Ground Control

Infrastructure, Security and Storms: Challenges and Opportunities for Utilities and Renewables

Introduction

It's a challenging time to be a Utility provider. Where once there was predictability, there is now uncertainty. Consider the climate: whether you consider the issue to be human-exacerbated or not, the fact is, temperatures are rising, which places greater strain on the grid as people seek to cool their homes and premises down. Further, extreme weather events are increasing, impacting power lines and towers, and the communication networks that help Utilities companies find and identify the issue.

There's also the growing threat around cyber security. With the Colonial pipeline incident fresh in consumers' memories, 44% of respondents to our recent survey of US homeowners said that they considered hackers to present a threat to their Utilities supply, and 44% would switch Utilities provider for one in whom they had greater confidence that they were able to limit outages.

Related to this is the challenge of ageing infrastructure. With the sunsetting of 2G and 3G networks impacting telemetry and control, Utilities providers need to explore new means of securely collecting data for their SCADA systems - not least so that when the worst happens, any outages are identified and tackled quickly.

In this eBook we're going to explore these issues and what the general public think about the state of Utilities in the USA today. We'll then look at some of the considerations Utilities companies need to make to shore up their adaptability.

Challenges facing Utilities and Renewables

Security

According to IBM, in 2021, data breach costs rose from USD 3.86 million per incident to 4.24 million, the highest average total cost in the 17-year history of their annual report.

These costs were not attributed exclusively to the cost of exposure, but also included the expenses of discovering and responding to the breach, the cost of downtime and loss in revenue, and, more challenging to calculate, the long-term reputational damage to a business and its brand. Indeed, there's potential threat impact across the whole value chain.

In Utilities, the main issue is the extraction of data from Remote Terminal Units (RTUs) to companies' SCADA systems. But this vulnerability is not, according to some analysts, getting the attention it warrants from Utilities companies:

> *"…the digital security of U.S. computer networks controlling the machines that produce and distribute water and power is woefully inadequate, a low priority for operators and regulators, posing a terrifying national threat."*

90% of customers had "extremely limited to no visibility" inside their industrial control systems. [Dragos report, 2020] This means that once a hacker has breached a Utility company's defenses, there is nothing preventing them from collecting sensitive data, exploring your system configuration, and planning the best time to attack your systems.

Ageing Infrastructure

The average age of the electric transmission infrastructure in the United States is forty years old, with more than a quarter of the grid fifty years old or older.

In 2015, the US Department of Energy reported that:

70%
of power transformers are **25+ years old**

60%
of circuit breakers are **30+ years old**

70%
of transmission lines are **25+ years old**

Is it any wonder that system operation failures are the second most common cause of outages?

A $1.2 trillion infrastructure bill was recently passed to address, amongst other things, energy infrastructure. Clearly, the industry and regulators have taken note that infrastructure is a priority. However, there is still a sizable gap between what has been upgraded and what needs to be done.

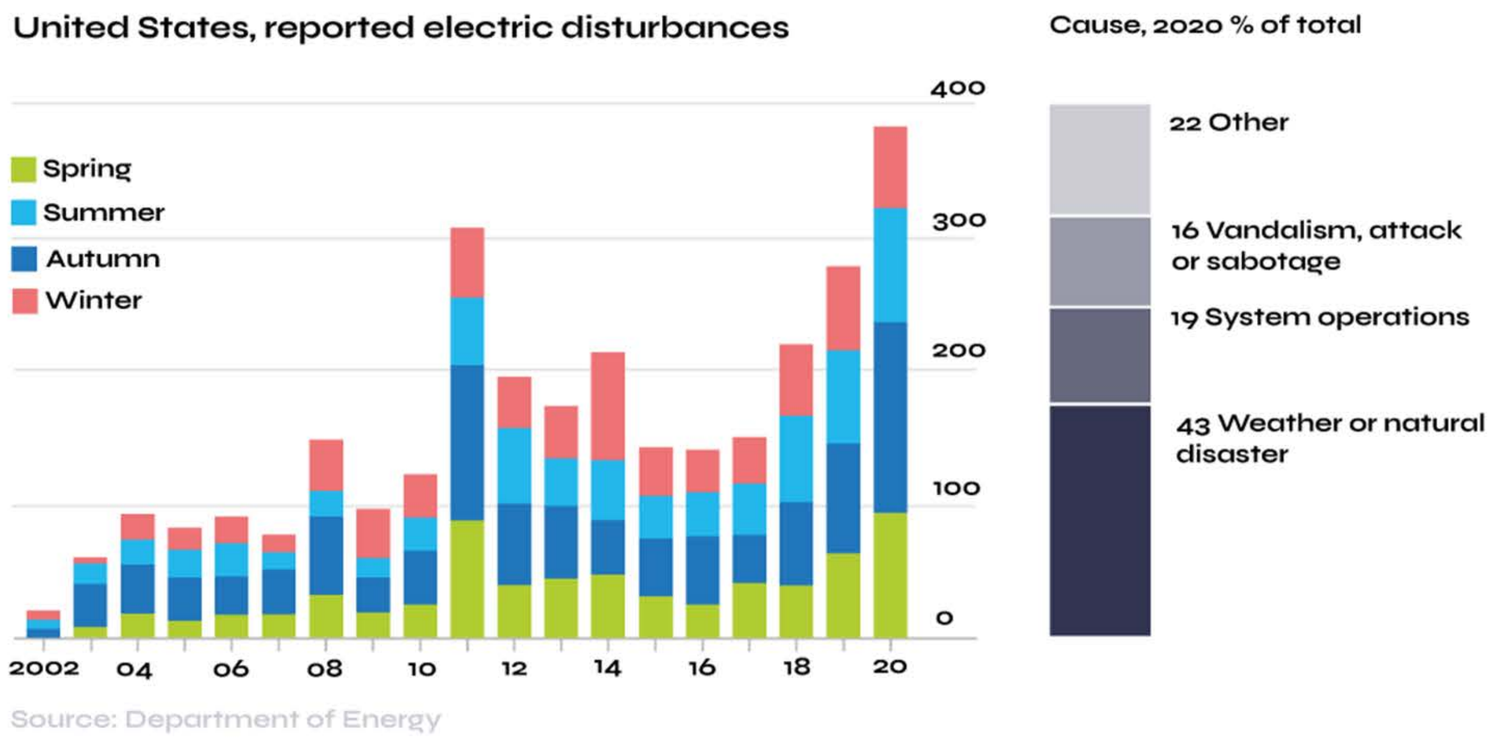
According to the American Society of Civil Engineers, if current trends continue, the gap between what is needed and the funding actually provided will be $208 billion by 2029, and $338 billion by 2039.

