Building on belief

Building 360-degree resilience in the utilities sector

Abstract

Utilities are the lifelines of social and economic activities. The vulnerabilities of utility infrastructures have been laid bare on several occasions in the recent years. Outages, caused by climate change driven extreme weather events and cyberattacks, disrupt normal day-to-day life at many levels. The onus to build resilience and fortify the critical physical and digital infrastructure in order to avoid and mitigate risk of damage, attacks, and consequent service shutdowns, rests on the service providers.

Utility service providers are increasingly leveraging technologies such as smart analytics, cloud, IoT, mobility solutions, artificial intelligence (AI) and machine learning (ML) at scale as well as enhanced cybersecurity tools and practices, to solve new challenges and mitigate impacts.

Utilities sector is the backbone for growth

The utilities sector has been at the core of successive industrial revolutions and burgeoning economic activities. Basic amenities including water, electricity, gas, and other energy and waste management services have powered economic growth and advancement across industries and communities. Damage to infrastructure supporting these amenities leads to the imminent disruption of crucial services, resulting in magnified outages and stifling key economic and life activities. For example, the economic reliance of modern-day society on electricity supply is so high, that an outage can cost millions of dollars to the economy. The United States Department of Electricity (DoE) estimates that outages are costing the U.S. economy $150 billion annually[1]. Safe to say that utility services are the lifelines that keep the modern economy going.

The case for building resilience

Maintaining modern, flexible, and secure networks of pipelines and grids that support transmission and distribution of electricity, oil, natural gas, and water are fundamental to delivering affordable and reliable services. Utility infrastructure in most developed geographies was built decades ago and requires expensive and continuous maintenance. For example, water distribution pipelines in the UK were laid decades ago. It is common for burst plumbing lines to be reported in winter every year when the water freezes in these old pipelines, requiring these water lines to be repaired and re-laid while continuing to extend the network to newer areas every year. While keeping the infrastructure going, it needs significant investments for modernization to address to growing needs of a 21st century economy. President Biden's recent unveiling of a $2-trillion plan to remodel and upgrade infrastructure in the USA[2] substantiates the imminence of the same.

[1] Bloom Energy; A Day Without Power: Outage Costs for Businesses; October 8, 2019; https://www.bloomenergy.com/blog/a-day-without-power-outage-costs-for-businesses

[2] The New York Times; Biden Details $2 Trillion Plan to Rebuild Infrastructure and Reshape the Economy; March 31, 2021; https://www.nytimes.com/2021/03/31/business/economy/biden-infrastructure-plan.html

Digital upgrades and imminent cybersecurity challenges

The utility industry is set for massive transformation by embracing digitalization of processes and operations. Utilities are investing in digital technologies to enhance reliability, safety and to meet evolving needs of modern-day customers. Digitalization, however, has brought with it increased exposure to cyberattacks in recent times. Malicious hackers are becoming more tenacious in their strikes on critical operational networks like the Colonial Pipeline fuel infrastructure.

The cyberattack on the Los Angeles Department of Water and Power in 2018[3] was one of the earliest indicators of vulnerabilities susceptible to cyberthreats in utility infrastructure. Subsequent attacks such as the SolarWinds one in 2020, trickled down to various levels of customers and infamously breached and exposed vast amounts of sensitive data[4]. In 2021, cyberthreat actors compromised platforms deployed by the Metropolitan Water District of Southern California and numerous government agencies by hacking the network's secure remote access[5]. Nearly $5 million was extracted as a ransom for the software decryption key required to unscramble the attack on the Colonial Pipeline in May 2021[6]. These cyberattacks leave states at the risk of dealing with contaminated water, gas line leakages, and other casualties. Naturally, systemic cybersecurity upgrades are in order. America's Water Infrastructure Act (AWIA)[7] of 2018 call for large water providers to conduct security risk assessments and incorporate their results into organizational cybersecurity policies. Other utility spaces are also expected to comply with similar regulatory measures that emphasize on active cybersecurity threat monitoring.

Replacement or removal of hardware for upgrades is an expensive exercise and involves extensive service outages. The challenge lies in mapping existing, decades-old infrastructure with appropriate, advanced cybersecurity solutions without making incremental changes which may elevate a network's vulnerability to cyberattacks.

Challenges posed by climate change

Much has been said and written about the impact of climate change and global warming on life and earth in recent years. Reports state that climate change could wipe off up to 18% of global economic gross domestic product (GDP) by 2050.[8] While these may appear as doomsday scenarios, the utilities and energy sector has been dealing with the increasing impact and frequency of natural disasters and extreme weather events such as hurricanes, typhoons, heat-waves, wild-fires, and storms.

