treatment of failure and definition using reliability well. The so-called hardening of power distribution systems to achieve resilience has been promoted (NIAC 2018; DHS 2016); but improvement claims are based on the reduced average restoration times and damaged pole count for Hurricane Irma, not for the regions or outages with the worst access and degree of restoration difficulty issues. The full dynamic probability results in figure 2 and my published analysis of the regional (not the average) variation which states: "The least initially damaged cities and less flooded regions with easier access were fully restored by 200-300 h, except for the heavily inundated Naples/Collier region, which confirms that damage and access difficulty dominates recovery" (Duffey 2019a) do not confirm such improvement.

The present and new results also show that the probability of emergency systems failure and recovery follows the same general trends. Independent of the details and type of the severe event itself, they share the common issues of restoration delays caused by extensive damage, access problems, and the degree of difficulty. Hence, even so-called catastrophic power outages will follow the same trends, independent of what they are or how they occur (DHS 2016). This knowledge directly impacts the US President's National Infrastructure Advisory Council' (NAIC) recommendation to "develop a federal design basis and the design standards/criteria that identify what infrastructure sectors, cities, communities, and rural areas need to reduce the impacts and recover from a catastrophic power outage" (2018). The range of the emergency failure rate has been determined for real disasters, including all engineered systems, human actions, access issues, and restoration governance and procedural decisions.

There is also a recent recommendation to develop an "adaptable communications systems" (NAIC 2018). However, despite having a new National Joint Information Center (DHS 2017) and the US Department of Energy Eagle-I interactive geographic information system, apparently there is still no dynamic national power outage tracking system. The plethora of existing interwoven governmental emergency and commercial responsibilities (DHS, US Federal Emergency Management Agency [FEMA], Edison Electric Institute [EEI], North American Electric Reliability Corporation [NERC], National Association of Regulatory Utility Commissioners [NARUC], US Department of Defense [DoD], US Department of Transportation [DoT], American Public Power Association [APPA], and Nuclear Energy Institutute [NEI], for example) need a national outage data tracking center and enhanced and extended outage prevention and restoration to help ensure effective emergency management response.

CONCLUSIONS

The analysis of the restoration of failed and damaged infrastructure due to severe events (hurricanes, typhoons, floods, fires, and ice storms) enables the evaluation of engineered emergency backup systems deployment and reliability. I have derived comparisons and working correlations from extensive failure data for many major severe events. We can use the results to define the potential reliability and critical deployment timescales for engineered emergency systems.

We can measure the ability to respond in an emergency or disaster by the probability of outage restoration and is independent of the type of initiating severe event. The dynamic methodology shows the reliability requirements, deployment timescale, and severe event restoration rates are intrinsically coupled together. The implication is that for these major disasters, the emergency failure rate is $0.001 < \lambda < 0.01$ per hour, including all engineered systems, human actions, and decisions. I have shown the probability of a long or very extended outage to be non-negligible and estimated as of order 30% from the data and predictions for the Fukushima and Katrina severe events.

We can straightforwardly quantify the oft-used qualitative system resilience terminology for coping with severe flooding events by using the more traditional engineered systems reliability.

We need a national outage data tracking center and enhanced extended outage prevention and restoration, irrespective of the existing governmental emergency and commercial responsibilities. ■

ACKNOWLEDGEMENTS

I thank Katya L. LeBlanc for pointing out the important link to cyberattacks. I am indebted to all those who have collected and openly published the online power outage data; and to the US National Weather Service and its dedicated staff who supplied key references, reports, and online flood data. The access to public online resources of the DHS, FEMA, US National Oceanic and Atmospheric Administration, USACE, US Department of Energy, UK Environment Agency Città di Venezia, and the other entities and electric utilities I listed in the paper was also extremely important.

