# **Uptime**Institute<sup>®</sup>



# Examining and Learning from Complex Systems Failures

in Executive

Conventional wisdom blames "human error" for the majority of outages, but those failures are incorrectly attributed to front-line operator errors, rather than management mistakes

#### By Julian Kudritzki, with Anne Corning

Data centers, oil rigs, ships, power plants, and airplanes may seem like vastly different entities, but all are large and complex systems that can be subject to failures—sometimes catastrophic failure. Natural events like earthquakes or storms may initiate a complex system failure. But often blame is assigned to "human error"—front-line operator mistakes, which combine with a lack of PLEASE NOTE: This introduction was added by the Journal's editors. The article as I wrote it begins at the red subject header on the following page: "EXAMINING FAILURES" appropriate procedures and resources or compromised structures that result from poor management decisions.

"Human error" is an insufficient and misleading term. The front-line operator's presence at the site of the incident ascribes responsibility to the operator for failure to rescue the situation. But this masks the underlying causes of an incident. It is more helpful to consider the site of the incident as a spectacle of mismanagement.

Responsibility for an incident, in most cases, can be attributed to a senior management decision (e.g., design compromises, budget cuts, staff reductions, vendor selecting and resourcing) seemingly disconnected in time and space from the site of the incident. What decisions led to a situation where front line operators were unprepared or untrained to respond to an incident and mishandled it?

To safeguard against failures, standards and practices have evolved in many industries that encompass strict criteria and requirements for the design and operation of systems, often including inspection regimens and certifications. Compiled, codified, and enforced by agencies and entities in each industry, these programs and requirements help protect the service user from the bodily injuries or financial effects of failures and spur industries to maintain preparedness and best practices.

Twenty years of Uptime Institute research into the causes of data center incidents places predominant accountability for failures at the management level and finds only single-digit percentages of spontaneous equipment failure.

This fundamental and permanent truth compelled the Uptime Institute to step further into standards and certifications that were unique to the data center and IT industry. Uptime Institute undertook a collaborative approach with a variety of stakeholders to develop outcome-based criteria that would be lasting and developed by and for the industry. Uptime Institute<sup>1</sup>s Certifications were conceived to evaluate, in an unbiased fashion, front-line operations within the context of management structure and organizational behaviors.

#### **EXAMINING FAILURES**

The sinking of the Titanic. The Deepwater Horizon oil spill. DC-10 air crashes in the 1970s. The failure of New Orleans' levee system. The Three Mile Island nuclear release. The northeast (U.S.) blackout of 2003. Battery fires in Boeing 787s. The space shuttle Challenger disaster. Fukushima Daiichi nuclear disaster. The grounding of the Kulluk arctic drilling rig. These are a few of the most infamous, and in some cases tragic, engineering system failures in history. While the examples

come from vastly different industries and each story unfolded in its own unique way, they all have something in common with each other—and with data centers. All exemplify highly complex systems operating in technologically sophisticated industries.

The hallmarks of so-called complex systems are "a large number of interacting components, emergent properties difficult to anticipate from the knowledge of single components, adaptability to absorb random disruptions, and highly vulnerable to widespread failure under adverse conditions (Dueñas-Osorio and Vemuru 2009)." Additionally, the components of complex systems typically interact in non-linear fashion, operating in large interconnected networks.

Large systems and the industries that use them have many safeguards against failure and multiple layers of protection and backup. Thus, when they fail it is due to much more than a single element or mistake.

It is a truism that complex systems tend to fail in complex ways. Looking at just a few examples from various industries, again and again we see that it was not a single factor but the compound effect of multiple factors that disrupted these sophisticated systems. Often referred to as "cascading failures," complex system breakdowns usually begin when one component or element of the system fails, requiring nearby "nodes" (or other components in the system network) to take up the workload or service obligation of the failed component. If this increased load is too great, it can cause other nodes to overload and fail as well, creating a waterfall effect as every component failure increases the load on the other, already stressed components. The following transferable concept is drawn from the power industry:

Power transmission systems are heterogeneous networks of large numbers of components that interact in diverse ways. When component operating limits are exceeded, protection acts to disconnect the component and the component "fails" in the sense of not being available... Components can also fail in the sense of misoperation or damage due to aging, fire, weather, poor maintenance, or incorrect design or operating settings.... The effects of the component failure can be local or can involve components far away, so that the loading of many other components throughout the network is increased... the flows all over the network change (Dobson, et al. 2009).