But with 72% of US customers served by for-profit, investor-owned Utilities companies, the burden of investment falls upon the private sector rather than the government.

Climate change

The Fourth National Climate Assessment, released in late 2018, stated that climate change was already having noticeable effects in the United States and predicted "more frequent and intense extreme weather and climate-related events," such as floods and hurricanes. For Utilities, the assessment concluded, the possibilities were grave: lower efficiency, higher expenses, and more power outages—even as demand for energy rises.

And many Utility companies are not ready. As the assessment noted, "Infrastructure currently designed for historical climate conditions is more vulnerable to future weather extremes and climate change."



Source: Department of Energy

But as the above chart shows, weather conditions are not exclusively to blame for power outages, with 19% of outages due to failures in system operations, and 16% due to vandalism, attack or sabotage.

The total cost of these power outages to the US economy was estimated at $150 billion annually in 2019.

Overcoming the Challenges

The customer's perspective

Utility organizations need robust programs and projects that address these challenges across the complete enterprise. This means that programs and projects may be sponsored by other business areas, and will most certainly involve cross-department, and even inter-company participation and collaboration to be successful.

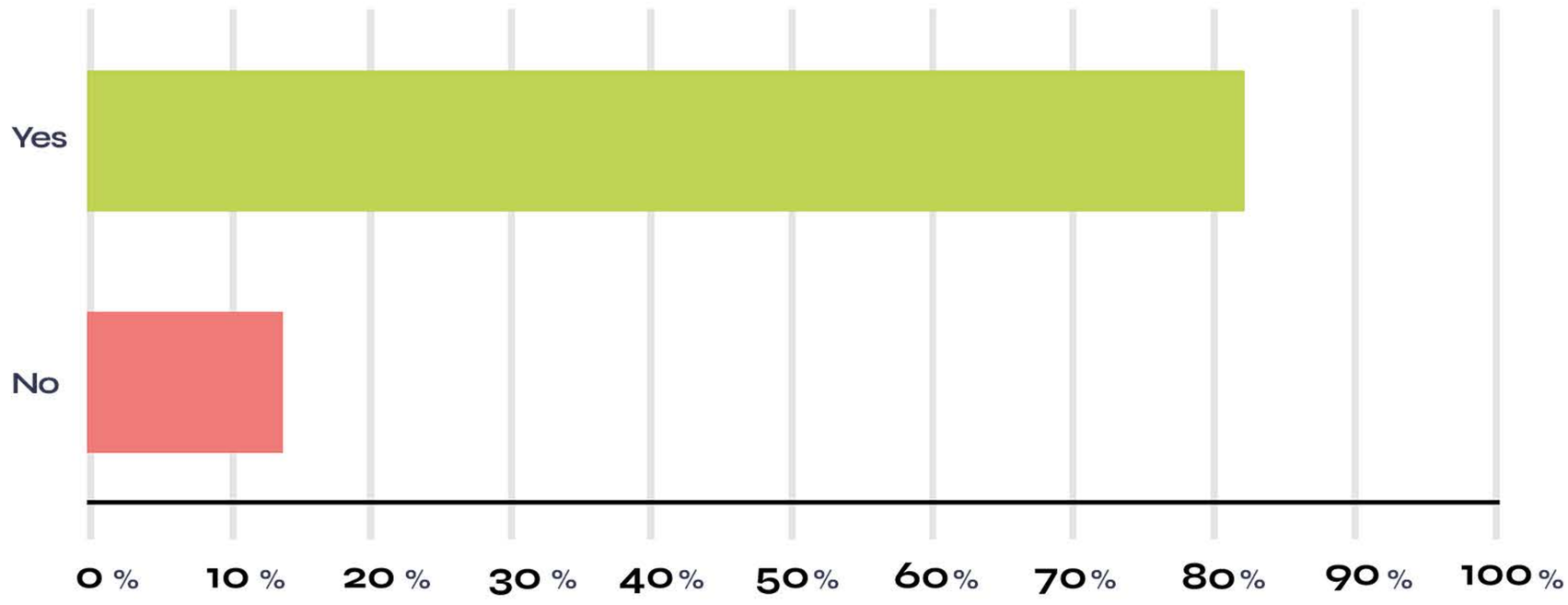
The challenges can be overcome, but will be restricted by both time and money. Even without all the regulations in the Utilities market, the capital required to address the programs and projects, together, at any given time, wouldn't be attainable. In addition, the workforces are aging and retiring and skilled workers are not always plentiful. Faced with limited or restricted capital and limited skilled resource, in addition to the high demand for modernization of aging infrastructure and enhanced security requirements; it's critical Utilities ask the right questions, and make the right choices.