Some recent instances include:

- Power outages in Texas owing to the 'Big Freeze' event in February 2021; the Electric Reliability Council of Texas (ERCOT) implemented rotating outages to keep the electrical grid from collapsing,

[3] Bloomberg; U.S. Water and Power Are Shockingly Vulnerable to Cyberhacks; June 12; 2021; https://www.bloomberg.com/news/articles/2021-06-12/u-s-water-and-power-are-shockingly-vulnerable-to-cyberhacks

[4] The New Yorker; After the SolarWinds Hack, We Have No Idea What Cyber Dangers We Face; January 25, 2021; https://www.newyorker.com/news/daily-comment/after-the-solarwinds-hack-we-have-no-idea-what-cyber-dangers-we-face

[5] Center for Strategic and International Studies; Significant Cyber Incidents; https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[6] The Guardian; Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack; May 20, 2021; https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom

[7] United States Environmental Protection Agency; America's Water Infrastructure Act of 2018 (AWIA); https://www.epa.gov/ground-water-and-drinking-water/americas-water-infrastructure-act-2018-awia

[8] The World Economic Forum; This is how climate change could impact the global economy; June 28, 2021; https://www.weforum.org/agenda/2021/06/impact-climate-change-global-gdp/

leaving millions of Texans without power for days. Residential heating shortages, burst pipes, and water treatment plant failures resulted from the impending crisis[9].

- Power, water, and gas outages caused by torrential rainfall-induced floods and landslides in parts of Germany, Belgium, Austria, and the Netherlands in July 2021[10].
- California's first rolling blackouts in 19 years, caused by extreme heat and high demand[11].
- As the California situation has shown, the power sector is at a tremendous risk due to wildfires – at being both, susceptible to and be the cause of such wildfires.

Arson and acts of terrorism targeting utility infrastructure

On the other hand, physical attacks on utility infrastructure caused by arson and acts of terrorism, are becoming increasingly frequent. Many countries are actively developing strategies to plan and support efforts to safeguard critical infrastructures such as power, water, and telecommunications against potential attacks[12]. To ensure good governance and secure upkeep of the state economy, retain public confidence and ensure safety, critical infrastructure owners and operators are being urged to assess potential vulnerabilities and consciously invest in enhancing their security posture.

To avert and mitigate the impact of risks and resultant shutdowns of services on communities and enterprises, organizations running critical services must build resilience in both their physical and digital infrastructure.

Technological solutions to leverage

With climate emergencies amplifying the level of threats as well as impact, players in the utility sector are shifting to more resilient strategies. The pandemic has turned the spotlight on the necessity of building resilience for utility companies and has driven home the need to embrace digitalization.

Leveraging digital tools in combination with state policies and best practices can help better predict and mitigate the extent of the impact of extreme weather events as well as aid in faster recovery after the event passes. Advanced technologies including AI/ML, IoT, and cloud-first solutions can help simulate and assess the level of preparedness for threats in a controlled, virtual environment. Such simulations aid the identification of vulnerabilities within the infrastructure, which could be remediated appropriately.

Modern technological solutions can be built to effectively achieve real-time monitoring and maintenance measures. With capabilities such as optical character recognition (OCR) and intelligent character recognition (ICR), image and text processing can be digitalized, and data entry of information such as infrastructure asset details can be automated. Satellite imaging is another safe and terrain-independent solution that aids round-the-clock surveillance of utility infrastructure as well as vegetation and weather. Further possibilities of tech-enabled maintenance solutions encompass:

[9] Utility Dive; The Texas Big Freeze: How a changing climate pushed the state's power grid to the brink; June 2, 2021; https://www.utilitydive.com/news/the-texas-big-freeze-how-a-changing-climate-pushed-the-states-power-grid/601098/

[10] Intelligencer: Scenes of Devastation After Deadly Floods in Germany and Belgium; July 18, 2021; https://nymag.com/intelligencer/2021/07/devastating-scenes-after-deadly-floods-in-germany-belgium.html

[11] Politico; California has first rolling blackouts in 19 years – and everyone faces blame; August 2020; https://www.politico.com/states/california/story/2020/08/18/california-has-first-rolling-blackouts-in-19-years-and-everyone-faces-blame-1309757

[12] The White House; The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets; February 2003 https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