A component of the network can be mechanical, structural or human agent, as front-line operators respond to an emerging crisis. Just as engineering components can fail when overloaded, so can human effectiveness and decision-making capacity diminish under duress. A defining characteristic of a high risk organization is that it provides structure and guidance despite extenuating circumstances—duress is its standard operating condition.

The sinking of the *Titanic* is perhaps the most well-known complex system failure in history. This disaster was caused by the compound effect of structural issues, management decisions, and operating mistakes that led to the tragic loss of 1,495 lives. Just a few of the critical contributing factors include design compromises (e.g., reducing the height of the watertight bulkheads that allowed water to flow over the tops and limiting the number of lifeboats for aesthetic considerations), poor discretionary decisions (e.g., sailing at excessive speed on a moonless night despite reports of icebergs ahead), operator error (e.g., the lookout in the crow's nest had no binoculars—a cabinet key had been left behind in Southampton), and misjudgment in the crisis response (e.g., the pilot tried to reverse thrust when the iceberg was spotted, instead of continuing at full speed and using the momentum of the ship to turn course and reduce impact). And, of course, there was the hubris of believing the ship was unsinkable.



[https://journal.uptimeinstitute.com/wp-content/uploads/2015/10/BB-Kudritzki-Figure-2B-

Boeing Dreamliner battery original and damaged.ipg]

Figure 1a. (Left) NTSB photo of the burned auxiliary power unit battery from a JAL Boeing 787 that caught fire on January 7, 2013 at Boston<sup>1</sup>s Logan International Airport. Photo credit: By National Transportation Safety Board (NTSB) [Public domain], via Wikimedia Commons. Figure 1b. (Right) A side-by-side comparison of an original Boeing Dreamliner (787) battery compared and a damaged Japan Air Lines battery. Photo credit: By National Transportation Safety Board (NTSB) [Public domain], via Wikimedia Commons.

Looking at a more recent example, the issue of battery fires in Japan Airlines (JAL) Boeing 787s, which came to light in 2013 (see Figure 1), was ultimately blamed on a combination of design, engineering, and process management shortfalls (Gallagher 2014). Following its investigation, the U.S. National Transportation Safety Board reported (NTSB 2014):

• Manufacturer errors in design and quality control. The manufacturer failed to adequately account for the thermal runaway phenomenon: an initial overheating of the batteries triggered a chemical reaction that generated more heat, thus causing the batteries to explode or catch fire. Battery "manufacturing defects and lack of oversight in the cell manufacturing process" resulted in the development of lithium mineral deposits in the batteries. Called lithium dendrites, these deposits can cause a short circuit that reacts chemically with the battery cell, creating heat. Lithium dendrites occurred in wrinkles that were found in some of the battery electrolyte material, a manufacturing quality control issue.

• **Shortfall in certification processes.** The NTSB found shortcomings in U.S. Federal Aviation Administration (FAA) guidance and certification processes. Some important factors were overlooked that should have been considered during safety assessment of the batteries.

• Lack of contractor oversight and proper change orders. A cadre of contractors and subcontractors were involved in the manufacture of the 787's electrical systems and battery components. Certain entities made changes to the specifications and instructions without proper approval or oversight. When the FAA performed an audit, it found that Boeing's prime contractor wasn't following battery component assembly and installation instructions and was mislabeling parts. A lack of "adherence to written procedures and communications" was cited.

How many of these circumstances parallel those that can happen during the construction and operation of a data center? It is all too common to find deviations from as-designed systems during the construction process, inconsistent quality control oversight, and the use of multiple subcontractors. Insourced and outsourced resources may disregard or hurry past written procedures, documentation, and communication protocols (search Avoiding Data Center Construction Problems @ journal.uptimeinstitute.com).

#### THE NATURE OF COMPLEX SYSTEM FAILURES

Large industrial and engineered systems are risky by their very nature. The greater the number of components and the higher the energy and heat levels, velocity, and size and weight of these components the greater the skill and teamwork required to plan, manage, and operate the systems safely. Between mechanical components and human actions, there are thousands of possible points where an error can occur and potentially trigger a chain of failures.