Utility customers also have a voice in amongst the corporate and macro challenges, and provide interesting insight into the service received and priorities, service levels and expectations from Utility providers. Commissioned by Ground Control, our survey highlights interesting trends and outcomes.

A customer's point of view - the state of utilities in the USA

1,050 Utility customers based in the USA participated in a survey about the state of utilities in February 2022. A number of questions were posed about the customer service, reliability and outages to energy supply. Here are some of the highlights.

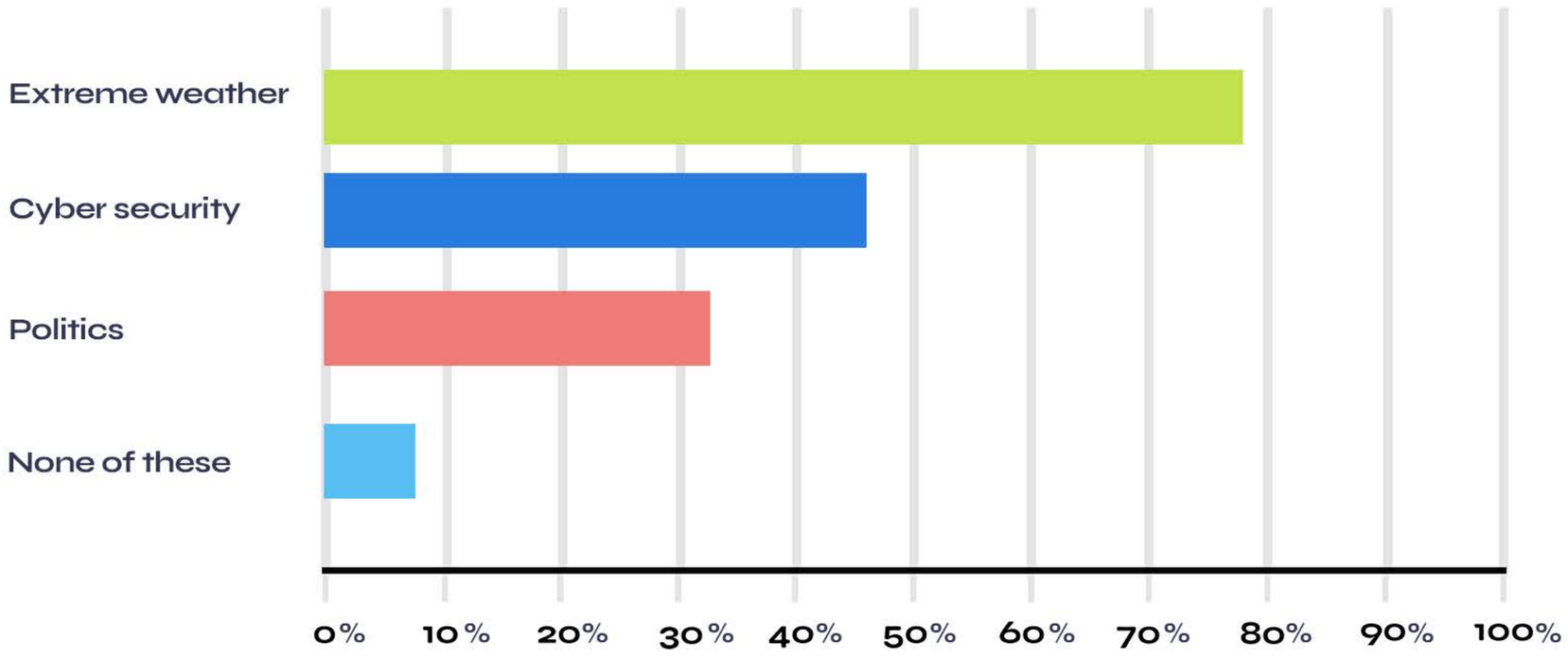
Have you ever experienced any service interuptions (outages) with your electricity, gas or water supply?