REFERENCES

- Adibi, M. M., and D. P. Milanicz. 1999. "Estimating Restoration Duration." *IEEE Transactions on Power Systems*. 14 (4): 1493–1497.
- Alam M. A., K. Emura, C. Farnham, and J. Yuan. 2018. "Best-Fit Probability Distributions and Return Periods for Maximum Monthly Rainfall in Bangladesh." *Climate* 6 (1). doi:10.3390/cli6010009.
- American Society of Mechanical Engineers Presidential (ASME) Task Force. 2013. "Forging a New Nuclear Safety Construct." Workshop summary report, ASME. https://files.asme.org/Events/NuclearSafetyConstructWorkshop/34231.pdf.
- Asquith, W., J. Kiang, T. Cohn. 2017. "Application of At-Site Peak-Streamflow Frequency Analyses for Very Low Annual Exceedance Probabilities." Scientific investigations report 2017-5038, US Geological Survey in cooperation with US Nuclear Regulatory Commission. https://doi.org/10.3133/sir20175038.
- Bonnin, G. M., D. Martin, L. Bingzhang, T. Parzybok, M. Yekta, D. Riley. 2006. Precipitation-Frequency Atlas of the United States. Vol. 2, Version 3.0. Silver Spring, US-MD: National Oceanic and Atmospheric Administration (NOAA). https://www.nws.noaa.gov/oh/hdsc/PF_documents/Atlas14_Volume2.pdf.
- Chow, M., L. S. Taylor, and M. Chow. 1996. "Time of Outage Restoration Analysis in Distribution Systems," IEEE Transactions on Power Delivery. 11 (3): 1652–1658. doi: 10.1109/61.517530.
- Città di Venezia. 2019. "Dati e Statistiche SUAP." www.comune.venezia.it/it/content/dati-e-statistiche.
- COMRISK. 2006. "Common Strategies to Reduce the Risk of Storm Floods in Coastal Lowlands." https://discomap.eea.europa.eu/map/Data/Milieu/OURCOAST_186_DE/OURCOAST_186_DE_Doc2_COMRISKbrochure.pdf.
- DeGaetano, A. T. 2009. "Time-Dependent Changes in Extreme-Precipitation Return-Period Amounts in the Continental United States." *Journal of Applied Meteorology and Climatology* (48): 2086-2099. doi: 10.1175/2009JAMC2179.1.
- DHS (US Department of Homeland Security). 2016. National Disaster Recovery Framework, Second Edition. June. http://www.fema.gov/media-library-data/1466014998123-4bec8550930f774269e0c5968b120ba2/National_Disaster_Recovery_Framework2nd.pdf.
- ——. 2017. "Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage." Power outage incident annex, US Federal Emergency Management Agency (FEMA). https://www.fema.gov/media-library-data/1512398599047-7565406438d0820111177a9a2d4ee3c6/POIA_Final_7-2017v2_(Compliant_pda)_508.pdf.
- ——. 2018. "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities." Report, Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/sites/default/files/publications/E013800-electricity-subsector-report.pdf.
- Duffey, R. B. 2015. "Extreme Events: Causes and Prediction." Paper presented at the PSA 2015 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Sun Valley, US-ID, 26-30 April.
- ——. 2018. "Power Restoration for Major Events and Disasters: The Influence of Distribution System Scale." Paper presented at the International Conference on Energy Engineering and Smart Grids, Cambridge, GB, 25-26 June.
- ——. 2019a. "Power Restoration Prediction Following Extreme Events and Disasters." *International Journal of Disaster Risk Science* 10 (1): 134-148. doi: 10.1007/s13753-018-0189-2.
- ——. 2019b. "The Risk of Extended Power Loss and the Probability of Emergency Restoration for Severe Events and Nuclear Accidents." *Journal of Nuclear Engineering and Radiation Science* 5 (3). doi: 10.1115/1.4042970.
- ——. 2020. "Record Flooding Risk and Emergency Power Outage Restoration." Paper to be presented at the 30th European Safety and Reliability Conference, Venice, IT, 1-6 November.
- Duffey, R. B., and J. W. Saull. 2008. *Managing Risk: The Human Element*. West Sussex, GB: John Wiley & Sons.
- Eide, S. A., C. D. Gentillon, T. E. Wierman, D. M. and Rasmussen. 2005. "Reevaluation of Station Blackout Risk at Nuclear Power Plants: Analysis of Loss of Offsite Power Events: 1986-2004 (NUREG-CR6890)." Report, US Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML0602/ML060200477.pdf.
- Emanuel, K. 2017. "Assessing the Present and Future Probability of Hurricane Harvey's Rainfall." *Proceedings of the National Academy of Sciences* 114 (48): 12681-12684. doi: 10.1073/pnas.176222114.
- England, J. F., Jr., T. A. Cohn, B. A. Faber, J. R. Stedinger, W. O. Thomas, Jr., A. G. Veilleux, J. E. Kiang, and R. R. Mason, Jr. 2018. "Guidelines for Determining Flood Flow Frequency: Bulletin 17C." Guidelines, US Department of the Interior Geological Survey. https://pubs.usgs.gov/tm/04/b05/tm4b5.pdf.
- Fang, Y., and E. Zio. 2019. "An Adaptive Robust Framework for the Optimization of the Resilience of Interdependent Infrastructures under Natural Hazards." *European Journal of Operational Research* 276 (3): 1119-1136. doi: 10.1016/j.ejor.2019.01.052.
- Fisher, L. 2013. "Preparing for Future Catastrophes: Governance Principles for Slow-Developing Risks that May Have Potentially Catastrophic Consequences." Report, International Risk Governance Council (IGRC). https://www.stat.berkeley.edu/~aldous/157/Papers/Prep.-for-Future-Catastrophes_final_11March13.pdf.
- Franz, K. J., and S. Sorooshian. 2002. "Verification of National Weather Service Probabilistic Hydrologic Forecasts." Final report, University of Arizona Department of Hydrology and Water Resources. http://nws.noaa.gov/ohd/hrl/verification/univ_of_az_verification_final_report.pdf.
- GAO (US Government Accountability Office). 2018. "2017 Hurricanes and Wildfires: Initial Observations on the Federal Response and Key Recovery Challenges." Report, GAO. https://www.gao.gov/assets/700/694231.pdf.