In his seminal article on the topic of complex system failure *How Complex Systems Fail*, first published in 1998 and still widely referenced today, Dr. Richard I. Cook identifies and discusses 18 core elements of failure in complex systems:

- 1. Complex systems are intrinsically hazardous systems.
- 2. Complex systems are heavily and successfully defended against failure.
- 3. Catastrophe requires multiple failures—single point failures are not enough.
- 4. Complex systems contain changing mixtures of failures latent within them.
- 5. Complex systems run in degraded mode.
- 6. Catastrophe is always just around the corner.
- 7. Post-accident attribution to a root cause is fundamentally wrong.
- 8. Hindsight biases post-accident assessments of human performance.
- 9. Human operators have dual roles: as producers and as defenders against failure.
- 10. All practitioner actions are gambles.
- 11. Actions at the sharp end resolve all ambiguity.
- 12. Human practitioners are the adaptable element of complex systems.
- 13. Human expertise in complex systems is constantly changing.
- 14. Change introduces new forms of failure.
- 15. Views of cause limit the effectiveness of defenses against future events.
- 16. Safety is a characteristic of systems and not of their components.
- 17. People continuously create safety.
- 18. Failure-free operations require experience with failure (Cook 1998).

Let's examine some of these principles in the context of a data center. Certainly high-voltage electrical systems, large-scale mechanical and infrastructure components, high-pressure water piping, power generators, and other elements create hazards [Element 1] for both humans and mechanical systems/structures. Data center systems are defended from failure by a broad range of measures [Element 2], both technical (e.g., redundancy, alarms, and safety features of equipment) and human (e.g., knowledge, training, and procedures). Because of these multiple

layers of protection, a catastrophic failure would require the breakdown of multiple systems or multiple individual points of failure [Element 3].

#### RUNNING NEAR CRITICAL FAILURE

Complex systems science suggests that most large-scale complex systems, even well-run ones, by their very nature are operating in "degraded mode" [Element 5], i.e., close to the critical failure point. This is due to the progression over time of various factors including steadily increasing load demand, engineering forces, and economic factors.

The enormous investments in data center and other highly available infrastructure systems perversely incents conditions of elevated risk and higher likelihood of failure. Maximizing capacity, increasing density, and hastening production from installed infrastructure improves the return on investment (ROI) on these major capital investments. Deferred maintenance, whether due to lack of budget or hands-off periods due to heightened production, further pushes equipment towards performance limits—the breaking point.

The increasing density of data center infrastructure exemplifies the dynamics that continually and inexorably push a system towards critical failure. Server density is driven by a mixture of engineering forces (advancements in server design and efficiency) and economic pressures (demand for more processing capacity without increasing facility footprint). Increased density then necessitates corresponding increases in the number of critical heating and cooling elements. Now the system is running at higher risk, with more components (each of which is subject to individual fault/failure), more power flowing through the facility, more heat generated, etc.

This development trajectory demonstrates just a few of the powerful "self-organizing" forces in any complex system. According to Dobson, et al (2009), "these forces drive the system to a dynamic equilibrium that keeps [it] near a certain pattern of operating margins relative to the load. Note that engineering improvements and load growth are driven by strong, underlying economic and societal forces that are not easily modified."

Because of this dynamic mix of forces, the potential for a catastrophic outcome is inherent in the very nature of complex systems [Element 6]. For large-scale mission critical and business critical systems, the profound implication is that designers, system planners, and operators must acknowledge the potential for failure and build in safeguards.

#### WHY IS IT SO EASY TO BLAME HUMAN ERROR?

Human error is often cited as the root cause of many engineering system failures, yet it does not often cause a major disaster on its own. Based on analysis of 20 years of data center incidents,

Uptime Institute holds that human error must signify management failure to drive change and improvement. Leadership decisions and priorities that result in a lack of adequate staffing and training, an organizational culture that becomes dominated by a fire drill mentality, or budget cutting that reduces preventive/proactive maintenance could result in cascading failures that truly flow from the top down.

Although front-line operator error may sometimes appear to cause an incident, a single mistake (just like a single data center component failure) is not often sufficient to bring down a large and robust complex system unless conditions are such that the system is already teetering on the edge of critical failure and has multiple underlying risk factors. For example, media reports after the 1983 *Exxon Valdez* oil spill zeroed in on the fact that the captain, Joseph Hazelwood, was not at the bridge at the time of the accident and accused him of drinking heavily that night. However, more measured assessments of the accident by the NTSB and others found that Exxon had consistently failed to supervise the captain or provide sufficient crew for necessary rest breaks (see Figure 2).



