Resilient Infrastructures via Digital Unification

Ang Chen[1], Sylvia Ratnasamy[2], Mohammad Alizadeh[3], Mosharaf Chowdhury[1]
Seth Guikema[1], Ryan Huang[1], Suresh Jaganathann[4], Branko Kerkez[1], Edward Lee[2]
Steven Low[5], Morley Mao[1], Johanna Mathieu[1], Michael Reiter[6], Xinyu Wang[1], Vinton Cerf[7]

[1]*University of Michigan,* [2]*UC Berkeley,* [3]*MIT,* [4]*Purdue University,* [5]*Caltech,* [6]*Duke University,* [7]*Google*

Abstract

Industrial infrastructures are going through "digital transformation," but the quality of this transformation is only as good as the software tools and techniques. We argue for a principled stack design to produce rigorous software, to replace today's ad hoc approaches and increase infrastructure resilience.

Infrastructure resilience is a crucial but challenging goal

Industrial infrastructures like datacenters, power grids, and water systems must be reliable and resilient [1]—i.e., adaptive to changing conditions to withstand and recover from shocks, while maximizing resource efficiency. This is a daunting task because infrastructures are scaling up to address rising demands [2], and also because they are becoming more decentralized and diversified. Consider power grids: electrification of heating and transportation puts pressure on power supply, and the increase in distributed energy resources (e.g., solar, batteries, and flexible loads) creates a distributed and heterogeneous system. Furthermore, infrastructures are increasingly interdependent [3]. Power grids require more water for cooling due to higher energy demands, and water extraction consumes more energy because of a shrinking fresh water supply. Interdependence raises the stakes because problems often propagate across the infrastructure boundary—e.g., power failures often disrupt drinking water or natural gas distribution [4].

Digital transformation: promises and limitations

Digital transformation (DX) promises to better manage industrial infrastructures via software. Compute/networking devices are prevalently embedded in these infrastructures, and they can collect abundant data to automate complex decisions in real time. In smart grids, sensors track voltage, energy consumption, and equipment health; this enables dynamic management of renewables to match fluctuating demand, improving grid reliability and reducing carbon emissions. In smart water systems, sensors monitor flow, pressure, and water quality, allowing for precise leak detection and water waste reduction. Digital tools also apply to interdependent infrastructures—e.g., improving the freshwater efficiency of energy production, or the energy efficiency of water distribution, optimizing the "power/water nexus."

However, despite the significant potential of DX, the benefit of this transformation is bounded by the quality of digital tools. Existing tools fall short, because they do not have a rigorous design, and are point solutions that address specific problems (e.g., energy optimization/leak detection) but poorly compose. As each industry sector rolls out its own solutions, the overall digital complexity accrues with fragmented tools and incompatible data formats/protocols. This hampers interoperability, but also potentially undermines resilience and leads to cybersecurity concerns. Indeed, when critical infrastructures depend on the digital ecosystem, even minor software glitches can have significant impacts. CrowdStrike's disruption to air transport and hospitals was dramatic and costly [5], and cyberattacks on Ukrainian power grids and American Water caused large disruptions [6, 7]. To go from automation to resilience, we must invest in rearchitecting our digital tools, so that they are a match for their increasingly critical mission.

From digital transformation to digital unification

In our view, digital transformation describes a journey; we envision the logical end of this journey: the *digital unification* of industrial infrastructures, where a complete transformation fully unleashes the benefits of computing technologies. Unification means that the transformation is performed using principled designs—developing a "narrow waist" of algorithmic techniques to manage these infrastructures and their nexuses. Existing physical infrastructures will remain largely unmodified and distinct (e.g., one for producing energy and another for pumping water), but we rearchitect the digital layer atop so that computationally, their management relies on shared software abstractions, primitives, and algorithms. The analogy is to an OS, where all popular operating systems have common concepts like processes, files, and sockets; and where the POSIX standard provides a degree of interoperability. By distilling the universal computational structures, we can navigate the design space to identify the best "OS" architecture, interfaces, and abstractions for infrastructure management; and to derive a greater level of portability across the infrastructure nexus. In other words, we propose to design *systems software* for industrial infrastructures.

Why should computing researchers care?

First and foremost, digital transformation/unification is a computing challenge! The computing community has decades of experience in the art of composition and modularity (successes *and* failures), from which to draw. In particular, we can learn much from the Internet—a successful example where shared computing abstractions (e.g., packets, IP addresses) have enabled the digital unification of disparate physical networks. Inspired by the Internet architecture, we sketch a stacked design with three loosely-couple layers, providing the abstractions, mechanisms, and policies for industrial infrastructures.