- Goldsmith, M., and M. Brass. 2012. "Milton 2060 Flood Risk Management Strategy for Milton and the Tokomairiro Plain." Report, Otago Regional Council (ORC). https://www.orc.govt.nz/media/3796/milton-2060-strategy.pdf.
- Greiner, W., L. Neise, and H. Stocker. 1995. *Thermodynamics and Statistical Mechanics*. New York, US-NY: Springer.
- Hegger, D. L. T., P. P. J. Driessen, and M. H. N. Bakker. 2016. "A View on More Resilient Flood Risk Governance: Key Conclusions of the STAR-FLOOD Project." Technical report, STAR-FLOOD Consortium.
- Jaynes, E. T. 2003. *Probability Theory: The Logic of Science*. Edited by G. L. Bretthorst. New York, US-NY: Cambridge University Press.
- Jorissen, R., E. Kraaij, and E. Tromp. 2016. "Dutch Flood Prevention Policy and Measures Based on Risk Assessment." Paper presented at the 3rd European Conference on Flood Risk Management, Lyon, FR, 17-21 October.
- Langat, P., K. Langat, L. Kuma, and R. Koech. 2019. "Identification of the Most Suitable Probability Distribution Models for Maximum, Minimum, and Mean Streamflow." *Water* 11 (4): 734. doi: 10.3390/w11040734.
- Lee, R. M., M. J. Assante, and T. Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case." Report, Electricity Information Sharing and Analysis Center (E-ISAC). https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- Ma, Z., C. Parisis, H. Zhang, D. Mandelli, C. Blakely, J. Yu, R. Youngblood, and N. Anderson. 2018. "Plant-Level Scenario-Based Risk Analysis for Enhanced Resilient PWR–SBO and LBLOCA." Report, US Department of Energy, Office of Nuclear Energy. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_7347.pdf.
- Matczak, P., M. Wiering, J. Lewandowski, T. Schellenberger, Trémorin J.-B., A. Crabbé, W. Ganzevoort, M. Kaufmann, C. Larrue, D. Liefferink, H. and Mees. 2016. "Comparing Flood Risk Governance in Six European Countries: Strategies, Arrangements, and Institutional Dynamics." Report, STAR- FLOOD Consortium. https://www.starflood.eu/documents/2016/04/comparison-of-countries.pdf/.
- Mel, R. and P. Lionello. 2014. "Storm Surge Ensemble Prediction for the City of Venice." *Weather and Forecasting* 29 (4): 1044-1057. doi: 10.1175/WAF-D-13-00117.1.
- Mohsson, M. 2008. "Flood Recovery, Innovation and Response I: An insight into Flood Frequency for Design Floods." *WIT Transactions on Ecology and the Environment* 118:155-164. doi:10.2495/FRIAR080161.
- NAS (US National Academies of Sciences, Engineering, and Medicine). 2019. *Framing the Challenge of Urban Flooding in the United States*. Washington, US-DC: The National Academies Press. doi:10.17226/25381.
- NIAC (US President's National Infrastructure Advisory Council). 2018. "Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of a Nation." Report, NIAC. https://www.cisa.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf.
- NRC (US Nuclear Regulatory Commission). 2016. "Mitigation of Beyond-Design Basis Events and Associated Regulatory Guidance." Report, NRC.
- Perica, S., D. Martin, S. Pavlovic, I. Roy, M. St. Laurent, C. Trypaluk, D. Unruh, M. Yekta, and G. Bonnin. 2013. *Precipitation-Frequency Atlas of the United States*, Vol. 9, Version 2.0. Silver Spring, US: MD: National Oceanic and Atmospheric Administration (NOAA). https://www.nws.noaa.gov/oh/hdsc/PF_documents/Atlas14_Volume9.pdf.
- Sandoval, C. E., and J. Raynal-Villaseñor. 2008. "Trivariate Generalized Extreme Value Distribution in Flood Frequency Analysis." *Journal Hydrological Sciences* 53 (3): 550-567. doi: 10.1623/hysj.53.3.550.
- Shukla, R. K., and M. K. Trivedi. 2010. "On the Proficient Use of GEV Distribution: A Case Study of Subtropical Monsoon Region in India." *Annals. Computer Science Series*, 8th Tome 1st Fasc.–2010: 81-92. arxiv.org/pdf/1203.0642.pdf.
- TEPCO (Tokyo Electric Power Company). 2012. "Fukushima Nuclear Accident Analysis Report." Report, TEPCO. https://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0104.pdf.
- UK Environment Agency. 2009. "Flooding in England: A National Assessment of Flood Risk." Report, UK Environment Agency. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/292928/geho0609bqds-e-e.pdf.
- USACE (US Army Corps of Engineers). 2006. "Performance Evaluation of the New Orleans and Southeast Louisiana Hurricane Protection System: Draft Final Report of the Interagency Performance Evaluation Task Force." Report, US Army Corps of Engineers, Interagency Performance Evaluation Task Force. usace.contentdm.oclc.org/digital/collection/p266001coll1/id/2844/.
- Wing, O. E. J., P. D. Bates, A. M. Smith, C. C. Sampson, K. A. Johnson, J. Fargione, and P. Morefield. 2018. "Estimates of Present and Future Flood Risk in the Conterminous United States." *Environmental Research Letters* 13 (3): 034023. doi.org/10.1088/1748-9326/aaac65.
- Wright, J.M. 2007. "Floodplain Management: Principles and Current Practices." US Federal Emergency Management Agency (FEMA) Academic Emergency Management and Related Courses (AEMRC) for the Higher Education Program. https://training.fema.gov/hiedu/aemrc/courses/coursetreat/fm.aspx).
- Zio, E. 2016. "Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures." *Reliability Engineering and System Safety* 152:137-150. doi: 10.1016/j.ress.2016.02.009.