[https://journal.uptimeinstitute.com/wp-content/uploads/2015/10/BB-Kudritzki-Figure-3-

ExxonValdezAground.jpeg]

Figure 2. Shortly after leaving the Port of Valdez, the Exxon Valdez ran aground on Bligh Reef. The picture was taken three days after the vessel grounded, just before a storm arrived. Photo credit: Office of Response and Restoration, National Ocean Service, National Oceanic and Atmospheric Administration [Public domain], via Wikimedia Commons.

Perhaps even more critical was the lack of essential navigation systems: the tanker's radar was not operational at time of the accident. Reports indicate that Exxon's management had allowed the RAYCAS radar system to stay broken for an entire year before the vessel ran aground because it was expensive to operate. There was also inadequate disaster preparedness and an insufficient quantity of oil spill containment equipment in the region, despite the experiences of previous small oil spills. Four years before the accident, a letter written by Captain James Woodle, who at that time was the Exxon oil group<sup>1</sup>s Valdez port commander, warned upper management, "Due to a reduction in manning, age of equipment, limited training and lack of personnel, serious doubt exists that [we] would be able to contain and clean-up effectively a medium or large size oil spill" (Palast 1999).

As Dr. Cook points out, post-accident attribution to a root cause is fundamentally wrong [Element 7]. Complete failure requires multiple faults, thus attribution of blame to a single isolated element is myopic and, arguably, scapegoating. Exxon blamed Captain Hazelwood for the accident, and his share of the blame obscures the underlying mismanagement that led to the failure. Inadequate enforcement by the U.S. Coast Guard and other regulatory agencies further contributed to the disaster.

Similarly, the grounding of the oil rig Kulluk was the direct result of a cascade of discrete failures, errors, and mishaps, but the disaster was first set in motion by Royal Dutch Shell's executive decision to move the rig off of the Alaskan coastline to avoid tax liability, despite high risks (Lavelle 2014). As a result, the rig and its tow vessels undertook a challenging 1,700-nautical-mile journey across the icy and storm-tossed waters of the Gulf of Alaska in December 2012 (Funk 2014).

There had already been a chain of engineering and inspection compromises and shortfalls surrounding the Kulluk, including the installation of used and uncertified tow shackles, a rushed refurbishment of the tow vessel Discovery, and electrical system issues with the other tow vessel, the Aivik, which had not been reported to the Coast Guard as required. (Discovery experienced an exhaust system explosion and other mechanical issues in the following months. Ultimately the tow company—a contractor—was charged with a felony for multiple violations.)

This journey would be the Kulluk's last, and it included a series of additional mistakes and mishaps. Gale-force winds put continual stress on the tow line and winches. The tow ship was captained on this trip by an inexperienced replacement, who seemingly mistook tow line tensile alarms (set to go off when tension exceeded 300 tons) for another alarm that was known to be falsely annunciating. At one point the Aivik, in attempting to circle back and attach a new tow line, was swamped by a wave, sending water into the fuel pumps (a problem that had previously been identified but not addressed), which caused the engines to begin to fail over the next several hours (see Figure 3).



[https://journal.uptimeinstitute.com/wp-content/uploads/2015/10/BB-Kudritzki-Figure-4-KullukAground.jpg]

Waves crash over the mobile offshore drilling unit Kulluk where it sits aground on the southeast side of Sitkalidak Island, Alaska, Jan. 1, 2013. A Unified Command, consisting of the Coast Guard, federal, state, local and tribal partners and industry representatives was established in response to the grounding. U.S. Coast Guard photo by Petty Officer 3rd Class Jonathan Klingenberg.

Despite harrowing conditions, Coast Guard helicopters were eventually able to rescue the 18 crew members aboard the Kulluk. Valiant last-ditch tow attempts were made by the (repaired) Aivik and Coast Guard tugboat Alert, before the effort had to be abandoned and the oil rig was pushed aground by winds and currents.

Poor management decision making, lack of adherence to proper procedures and safety requirements, taking shortcuts in the repair of critical mechanical equipment, insufficient contractor oversight, lack of personnel training/experience all of these elements of complex system failure are readily seen as contributing factors in the Kulluk disaster.