81% of survey respondents reported having experienced outages in their Utilities supply, and a further 30% said that these outages had grown in number in the last ten years. This echoes the trends in the Department of Energy data we saw earlier.

A customer's point of view - the state of utilities in the USA

Do you consider any of the following to be a threat to your Utilities supply? You can select multiple options.



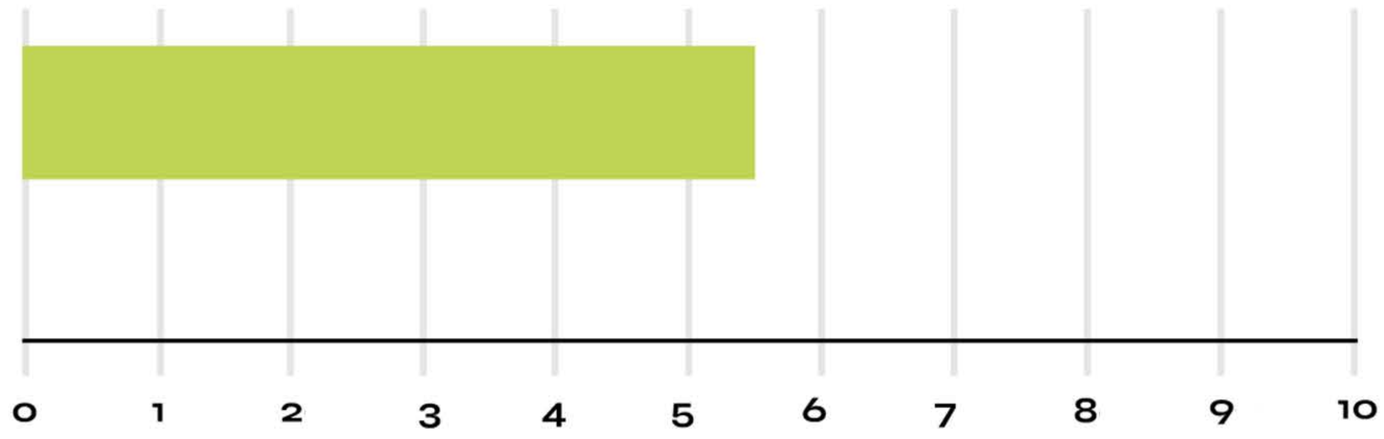
79% of respondents felt that extreme weather events presented a threat to their Utilities supply, and 44% felt that hackers were a threat to their energy supply.

This relatively high response is possibly due to the high profile attack on the Colonial Pipeline. Interestingly, those with a household income between $100,000 - $200,000 were, above all else, concerned by cyber security and hackers bringing down internal Utility systems.

A smaller number of respondents (31%) saw political unrest as being a threat, but only 7% of respondents saw no threats on the horizon to their Utilities supply.

How prepared do you think your Utility suppliers are to manage any of the above risks?