ABOUT THE AUTHOR

Romney B. Duffey is a nuclear scientist. Duffey has worked on modern energy systems, in the areas of thermohydraulics, system design, system analysis, risk assessment, human factors, and technological safety in Britain, Canada, and the United States, for about 40 years, and authored numerous publications, including several books, including two on the subject of risk. Duffey is an ASME fellow, former chair of ASME Nuclear Engineering Division, former chair of American Nuclear Society Thermal-Hydraulics Division, the chief scientist of Atomic Energy of Canada Limited, member of New York Academy of Sciences, member of American, Canadian and British Nuclear Associations. He served as advisor or program reviewer for numerous organizations, including NASA Ames, International Atomic Energy Agency, Natural Resources Canada, European Union, Generation IV International Forum, General Electric Corporation, Columbia University, and Stony Brook University.

Loss of Offsite Power Recovery Modeling in United States Nuclear Power Plants

Zhegang Ma, zhegang.ma@inl.gov; **Curtis L. Smith,** curtis.smith@inl.gov; and **Nancy E. Johnson,** nancy.johnson@inl.gov

■ **ABSTRACT**
Loss of offsite power (LOOP) can have a major, adverse impact on a nuclear power plant's (NPP) ability to achieve and maintain safe shutdown conditions. The time required for subsequent restoration of offsite power after a LOOP event occurred and the probabilities of LOOP events exceeding various durations (or LOOP non-recovery probabilities) are important inputs to NPP probabilistic risk assessments (PRA). This paper reviews the analysis of LOOP events at United States commercial NPPs conducted by Idaho National Laboratory (INL) for the US Nuclear Regulatory Commission (NRC). This paper presents the current LOOP recovery modeling that estimates probabilities of LOOP events exceeding various durations (or LOOP non-recovery probabilities) based on operating experience. NPPs use these LOOP results in PRA models for various risk-informed activities. Finally, this paper provides the LOOP non-recovery probability results for the four LOOP categories: plant-centered, switchyard-centered, grid-related, and weather-related with LOOP recovery data from 1988 to 2018.