#### EXAMINING DATA CENTER SYSTEM FAILURES

Two recent incidents demonstrate how the dynamics of complex systems failures can quickly play out in the data center environment.

#### Example A

Tier III Concurrent Maintenance data center criteria (see Uptime Institute Tier Standard: Topology) require multiple, diverse independent distribution paths serving all critical equipment to allow maintenance activity without impacting critical load. The data center in this example had been designed appropriately with fuel pumps and engine- generator controls powered from multiple circuit panels. As built, however, a single panel powered both, whether due to implementation oversight or cost reduction measures. At issue is not the installer, but rather the quality of communications from the implementation team and the operations team.

In the course of operations, technicians had to shut off utility power during the performance of routine maintenance to an electrical switchgear. This meant the building was running on engine-generator sets. However, when the engine-generator sets started to surge due to a clogged fuel line. The UPS automatically switched the facility to battery power. The day tanks for the engine-generator sets were starting to run dry. If quick-thinking operators had not discovered the fuel pump issue in time, there would have been an outage to the entire facility: a cascade of events leading down a rapid pathway from simple routine maintenance activity to complete system failure.

#### Example B

Tier IV Fault Tolerant data center criteria require the ability to detect and isolate a fault while maintaining capacity to handle critical load. In this example, a Tier IV enterprise data center shared space with corporate offices in the same building, with a single chilled water plant used to cool both sides of the building. The office air handling units also brought in outside air to reduce cooling costs.

One night, the site experienced particularly cold temperatures and the control system did not switch from outside air to chilled water for office building cooling, which affected data center cooling as well. The freeze stat (a temperature sensing device that monitors a heat exchanger to prevent its coils from freezing) failed to trip; thus the temperature continued to drop and the cooling coil froze and burst, leaking chilled water onto the floor of the data center. There was a limited leak detection system in place and connected, but it had not been fully tested yet. Chilled water continued to leak until pressure dropped and then the chilled water machines started to spin offline in response. Once the chilled water machines went offline neither the office building nor data center had active cooling.

At this point, despite the extreme outside cold, temperatures in the data hall rose through the night. As a result of the elevated indoor temperature conditions, the facility experienced myriad device-level (e.g., servers, disc drives, and fans) failures over the following several weeks. Though a critical shut down was not the issue, damage to components and systems—and the cost of cleanup and replacement parts and labor—were significant. One single initiating factor—a cold night—combined with other elements in a cascade of failures.

In both of these cases, severe disaster was averted, but relying on front-line operators to save the situation is neither robust not reliable.

#### PREVENTING FAILURES IN THE DATA CENTER

Organizations that adhere to the principles of Concurrent Maintainability and/or Fault Tolerance, as outlined in Tier Standard: Topology, take a vital first step toward reducing the risk of a data center failure or outage.

However, facility infrastructure is only one component of failure prevention; how a facility is run and operated on a day-to-day basis is equally critical. As Dr. Cook noted, humans have a dual role in complex systems as both the potential producers (causes) of failure as well as, simultaneously, some of the best defenders against failure [Element 9]. The fingerprints of human error can be seen on the two data center examples. In Example A, the electrical panel was not set up as originally designed, and the leak detection system, which could have alerted operators to the problem, had not been fully activated in Example B.

Dr. Cook also points out that human operators are the most adaptable component of complex systems [Element 12], as they "actively adapt the system to maximize production and minimize accidents." For example, operators may "restructure the system to reduce exposure of vulnerable parts," reorganize critical resources to focus on areas of high demand, provide "pathways for retreat or recovery," and "establish means for early detection of changed system performance in order to allow graceful cutbacks in production or other means of increasing resiliency." Given the highly dynamic nature of complex system environments, this human-driven adaptability is key.

#### STANDARDIZATION CAN ADDRESS MANAGEMENT SHORTFALLS

In most of the notable failures in recent decades, there was a breakdown or circumvention of established standards and certifications. It was not a lack of standards, but a lack of compliance or sloppiness that contributed the most to the disastrous outcomes. For example, in the case of the Boeing batteries, the causes were bad design, poor quality inspections, and lack of contractor oversight. In the case of the *Exxon Valdez*, inoperable navigation systems and inadequate crew manpower and oversight—along with insufficient disaster preparednesswere critical factors. If leadership, operators, and oversight agencies had adhered to their own policies and requirements and had not cut corners for economics or expediency, these disasters might have been avoided.