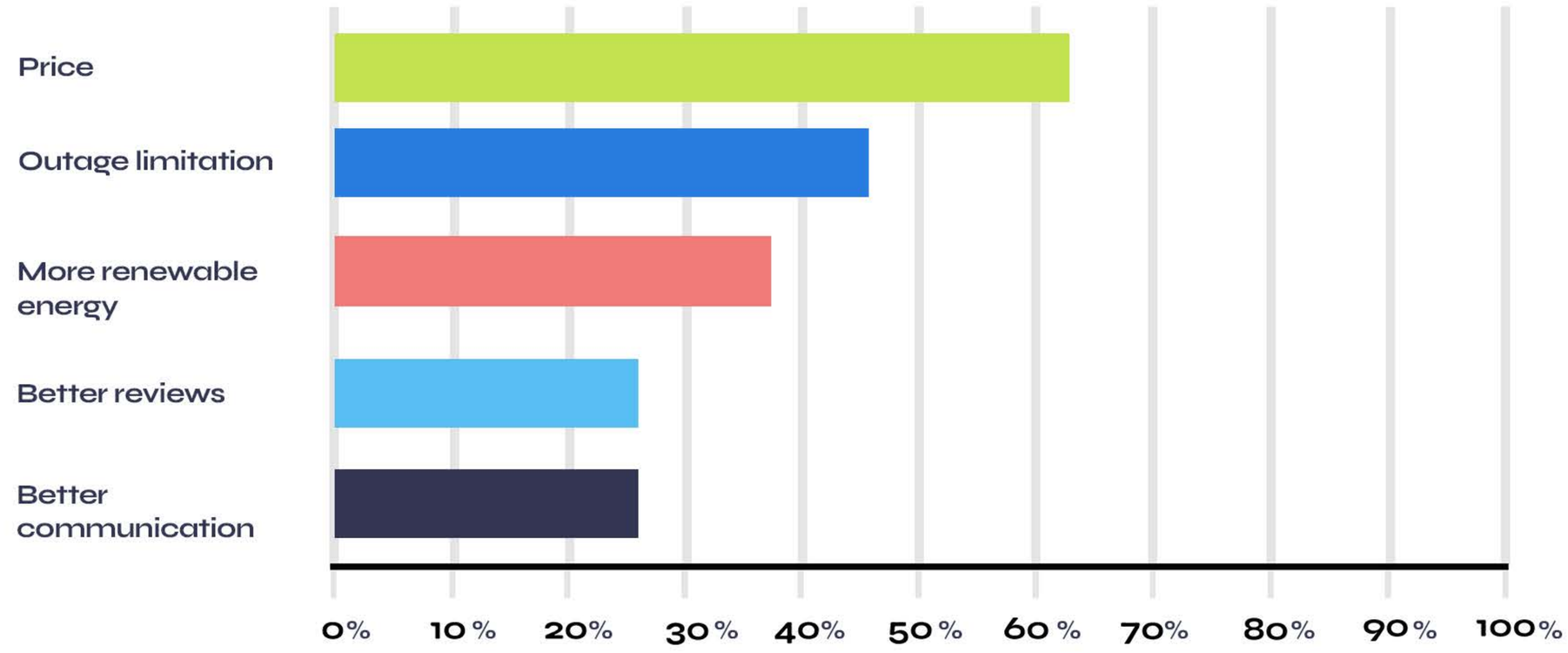
Average out of 10



Prevention is often better than cure. However, our survey respondents are not confident in their Utility providers' ability to prevent outages. Only 11% of respondents felt that their Utility company is well equipped to deal with risks to their energy supply. There is clearly a gap to improve risk management and a long way to go to improve consumer confidence in avoiding outages and supply disruption.

A customer's point of view - the state of utilities in the USA

What would prompt you to change supplier?
Please select all that apply.



Ultimately, consumers can most influence Utility providers by their buying behavior, so it's interesting to note that 44% of respondents would change their Utility provider if they were presented with an alternative provider who gave them greater confidence in their ability to limit outages.

That number climbs to 52% for consumers aged between 18 and 29, suggesting that younger customers find this more important than older customers.

39% of consumers would switch for more renewable energy sources, and, not unsurprisingly, 63% would switch for a lower price. With most customers believing that outages are caused by extreme weather and poor security, in order to retain and grow their customer base, Utilities companies need to both have a plan to limit outages, and be able to clearly articulate that plan to retain and grow their customer base.

While weather conditions are outside of a Utility company's control, cyber security is not, and so our key takeaway from this is that forward-thinking Utility companies should dedicate some resources to improving this element of their offering.

Cyber Security

Cyber security threats and the utility industry

For the Utilities and renewables industries, the remote site environments and silo operation sites make a tempting target for cyber crime.

Notably, in 2021, a ransomware group known as DarkSide attacked Colonial Pipeline - a large US refined products pipeline system. They hacked in via a Virtual Private Network (VPN) and the group gained access to the company's networks and caused malicious disruption to pipeline operations. In effect, DarkSide shut down the essential pipeline that carries 45% of the gas, diesel and jet fuel supplied to the US east coast. It was a massive problem for customers, employees and stakeholders alike. DarkSide held Colonial Pipeline to a USD 5 million ransom, which was paid by the CEO.

This is just one example but there are numerous examples of successful cyber attacks which have left organizations without control of their own operations and in many cases, great loss of revenue and ransom amounting to millions of dollars.