INTRODUCTION

United States commercial nuclear power plants (NPP) rely on alternating current (ac) power supplied through the electric grid for both routine operation and accident recovery. Normally, offsite sources supply ac power via the grid to safety and non-safety buses. Although the design of an NPP includes onsite generating equipment as the emergency power source, a loss of normal offsite power (LOOP) event, which is the simultaneous loss of electrical power to all unit safety buses requiring all emergency power generators to start and supply power to the safety buses, can still have a major negative impact on the NPP's ability to achieve and maintain safe shutdown conditions. Risk analyses have shown that LOOP and the subsequent station blackout (SBO), which involves the LOOP concurrent with the failure of the onsite emergency ac power system, is often a significant contributor to a NPP's internal events core damage risk. For example, NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (NRC 1990)" found that SBO could contribute 50% or more of analyzed plant core damage frequency. NUREG/CR-6890, "Reevaluation of Station Blackout Risk at Nuclear Power (Eide et al. 2005)," also indicated that the loss of all ac power could contributes over 70% of the overall risk at some plants. Although nuclear plants have since made modifications and improvements such as the new reactor coolant pump shutdown seal design or increased onsite power supply capability, LOOP/SBO analysis is still an important part in NPP probabilistic risk assessments (PRA). LOOP events and subsequent restoration of offsite power are important inputs to PRAs. These inputs must reflect current industry performance so PRAs accurately estimate the risk from LOOP-initiated scenarios.

Idaho National Laboratory (INL) has provided technical assistance to the US Nuclear Regulatory Commission (NRC) in the areas of reliability and risk analysis since the 1980's. NUREG/CR-6890 was published in 2005 documenting analysis of LOOP events from 1986-2004 at US NPPs. The NRC has updated the LOOP analysis annually with the latest one documented in INL/EXT-19-54699, "Analysis of Loss-of-Offsite-Power Events: 1987-2018 (Johnson and Ma 2019)," with operating experience data up to 2018. All the NRC/INL LOOP analysis reports are publicly available and you can find them in the NRC reactor operational experience results and databases website, http://nrcoe.inl.gov/resultsdb/LOSP. The presented analyses categorized LOOP events into four types by location or cause: plant-centered, switchyard-centered, grid-related, and weather-related. Table 1 presents the location or cause of each LOOP category as well as who performs the actions to restore offsite power to safety buses. We separated weather-related LOOP events from other categories as they often require a longer time due to the extent of the damage caused or the restrictions to the restoration efforts by the weather. Some weather-related events did have crossover

Table 1. LOOP event categories by location or cause

LOOP Category	Location/Cause	Personnel to Restore
Plant-Centered	Within the plant, up to but not including the auxiliary or station transformers	Plant personnel
Switchyard-Centered	Within the switchyard, up to and including the output bus bar	Plant and switchyard personnel
Grid-Related	In the interconnected transmission grid	Transmission grid personnel and outside the direct control of plant personnel
Weather-Related	Caused by severe or extreme weather	Varies

with other LOOP categories, and NUREG/CR-6890 provides glossaries and examples on how to classify LOOP events. The report used this event categorization scheme because offsite power restoration times and frequency may vary among these categories. The nuclear PRA industry has used this event categorization since early 2000s.

The following sections will present the current method to estimate LOOP non-recovery probability based on operating experience. The NRC uses the results in NRC PRA models for various risk-informed activities such as significance determination process, notice of enforcement discretion, and others. Finally, this paper investigates alternative approaches that the industry could use to model LOOP recovery and compares the results with those from the current approach.

LOOP RECOVERY MODELING

Probabilities of LOOPs exceeding various durations (or LOOP non-recovery probabilities) are important inputs to NPP PRA. LOOP non-recovery probability is the probability of a LOOP that is not recovered within a selected duration, which we can also state as the probability of a LOOP lasting longer than the selected duration.