Ongoing operating and management practices and adherence to recognized standards and requirements, therefore, must be the focus of long-term risk mitigation. In fact, Dr. Cook states that "failure-free operations are the result of activities of people who work to keep the system within the boundaries of tolerable performance....human practitioner adaptations to changing conditions actually create safety from moment to moment" [Element 17]. This emphasis on human activities as decisive in preventing failures dovetails with Uptime Institute's advocacy of operational excellence as set forth in the Tier Standard: Operational Sustainability. This was the data center industry's first standardization, developed by and for data centers, to address the management shortfalls that could unwind the most advanced, complex, and intelligent of solutions. Uptime Institute was compelled by its findings that the vast majority of data center incidents could be attributed to operations, despite advancements in technology, monitoring, and automation.

The Operational Sustainability criteria pinpoint the elements that impact long-term data center performance, encompassing site management and operating behaviors, and documentation and mitigation of site-specific risks. The detailed criteria include personnel qualifications and training and policies and procedures that support operating teams in effectively preventing failures and responding appropriately when small failures occur to avoid having them cascade into large critical failures. As Dr. Cook states, "Failure free operations require experience with failure" [Element 18]. We have the opportunity to learn from the experience of other industries, and, more importantly, from the data center industry<sup>1</sup>s own experience, as collected and analyzed in Uptime Institute's Abnormal Incident Reports database. Uptime Institute has captured and catalogued the lessons learned from more than 5,000 errors and incidents over the last 20 years and used that research knowledgebase to help develop an authoritative set of benchmarks. It has ratified these with leading industry experts and gained the consensus of global stakeholders from each sector of the industry. Uptime Institute's Tier Certifications and Management & Operations (M&O) Stamp of Approval provide the most definitive guidelines for and verification of effective risk mitigation and operations management.

Dr. Cook explains, "More robust system performance is likely to arise in systems where operators can discern the edge of the envelope. It also depends on calibrating how their actions move system performance towards or away from the edge of the envelope. [Element 18]" Uptime Institute's deep subject matter expertise, long experience, and evidence-based standards can help data center operators identify and stay on the right side of that edge. Organizations like CenturyLink are recognizing the value of applying a consistent set of standards to ensure operational excellence and minimize the risk of failure in the complex systems represented by their data center portfolio (See the sidebar CenturyLink and the M&O Stamp of Approval).

#### CONCLUSION

Complex systems fail in complex ways, a reality exacerbated by the business need to operate complex systems on the very edge of failure. The highly dynamic environments of building and operating an airplane, ship, or oil rig share many traits with running a high availability data center. The risk tolerance for a data center is similarly very low, and data centers are susceptible to the heroics and missteps of many disciplines. The coalescing element is management, which makes sure that frontline operators are equipped with the hands, tools, parts, and processes they need, and, the unbiased oversight and certifications to identify risks and drive continuous improvement against the continuous exposure to complex failure.

#### REFERENCES

ASME (American Society of Mechanical Engineers). 2011. Initiative to Address Complex Systems Failure: Prevention and Mitigation of Consequences. Report prepared by Nexight Group for ASME (June). Silver Spring MD: Nexight Group. http://nexightgroup.com/wpcontent/uploads/2013/02/initiative-to-address-complex-systems-failure.pdf

Bassett, Vicki. (1998). "Causes and effects of the rapid sinking of the Titanic," working paper. Department of Mechanical Engineering, the University of Wisconsin. http://writing.engr.vt.edu/uer/bassett.html#authorinfo.

BBC News. 2015. "Safety worries lead US airline to ban battery shipments." March 3, 2015. http://www.bbc.com/news/technology-31709198

Brown, Christopher and Matthew Mescal. 2014. View From the Field. Webinar presented by Uptime Institute, May 29, 2014. https://uptimeinstitute.com/research-publications/asset/webinar-recording-view-from-the-field

Cook, Richard I. 1998. "How Complex Systems Fail (Being a Short Treatise on the Nature of Failure; How Failure is Evaluated; How Failure is Attributed to Proximate Cause; and the Resulting New Understanding of Patient Safety)." Chicago, IL: Cognitive Technologies Laboratory, University of Chicago. Copyright 1998, 1999, 2000 by R.I. Cook, MD, for CtL. Revision D (00.04.21), http://web.mit.edu/2.75/resources/rando/How%20Complex%20Systems%20Fail.pdf

Dobson, Ian, Benjamin A. Carreras, Vickie E. Lynch and David E. Newman. 2009. "Complex systems analysis of a series of blackouts: Cascading failure, critical points, and self-organization." *Chaos: An Interdisciplinary Journal of Nonlinear Science* 17: 026103 (published by the American Institute of Physics).