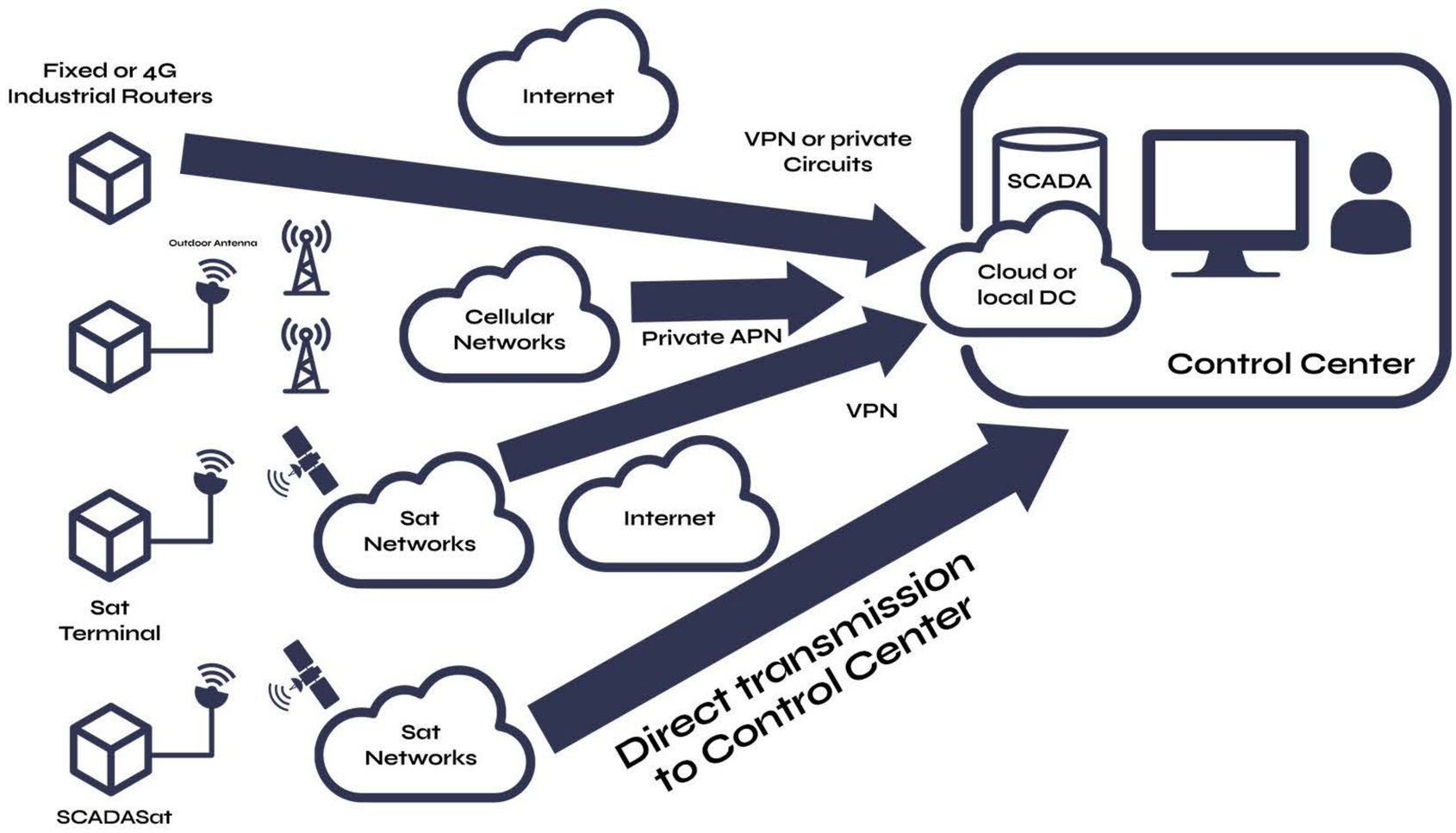
But a 2020 report from McKinsey found room for optimism:

"Electric-power and gas companies are especially vulnerable to cyberattacks, but a structured approach that applies communication, organizational, and process frameworks can significantly reduce cyber-related risks." McKinsey, 2020

To improve overall grid security, Utilities need to implement reliable communication and cyber security solutions for their remote power generation and power substation facilities.

Cyber security threats and the utility industry

As touched upon earlier, a key data transfer requirement, with an associated data security vulnerability, exists between RTUs and your SCADA system. Extracting this sensor data, however remote, is critical to the prevention and mitigation of outages, and there are several options available as the diagram below shows:



Internet

Utility providers can connect their multi-site, remote operations via fixed and traditional broadband or fiber internet. Broadband digital connections are highly reliable, with fewer breaks and the transmission is fast. The ability to link multiple users at any one time, with no cut-offs or time-outs, coupled with an 'always on' connection makes for a very stable and reliable means to connect Utility sites. However, the 'always on' nature can mean that security can be comprised more readily due to the constant and continuous online status.

Cyber security threats and the utility industry

Cellular networks

Cellular networks are the most commonly used form of connectivity due to the expanse and very nature of silo Utility sites, often miles from each other and any fixed infrastructure. The development of 5G has also increased the speed of these cellular networks. In areas such as offshore wind farms and rural inland sites where cables cannot be laid, cellular is often an alternative solution but it is not without its vulnerabilities. Wireless communication can be influenced by physical obstructions, climate conditions and interference from other mobile, wireless devices. As the communication is over the air, there are also security vulnerabilities.

Satellite networks

Some satellite networks have the advantage of not needing any terrestrial infrastructure in order to extract data from your RTUs' location to your SCADA system - so if your wind farm, reservoir or pipeline doesn't receive reliable cellular coverage, satellite is an increasingly cost-effective option, either as primary or failover. Satellite networks use public infrastructure in the transmission of data from the ground station to your premises, which travels via the internet, usually protected by VPN and/or firewalls. In some cases, there is the option of renting a private line, which avoids utilizing the internet.