We performed LOOP non-recovery probability analysis on LOOP duration data at the site event level instead of individual plant level. For example, if a single grid-related event resulted in a LOOP at both plants at a two-plant site, we then averaged the restoration times of the two individual plants and considered them as one entry for grid-related LOOP durations. For simultaneous LOOPs at more than one site, such as the 2003 northeast blackout that included nine plant LOOPs at six sites, using the site level LOOP durations preserves the site-to-site variation observed.

The analysis uses the LOOP restoration data that are primarily based on licensee event reports (LER) in which NPPs must report to the NRC significant plant events, including those LOOP events that trip the reactor. Appendix A of INL/EXT-19-54699 provides a list of the LERs that are associated with the LOOP events that occurred from 1987 to 2018 (Johnson and Ma 2019). The list includes three types of restoration time: switchyard restoration time (which is the duration from the start of the LOOP to when offsite power was restored), potential bus recovery time (which is the duration from the start of the LOOP to when offsite power could have been recovered to a safety bus), and actual bus restoration time (which is the duration from the start of the LOOP to when offsite power was actually restored to a safety bus). We use potential bus recovery time rather than the actual bus restoration time in the analysis. This is because if the emergency electrical power sources are available, plants may decide to delay the restoration of offsite power to safety buses due to other higher priory activities related to the LOOP event. We estimated potential bus recovery times based on the switchyard restoration times (coming from the LERs) plus the times required for the operator to restore power from the switchyard to a safety bus. We only used sustained LOOP recovery times for modeling the duration of recovery from LOOP. Sustained recovery times are times that are at least two minutes long.

We fitted the potential bus recovery times for each LOOP category in Table 1 to a density function such as lognormal and Weibull. In almost all cases, the lognormal curve fit the data better, so we used it in the analysis. The lognormal density and cumulative distribution functions used for the recovery times are as follows:

$$ft = 1t2\pi\sigma e - 12\ln t - \mu\sigma 2$$

$$F(t) = \Phi\left[\frac{\ln(t) - \mu}{\sigma}\right] = \text{Prob [potential recovery time} <= 1$$

Where

t = offsite power potential bus recovery time
μ = mean of natural logarithms of data
σ = standard deviation of natural logarithms of data
Φ = cumulative distribution function of the standard normal distribution

Table 2. Fitted lognormal recovery time distributions

Parameter	Plant-centered	Switchyard-centered	Grid-related	Weather-related
LOOP event count	33	70	16	24
Mu (μ)	-0.10	0.15	0.80	1.73
Standard error of μ	0.31	0.18	0.29	0.41
Sigma (σ)	1.80	1.49	1.17	1.99
Standard error of σ	0.22	0.13	0.21	0.29
Fitted median, hour	0.90	1.16	2.23	5.62
Fitted mean, hour	4.53	3.53	4.40	40.98
Fitted 95th percentile, hour	17.31	13.48	15.18	149.21
Error Factor	19.18	11.65	6.81	26.56

We should note that the LOOP recovery modeling in figure 1 reflects the state-of-the-practice and classic approach in the LOOP analysis in nuclear industry, which uses the industry operating experiences, or the nuclear data, to develop statistical model and estimate failure probabilities or failure rates as the inputs to the industry PRA models. The analysis is thus data-driven instead of mechanics- or physics-driven. Recently there were some efforts that proposed alternative approaches. For example, (Duffey 2019) found that the outage data for all types of major events including NPP LOOPs, earthquakes, ice storms, hurricanes, fires, and floods follow the same fundamental trends. Simple exponential functions were then developed for a general power non-restoration probability, which is dependent on and grouped by the degree of difficulty as characterized by damage and social disruption.