Dobson, Ian, Benjamin A. Carreras, Vickie E. Lynch and David E. Newman. 2009. "Complex systems analysis of a series of blackouts: Cascading failure, critical points, and self-organization." *Chaos: An Interdisciplinary Journal of Nonlinear Science* 17: 026103 (published by the American Institute of Physics).

Dueñas-Osorio, Leonard and Srivishnu Mohan Vemuru. 2009. Abstract for "Cascading failures in complex infrastructure systems." *Structural Safety* 31 (2): 157-167.

Funk, McKenzie. 2014. "The Wreck of the Kulluk." *New York Times Magazine* December 30, 2014. http://www.nytimes.com/2015/01/04/magazine/the-wreck-of-the-kulluk.html?\_r=0 Gallagher, Sean. 2014. "NTSB blames bad battery designand bad managementin Boeing 787 fires." *Ars Technica*, December 2, 2014. http://arstechnica.com/information-technology/2014/12/ntsb-blames-bad-battery-design-and-bad-management-in-boeing-787-fires/

Glass, Robert, Walt Beyeler, Kevin Stamber, Laura Glass, Randall LaViolette, Stephen Contrad, Nancy Brodsky, Theresa Brown, Andy Scholand, and Mark Ehlen. 2005. Simulation and Analysis of Cascading Failure in Critical Infrastructure. Presentation (annotated version) Los Alamos National Laboratory, National Infrastructure Simulation and Analysis Center (Department of Homeland Security), and Sandia National Laboratories, July 2005..New Mexico: Sandia National Laboratories. http://www.sandia.gov/CasosEngineering/docs/Glass\_annotatedpresentation.pdf

Kirby, R. Lee. 2012. "Reliability Centered Maintenance: A New Approach." *Mission Critical*, June 12, 2012. http://www.missioncriticalmagazine.com/articles/84992-reliability-centered-maintenance-a-new-approach

Klesner, Keith. 2015. "Avoiding Data Center Construction Problems." *The The Uptime Institute Journal*. 5: Spring 2014: 6-12. https://journal.uptimeinstitute.com/avoiding-data-center-construction-problems/

Lipsitz, Lewis A. 2012. "Understanding Health Care as a Complex System: The Foundation for Unintended Consequences." *Journal of the American Medical Association* 308 (3): 243244. http://jama.jamanetwork.com/article.aspx?articleid=1217248

Lavelle, Marianne. 2014. "Coast Guard blames Shell risk taking in the wreck of the Kulluk." *National Geographic*, April 4, 2014.

http://news.nationalgeographic.com/news/energy/2014/04/140404-coast-guard-blames-shell-in-kulluk-rig-accident/

"Exxon Valdez Oil Spill." *New York Times*. On NYTimes.com, last updated August 3, 2010. http://topics.nytimes.com/top/reference/timestopics/subjects/e/exxon\_valdez\_oil\_spill\_1989/index.html

NTSB (National Transportation Safety Board). 2014. "Auxiliary Power Unit Battery Fire Japan Airlines Boeing 787-8, JA829J." Aircraft Incident Report released 11/21/14. Washington, DC: National Transportation Safety Board.

http://www.ntsb.gov/Pages/..%5Cinvestigations%5CAccidentReports%5CPages%5CAIR1401.aspx

Palast, Greg. 1999. "Ten Years After But Who Was to Blame?" for *Observer/Guardian UK*, March 20, 1999. http://www.gregpalast.com/ten-years-after-but-who-was-to-blame/

Pederson, Brian. 2014. "Complex systems and critical missionstoday's data center." *Lehigh Valley Business*, November 14, 2014. http://www.lvb.com/article/20141114/CANUDIGIT/141119895/complex-systems-and-critical-missions-todays-data-center

Plsek, Paul. 2003. Complexity and the Adoption of Innovation in Healthcare. Presentation, Accelerating Quality Improvement in Health Care Strategies to Speed the Diffusion of Evidence-Based Innovations, conference in Washington, DC, January 27-28, 2003. Roswell, GA: Paul E Plsek & Associates, Inc. http://www.nihcm.org/pdf/Plsek.pdf