Private satellite network

A private satellite network, by very virtue, is intrinsically different to both internet and cellular networks, and 'standard' satellite networks - all of which have some reliance on public infrastructure - in that it is highly secure and an entirely privately owned connectivity solution. The end-to-end private network is highly scalable for multiple devices and with exceptionally reliable up-time, without the interference of other devices or impacted by adverse, extreme weather conditions. SCADAsat is a private satellite network that works without any third party ground sites or data hubs, to connect remote Utility sites.

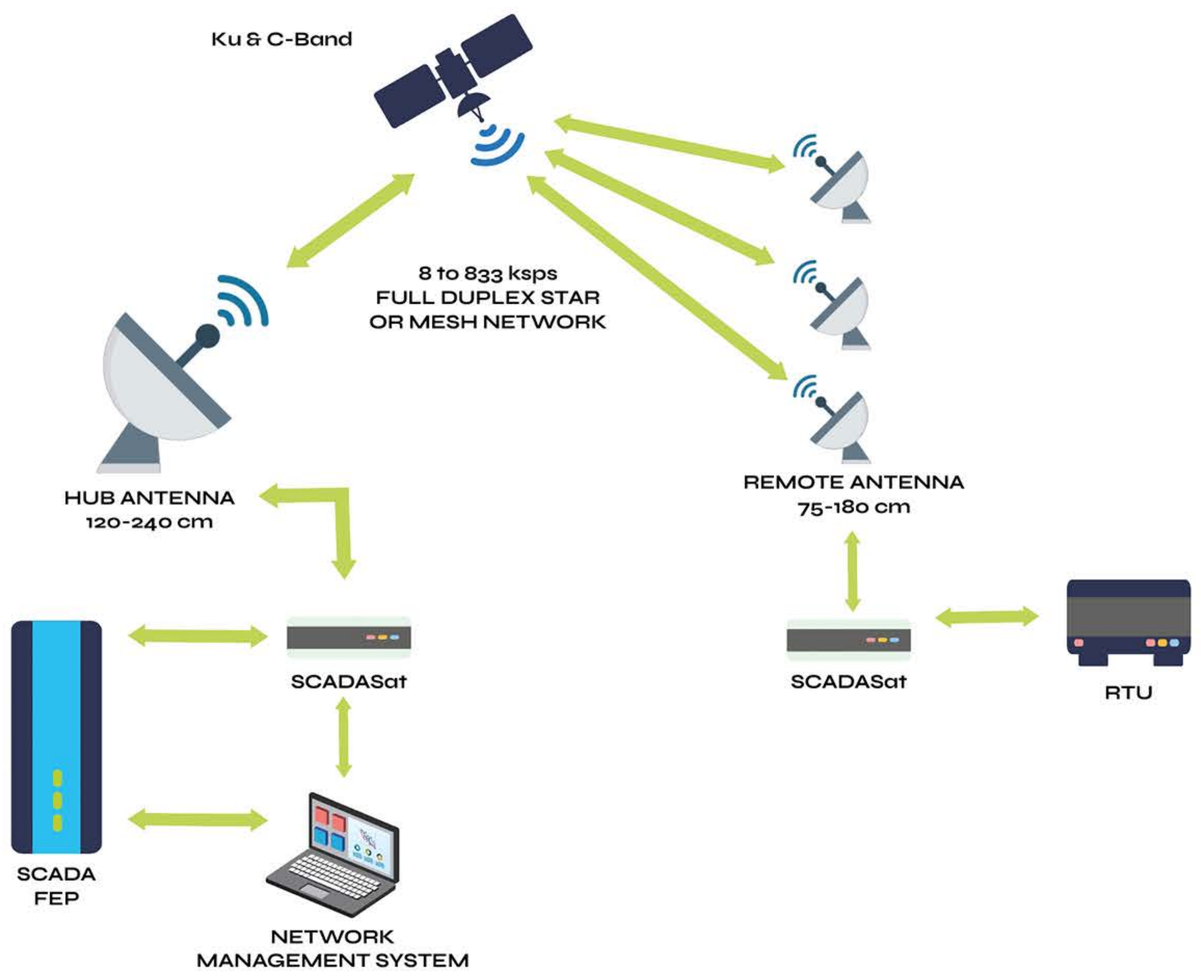
SCADASat

Using satellite communications to reduce the cyber security threat to renewable and utility data

The SCADASat solution provides high reliability and improves cyber security. It allows SCADA and Utility organizations to transmit their data while keeping it safe from cyber attack. It also extends secure networks for oil and gas, power Utilities and water management systems.

The solution is specifically designed to handle mission critical applications such as SCADA, M2M and Telemetry in the energy and utility markets. The rugged SCADASat hardware is engineered to provide years of reliable operation in remote locations and harsh environments. It is also designed to comply with IEC-61850 - the global standard for Utility and industrial communication and automation.

Completely independent from public infrastructure and the internet, SCADASat provides cyber secure and reliable communications for all Utility and renewables applications, and throughout the value chain. To further improve reliability, it is possible to install a load-sharing and geo-redundant HUB solution.