The first layer consists of a set of universal compute *abstractions* for infrastructures (e.g., devices, interconnections), hiding away the physical details. This layer offers a digital representation of how physical devices are interconnected and how services are derived from these infrastructures. We envision these abstractions to be associated with formal semantics, so that we can provid high assurance of management operations. These abstractions can also be "subclassed" to describe different scenarios—e.g., capturing the fact that some devices have trusted execution environments, whereas others are insecure IoT devices that cannot be patched, so that we will protect the deployment holistically. This library of abstractions will enable infrastructures to interoperate with each other—akin to the IP layer of the Internet, which transports data in the same format across distinct networks for global connectivity; in our case, we need to capture a more diverse range of services, not just networking but also compute, power, water, and more.

The second layer will develop the *mechanisms* for realizing these common abstractions, both for individual infrastructures and their nexuses. For example, at the power/water nexus, this layer would allow for the coordinated management of energy and water resources, optimizing their use in tandem rather than in isolation. To protect cross-domain collaboration, e.g., for data sharing or cross-infrastructure optimization, we need federation mechanisms that provide security and privacy, enabling different trust domains to work together. We draw an analogy to the BGP protocol for federating different networks, and envision a set of "infrastructure peering points" that transform the infrastructure nexus, from today's ad hoc interactions to secure protocols that, for instance, rely on cryptography and secure hardware. Accounting and accountability mechanisms will be needed to locate and attribute faults, and to produce digital evidence.

The top layer provides *policy* decisions to control the infrastructures for resilient service. For example, data analytics will optimize resource allocation across infrastructures, and machine learning will be used for predictive maintenance. Joint control enables novel use cases previously unattainable with isolated infrastructures—e.g., telco providers under high load might leverage an enterprise's private 5G network, in exchange for a discount on the enterprise's optical WAN connection; or they may route traffic away from metro areas experiencing grid overload, while choosing paths based on availability of low-carbon energy. These end-to-end services will unleash the full potential of digital unification—advancing the security, efficiency, and reliability of individual and interconnected infrastructures to achieve higher resilience.

How should we get there?

While we have outlined a computing-centric view, this challenge is multidisplinary in nature. The computing community needs to expand beyond traditional focuses, collaborating with researchers in infrastructure sectors—to better understand their domains, to showcase how computing advances in formal methods, machine learning, or secure execution can help; but also to identify the limitations of our tools, and devise new ones that will likely be required by the extreme scale and heterogeneity of infrastructures. Moreover, these techniques need to be designed with an eye on incremental deployment, so that they can support both "greenfield" and "brownfield" infrastructures, and digitalize existing and create new nexuses. Digital unification also a socio-technological problem, where standardization efforts are crucial and policy regulations and governance bodies play a key role. Fortunately, there are exciting trends that we can capitalize on. Cross-sector stakeholders (e.g., grid/datacenter, power/water providers) do not compete with each other, and collaboration could be mutually beneficial; in fact, many are already collaborating with each other [8, 9, 10], and these conversations will help identify new business models and incentives. Governance bodies (e.g., FERC) are passing infrastructure interoperability regulations. New infrastructures are being constructed frequently, able to incorporate novel techniques from the outset. These create the perfect timing to engage diverse stakeholders for the betterment of tomorrow's infrastructure.

A grand challenge with great payoffs

If we are successful in tackling this grand challenge, we will not only produce resilient infrastructures for our society and accelerate their digital transformation, but also develop novel computing techniques that address unprecedented scale and heterogeneity. We will be able to create a systematic interface between computing and engineering, establishing a new domain at their intersection.

References

[1] Critical infrastructure security and resilience. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.

[2] The AI data centers of the future. https://ifp.org/future-of-ai-compute/.

[3] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 2001.

[4] Lessons learned from the Texas blackouts: Research needs for a secure and resilient grid. https://www.nationalacademies.org/ocga/testimony-before-congress/lessons-learned-from-the-texas-blackouts-research-needs-for-a-secure-and-resilient-grid.

[5] Widespread IT outage due to crowdstrike update. https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update.

[6] Cyber-attack against Ukrainian critical infrastructure. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

[7] America's largest water utility hit by cyberattack at time of rising threats against U.S. infrastructure. https://www.cnbc.com/2024/10/08/american-water-largest-us-water-utility-cyberattack.html.

[8] National grid renewables signs power purchase agreement with Microsoft. https://nationalgridrenewables.com/press-release/national-grid-renewables-signs-power-purchase-agreement-with-microsoft/.

[9] Microsoft highlights innovation in power and utilities. https://www.microsoft.com/en-us/industry/blog/energy-and-resources/2023/05/04/microsoft-highlights-innovation-in-power-and-utilities/.

[10] New nuclear clean energy agreement with Kairos power. https://blog.google/outreach-initiatives/sustainability/google-kairos-power-nuclear-energy-agreement/.