Reason, J. 2000. "Human Errors Models and Management." *British Medical Journal* 320 (7237): 768770. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/

Reuters. 2014. "Design flaws led to lithium-ion battery fires in Boeing 787: U.S. NTSB." December 2, 2014. http://www.reuters.com/article/2014/12/02/us-boeing-787-batteryidUSKCN0JF35G20141202

Wikipedia, s.v. "Cascading Failure," last modified April 12, 2015. https://en.wikipedia.org/wiki/Cascading\_failure

Wikipedia, s.v. "The Sinking of The Titanic," last modified July 21, 2015. https://en.wikipedia.org/wiki/Sinking\_of\_the\_RMS\_Titanic

Wikipedia, s.v. "SOLAS Convention," last modified June 21, 2015. https://en.wikipedia.org/wiki/SOLAS\_Convention

John Maclean, author of numerous books, including *Fire on the Mountain* (Morrow 1999), analyzing deadly wildland fires, suggests rebranding of high reliability organizations, which is a fundamental concept of firefighting crews, military, and commercial airline industry. He argued for high risk organizations. A high reliability organization may only fail, like a goalkeeper, as performance is so highly anticipated. A high risk organization is tasked with averting or minimizing impact and may gauge success in a non-binary fashion. It is a recurring theme in Mr. Maclean's forensic analyses of deadly fires that front-line operators, including the perished, carry the blame for the outcome and management shortfalls are far less exposed.

The IT industry has growing awareness of the importance of management-people-process issues. That's why Uptime Institute<sup>1</sup>s Management & Operations (M&0) Stamp of Approval focuses on assessing and evaluating both operations activities and management as equally critical to ensuring data center reliability and performance. The M&O Stamp can be applied to a single data center facility, or administered across an entire portfolio to ensure consistency.

Recognizing the necessity of making a commitment to excellence at all levels of an organization, CenturyLink is the first service provider to embrace the M&O assesment for all of its data centers. It has contracted Uptime Institute to assess 57 data center facilities across a global portfolio. This decision shows the company is willing to hold itself to a uniform set of high standards and operate with transparency. The company has committed to achieve M&O Stamp of Approval standards and certification across the board, protecting its vital networks and assets from failure and downtime and providing its customers with assurance.



Julian Kudritzki joined Uptime Institute in 2004 and currently serves as Chief Operating Officer. He is responsible for the global proliferation of Uptime Institute standards. He has supported the founding of Uptime Institute offices in numerous regions, including Brasil, Russia, and North Asia. He has collaborated on the development of numerous Uptime Institute publications,

education programs, and unique initiatives such as Server Roundup and <u>[https://journal.uptimeinstitute.com/wp-</u> FORCSS. He is based in Seattle, WA. <u>content/uploads/2015/10/03b.jpg]</u>

Julian Kudritzki



Anne Corning is a technical and business writer with more than 20 years experience in the high tech, healthcare, and engineering fields. She earned her B.A. from the University of Chicago and her M.B.A. from the University of Washington's Foster School of Business. She has provided marketing, research, and writing for

<u> /https://journal.uptimeinstityte្អាវេឌាវែយអ</u>ិទ such as Microsoft, Skanska USA Mission <u>content/uploads/2015/10/sਸ਼ਰੀ5،ip</u>f

Anne Corning

Consulting, Seattle Children's Hospital Center for Clinical Research, Adaptive Energy, Thinking Machines

Corporation (now part of Oracle), BlueCross BlueShield of Massachusetts, and the University of Washington Institute for Translational Health Sciences. She has been a part of several successful entrepreneurial ventures and is a Six Sigma Green Belt.

### Share this entry

f ¥ 8+ in ☺ ¥
---------------

## You might also like



REPLY

## **Trackbacks & Pingbacks**

1. <u>Signs your data centre may be at risk of a crisis | ITProPortal.com</u> November 22, 2015 at 4:02 am

[...] on the surface that they can be attributable to one person's mistake, they are almost invariably, the downstream impact of leadership or management policies and decisions, or a reflection of the bro.... Even a great facilities team can be stymied by scarcity of resources, unclear mandates, or a lack [...]

## Comments are closed.

© 2014-16 Uptime Institute, LLC All rights reserved.