But what about the costs? The SCADASat HUB is the lowest cost VSAT HUB on the market. By efficiently using the satellite spectrum, and tailoring satellite bandwidth to the actual application needs, the annual communication cost is reduced to a minimum. This makes SCADASat the ideal solution to replace expensive leased equipment, or as back-up for existing terrestrial communications.

Why install SCADASat as a cyber security solution?

'53 percent of cyber attacks resulted in damages of $500,000 or more' Cisco Systems Inc, 2022.

The benefits of SCADASat are broad. Utility providers can benefit from integrating satellite communications with terrestrial communications solutions to obtain environmental monitoring data with both maximum security capabilities and maximum uptime. Primarily, SCADASat delivers three key features:

Reducing recurring costs - SCADASat enables tailoring of satellite bandwidth to actual application throughout requirements. The SCADASat flat-fee subscription model makes it an affordable solution.

Improving cyber security - SCADASat is implemented as a private network solution and is not connected to the internet, thereby improving the cyber security of the environmental monitoring assets.

Maximizing uptime - To ensure no gaps in the data collection, SCADASat networks can be easily implemented with geo-redundant and load-sharing HUB systems.

The SCADASat system, which runs on a private network, low bandwidth satellite system, is the ideal solution for organizations that require high reliability and security of data for mission critical applications and infrastructure.

As a Utility and renewable energy company, throughput requirements are both frequent and limited in size, but high security is key. SCADASat has a number of features to ensure an organization's data traffic remains their own.

Why install SCADASat as a cyber security solution?

Key features and security enhancements include, but are not limited to:

- Runs runs independently from third party hubs and from public infrastructure such as the internet
- Option of 256 AES Encryption
- VLAN functionality for logical separation of network traffic types on same physical network
- An ongoing number of new cyber security enhancements such as System level and user access authentication, NMS/IDU interface encryption and NAT/DHCP implementation
- Increase of max data rate across satellite channel to 768 kbps.
- New Hub/Air interface

SCADASat can also be effective in a number of different configurations:

- Point to Point - stand alone, single sits communicating to one another
- STAR - spoke design where all data returns to a central HUB
- MESH - a multi point to point network with remote sites, directly connected to one another with a centralized HUB being used for management and control

Summary

Summary

In summary, the industry is currently facing multiple challenges. To thrive amid these challenges, the Utility provider of the future needs to be a fully “digital system”: connected, collaborating, and responding. This isn’t easy in an Utility business that includes legacy infrastructure that may be as old as the industry itself. Solving these challenges is also restricted by time and money but changes can be made in a pragmatic and planned approach to ensure the robustness of services to customers and the assurance of high security.

Utility and renewable companies are exposed and at risk of expensive and disruptive cyber attack throughout their value chain due to the geographical spread and silo operation sites. However, organizations can significantly reduce the success of cyber attacks with an effective cybersecurity system - such as the SCADASat solution. This scalable, configurable and cost effective satellite based solution prevents cyber attacks by using private networks, high level encryption and IEC-61850 standard compliant technology for Utility and industrial communication and automation.

The threats to Utilities have been realized many times, with multi-million dollar settlements paid as ransom from some of the largest energy companies. However, proactive cyber security policy, best practice and the adoption of satellite enhanced security solutions - such as SCADASat will reduce and mitigate attacks on these otherwise at-risk organizations.

Who are Ground Control?

Ground Control was launched when three leading brands united to create a best-of- breed technology and service provider in satellite and IoT.

We provide customers with a remote critical communications solution, through a comprehensive range of satellite and cellular connectivity options whether in flight, on land or at sea. We deploy leading IoT technology to enable you to track and protect your valued assets, including fleet, plant, and people.

We recognize that rapid responses and optimal decision making rely on accurate and real-time data. Our data suite ensures information is securely delivered, and easily accessible for alerts and analysis.

Our mission is nothing less than to provide you with complete connectivity and control.

Sources:

https://www.aljazeera.com/economy/2021/6/14/recent-cyber-attacks-reveal-us-utilities-extreme-vulnerability

https://www.powermag.com/three-things-utility-companies-need-to-do-to-prevent-the-next-cyberattack/

https://www.mckinsey.com/business-functions/risk-and-resil-

ience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

https://www.itpro.co.uk/security/cyber-attacks/361142/why-is-the-energy-sector-so-vulnerable-to-hacking

https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf

https://securityintelligence.com/articles/energy-utility-data-breaches-2021/

https://tsat.net/tsat-satellite-backhaul-for-industrial-iot-devices/

https://www.bloomberg.com/news/articles/2021-05-08/colonial-is-just-the-latest-energy-asset-hit-by-cyberattacks

https://purplesec.us/prevent-cyber-attacks/#Data

https://systemexperts.com/compliance/

https://www.dragos.com/blog/industry-news/cyber-threats-to-global-electric-sector-on-the-rise/

Ground Control

Thanks for reading!

www.groundcontrol.com

sales@groundcontrol.com

USA: 800 773 7168

UK: +44 (0) 1452 751940