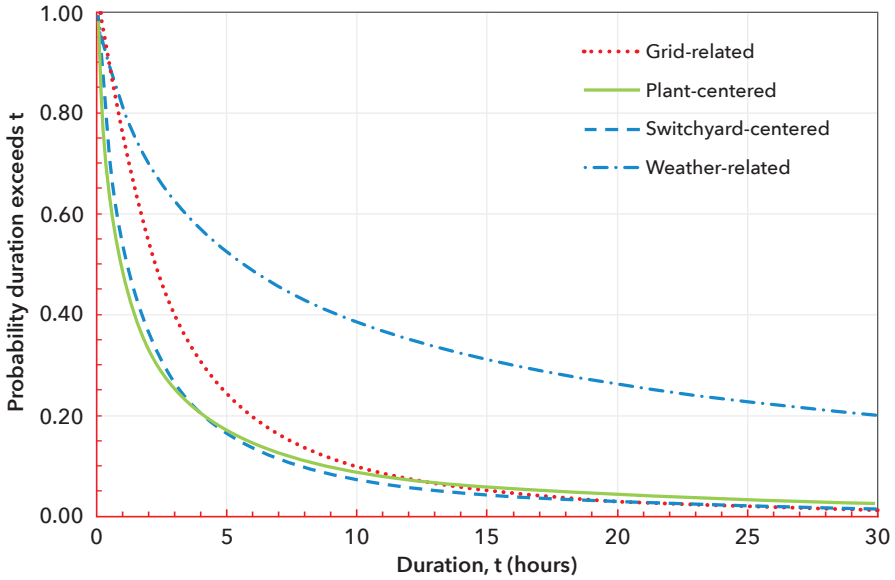


Figure 1. Non-recovery probability curves for different LOOP categories

LOOP RECOVERY ANALYSIS RESULTS

As an example of the LOOP recovery modeling results in figure 1, Table 2 shows the parameters of the fitted lognormal distributions and the fitted median, mean, 95% percentile offsite power potential bus recovery times for LOOP recovery data from 1988 to 2018.

We can then determine the probability of exceedance for a given duration or LOOP non-recovery probability by one minus the cumulative distribution function for the duration. We plotted the distributions in Table 2 as the curve of probability of exceedance versus duration in figure 1. The results show that weather-related LOOPs have the longest recovery times and highest non-recovery probabilities; plant-centered and switchyard-centered LOOPs have comparable non-recovery probabilities; and grid-related LOOPs have higher non-recovery probabilities than those of plant-centered and switchyard-centered LOOPs for LOOP durations less than 10 hours, but comparable probabilities for LOOP durations greater than 10 hours.

CONCLUSION

US commercial NPPs rely on alternating current power supplied through the electric grid for both routine operation and accident recovery. LOOP events have a major negative impact on NPP's ability to achieve and maintain safe shutdown conditions. LOOP events and subsequent restoration of offsite power are important inputs to NPP PRAs. This paper presents the current LOOP recovery modeling and the estimation of probabilities of LOOPs exceeding various durations or LOOP non-recovery probabilities. NPPs use these LOOP results in PRA models for various risk-informed activities. The analysis results with LOOP data from 1988 to 2018 show that weather-related LOOPs have the longest recovery times and highest non-recovery probabilities. The plant-centered LOOP non-recovery probabilities are comparable with those of switchyard-centered LOOPs. The grid-related LOOPs have higher non-recovery probabilities than those of plant-centered and switchyard-centered LOOPs for LOOP durations less than 10 hours, but comparable probabilities for LOOP durations greater than 10 hours. ■

DISCLAIMER

REFERENCES

- Duffey, R. B. 2019. "The Risk of Extended Power Loss and the Probability of Emergency Restoration for Severe Events and Nuclear Accidents." *The American Society of Mechanical Engineers Journal of Nuclear Engineering and Radiation Science* 5(3): 031601, 1-14.
- Eide, S. A., C. D. Gentillon, T. E. Wierman, D. M. and Rasmussen. 2005. "Reevaluation of Station Blackout Risk at Nuclear Power Plants: Analysis of Loss of Offsite Power Events: 1986-2004 (NUREG-CR6890)." Report, US Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML0602/ML060200477.pdf.
- Johnson, N., and Z. Ma. 2019. "Analysis of Loss-of-Offsite-Power Events: 1987-2018 INL/EXT-19-54699." Report, Idaho National Laboratory. https://nrcoe.inl.gov/resultsdb/publicdocs/LOSP/loop-summary-update-2017.pdf.
- NRC (US Nuclear Regulatory Commission). 1990. "Severe Accident Risks: An Assessment fro Five US Nuclear Power Plants (NUREG-1150)". Report, US Nuclear Regulatory Commission.

Systems Engineering: The Journal of The International Council on Systems Engineering

Call for Papers

The *Systems Engineering* journal is intended to be a primary source of multidisciplinary information for the systems engineering and management of products and services, and processes of all types. Systems engineering activities involve the technologies and system management approaches needed for

- definition of systems, including identification of user requirements and technological specifications;
- development of systems, including conceptual architectures, tradeoff of design concepts, configuration management during system development, integration of new systems with legacy systems, integrated product and process development; and
- deployment of systems, including operational test and evaluation, maintenance over an extended life cycle, and re-engineering.