- Using drones, unmanned aerial vehicles (UAVs), vehicle-mounted cameras for quick and enhanced field data collection
- Deploying high-definition pan-tilt-zoom (PTZ) cameras for fire ignition hazard monitoring and surveillance of utility assets and premises
- Leveraging machine vision technology (MVT) to expedite processes such as asset inspections and vegetation management
- Using state-of-art digital technologies to manage emergency events

Digitally enabled smart solutions can endow susceptible infrastructure elements with a greater degree of resilience. Some of these solutions are preventive while others focus on consistent maintenance and monitoring. A prospective slew of digitally enhanced preventive measures include:

- Infrastructure hardening - preventive measures such as covered conductors and undergrounding of lines can be accomplished with the aid of automated remote monitoring, digital sensors and meters, and other intelligent devices.
- Enhanced vegetation management - bespoke solutions software, automation, drone-based monitoring in combination with utility staff coordination can efficiently mitigate risk to electrical infrastructure.
- Deploying assorted weather sensors and weather stations - IoT-based weather monitoring systems can monitor the weather conditions at a given place; can be leveraged to forecast, plan and prepare in advance for, or even alleviate imminent weather-induced casualties.
- Setting up dedicated operations centers - AI-driven applications and solutions can enhance operational efficiencies in several key areas such as predictive maintenance, load forecasting/ optimization, grid reliability, energy theft prevention, and renewable resource optimization for wildfire safety, storm response, and other emergencies.
- Leveraging AI/ML technology and real-time inputs - accurate field data on weather and vegetation can be leveraged to streamline risk-based modeling of infrastructure utility assets.
- Enhanced cybersecurity threat monitoring - pre-built assessment frameworks and aligned services to achieve enterprise-level services for vulnerability management and application security driven by automated scanning, remediation tracking, actionable reporting, and triaging of vulnerabilities.

Advanced digital technologies to the rescue

Players in the utility sector are faced with challenges at multiple levels as developed and developing economies continue to depend on decades-old infrastructure for their basic operational needs. Measures for mitigating risks imposed by global warming, infrastructural wear-and-tear, vegetation, deliberate physical and cyberattacks, etc., call for building layered resilience across operations.

Advanced digital technologies have proven to be useful in monitoring and supporting large-scale utility operations that span complex installations. This can be further leveraged to maintain holistic coordination across overlapping processes and functionalities. Powered by AI, cloud, and ML, digital tech can build the trust that operators, engineers, and stakeholders need to address urgent issues efficiently. Concerted digital systems may hold the key to enabling 360 degree situational awareness to detect, predict and solve issues as critical as an entire city’s water, gas and electric supply.

About the author

Ranjeet Vaishnav

Ranjeet Vaishnav leads the advisory function for Electric Transmission & Distribution Sector at TCS. He works with utility companies to help them navigate disruptions caused by the energy revolution and by digital technologies. Ranjeet has been in the industry for over 25 years and carries a rich and diverse experience of working with power sector organizations in India and North America.

TATA CONSULTANCY SERVICES

Awards and accolades

#1 IN CUSTOMER SATISFACTION
2020/21 EUROPE
Whitelane Research
top EMPLOYER NORTH AMERICA 2021
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS
top EMPLOYER GLOBAL 2020
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS
ASIA'S OUTSTANDING COMPANIES POLL 2020
ASIAMONEY
STEVIES 2020
CONGRATULATIONS CIO100 WINNERS 2020
FinanceAsia ASIA'S BEST COMPANIES 2020
DIGITAL IMPACT AWARDS WINNER
CANADIAN HR AWARDS 2020
THE CIVIC 50
FTSE4Good
CDP
DISCLOSURE INSIGHT ACTION
2020 Brand Finance® Awards
TOP 3 IT SERVICES BRAND
2020 Brand Finance® Awards
FASTEST GROWING IT SERVICES BRAND FOR THE DECADE 2010 - 2020
AWARDED Superbrands BRITAIN'S CHOICE 2020
AWARDED Superbrands AMERICA'S CHOICE 2020

Contact

Visit the Energy, Resources & Utilities page on https://www.tcs.com

Email: utilities.marketing@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS_News.**

All content/information present here is the exclusive property of Tata Consultancy Services Limited (TCS). The content/information contained here is correct at the time of publishing. No material from here may be copied, modified, reproduced, republished, uploaded, transmitted, posted or distributed in any form without prior written permission from TCS. Unauthorized use of the content/information appearing here may violate copyright, trademark and other applicable laws, and could result in criminal or civil penalties.

Corporate Marketing | Design Services | M | 11 | 21