Systems Engineering is the archival journal of, and exists to serve the following objectives of, the International Council on Systems Engineering (INCOSE):

- To provide a focal point for dissemination of systems engineering knowledge
- To promote collaboration in systems engineering education and research
- To encourage and assure establishment of professional standards for integrity in the practice of systems engineering
- To improve the professional status of all those engaged in the practice of systems engineering
- To encourage governmental and industrial support for research and educational programs that will improve the systems engineering process and its practice

The journal supports these goals by providing a continuing, respected publication of peer-reviewed results from research and development in the area of systems engineering. Systems engineering is defined broadly in this context as an interdisciplinary approach and means to enable the realization of successful systems that are of high quality, cost-effective, and trustworthy in meeting customer requirements.

The *Systems Engineering* journal is dedicated to all aspects of the engineering of systems: technical, management, economic, and social. It focuses on the life cycle processes needed to create trustworthy and high-quality systems. It will also emphasize the systems management efforts needed to define, develop, and deploy trustworthy and high quality processes for the production of systems. Within this, *Systems Engineering* is especially concerned with evaluation of the efficiency and effectiveness of systems management, technical direction, and integration of systems. *Systems Engineering* is also very concerned with the engineering of systems that support sustainable development. Modern systems, including both products and services, are often very knowledge-intensive, and are found in both the public and private sectors. The journal emphasizes strategic and program management of these, and the information and knowledge base for knowledge principles, knowledge practices, and knowledge perspectives for the engineering of systems. Definitive case studies involving systems engineering practice are especially welcome.

The journal is a primary source of information for the systems engineering of products and services that are generally large in scale, scope, and complexity. *Systems Engineering* will be especially concerned with process- or product-line–related efforts needed to produce products that are trustworthy and of high quality, and that are cost effective in meeting user needs. A major component of this is system cost and operational effectiveness determination, and the development of processes that ensure that products are cost effective. This requires the integration of a number of engineering disciplines necessary for the definition, development, and deployment of complex systems. It also requires attention to the lifecycle process used to produce systems, and the integration of systems, including legacy systems, at various architectural levels. In addition, appropriate systems management of information and knowledge across technologies, organizations, and environments is also needed to insure a sustainable world.

The journal will accept and review submissions in English from any author, in any global locality, whether or not the author is an INCOSE member. A body of international peers will review all submissions, and the reviewers will suggest potential revisions to the author, with the intent to achieve published papers that

- relate to the field of systems engineering;
- represent new, previously unpublished work;
- advance the state of knowledge of the field; and
- conform to a high standard of scholarly presentation.

Editorial selection of works for publication will be made based on content, without regard to the stature of the authors. Selections will include a wide variety of international works, recognizing and supporting the essential breadth and universality of the field. Final selection of papers for publication, and the form of publication, shall rest with the editor.

Submission of quality papers for review is strongly encouraged. The review process is estimated to take three months, occasionally longer for hard-copy manuscript.

Systems Engineering operates an online submission and peer review system that allows authors to submit articles online and track their progress, throughout the peer-review process, via a web interface. All papers submitted to *Systems Engineering*, including revisions or resubmissions of prior manuscripts, must be made through the online system. Contributions sent through regular mail on paper or emails with attachments will not be reviewed or acknowledged.

All manuscripts must be submitted online to *Systems Engineering* at ScholarOne Manuscripts, located at:

http://mc.manuscriptcentral.com/SYS

Full instructions and support are available on the site, and a user ID and password can be obtained on the first visit.

INCOSE®

INCOSE Certification

See why the top companies are **seeking out INCOSE Certified Systems Engineering Professionals.**

Are you ready to advance your career in systems engineering? Then look into INCOSE certification and set yourself apart. We offer three levels of certification for professionals who are ready to take charge of their career success.

Apply for INCOSE Certification Today!

ASSOCIATE INCOSE ASEP SYSTEMS ENGINEERING PROFESSIONAL™

CERTIFIED INCOSE CSEP SYSTEMS ENGINEERING PROFESSIONAL™

EXPERT INCOSE ESEP SYSTEMS ENGINEERING PROFESSIONAL™

Visit www.INCOSE.ORG or call 800.366.1164