INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

TEXAS CRITICAL INFRASTRUCTURE SUPPLY CHAIN PROTECTION

REACHING THE ENERGY INDUSTRY

Institute for Homeland Security

Sam Houston State University

Scott Lynn

September 6, 2022

Table of Contents

INTRODUCTION

The Homeland Security Institute of Sam Houston State University commissioned this paper as part of a series of papers regarding to help in marketing the need for Supply Chain *Preparation, Response, Resilience and Recovery* to the four Texas Critical Industries (Health Care, Energy, Chemical and Transportation).

Supply chain disruptions will occur – it is not a question of "if" but "when." They may come from natural disasters, industrial accidents, internal or external attackers, but they will come. Preparing for them is the best way to help Texas Critical Infrastructure stay online, in business and prepared to serve the people of the state.

The purpose is to identify:

1) Energy supply chain requirements.
2) Potential supply chain threats affecting power plants and electrical distribution.
3) What Texas energy business sectors are "Critical Infrastructure.
4) Approximately how many power plants and distribution entities of various sizes exist in Texas
5) Ways to plan for Supply Chain Disruptions.
6) Existing resources available to the energy industry for supply chain protection.

Having identified the above, CI protection materials should be able to be prepared that focus on the needs of small vs. large companies, knowing those may be different.

Note that this document does not focuses extensively on internet or information-related vulnerabilities. They will be mentioned but the full breadth of that threat is beyond the scope of this paper.

ENERGY SUPPLY CHAINS

A useful definition of supply chain is a "linked set of resources and processes… …that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. [1]

In this document, the supply chain description differs from typical supply chains in that typical supply include products being delivered to end users. In this document, while the energy is the end-product, the supply chain will include not only the energy but all aspects of the means to deliver it – refineries, power plants, transmission and control systems, etc.

In the energy world, supply chains emphasize continuous reliability, so the discussion will also include the effect of demand, information exchange and how the effect market conditions have on reliability.

Energy Supply Chain Requirements

Fundamentally all, energy supply chains require the ability to acquire fuel, convert it to useful energy and reliably deliver it to customers. Each aspect of the chain has specific items required for proper operation. Most rely on other Texas Critical Infrastructure (CI) in order to function.

Following is a list of some energy supply chain requirements. To illustrate the interconnectedness of the energy supply chain, the table also lists other Critical Industries required for to supply the item on the left.

		General	*Critical Industry In Supply Chain*		
Item Required in Supply Chain	Type	Use	Energy	Chemical	Transportation
Fuel (NG, Coal)	Fuel	Fuel	x	x	x
Fuel supply distribution	Fuel	Fuel	x		x
Wind (Wind power)	Fuel	Fuel			
Solar Energy	Fuel	Fuel	x		
Water (Hydroelectric)	Fuel	Fuel			x
Fuel storage	Fuel	Fuel			x
Generating equipment	Equipment	Generation	x	x	x
Cooling (Thermal Plants)	Equipment	Generation	x		
Control Systems	Equipment	Generation	x		
Maintenance & Repair	Equipment	Generation	x	x	x
Load stability	Infrastructure	Distribution	x		
High voltage distribution	Infrastructure	Distribution	x		
Substations	Infrastructure	Distribution	x		x
Low voltage distribution	Infrastructure	Distribution	x		
NG Distribution	Infrastructure	Distribution	x		x

[1] Risk Management Framework for Information Systems and Organizations; A System Life Cycle Approach for Security and Privacy, National Institute of Standards and Technology Special Publication 800-37 Revision 2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Electricity distribution

Below is a simple illustration of the electricity supply chain, showing principal components, including:

- Power generation
- Step-up (High voltage) transformers
  - Monitoring and controls
- High voltage power lines
- Substations
- Transformers
  - Monitoring and controls
- Low voltage power lines

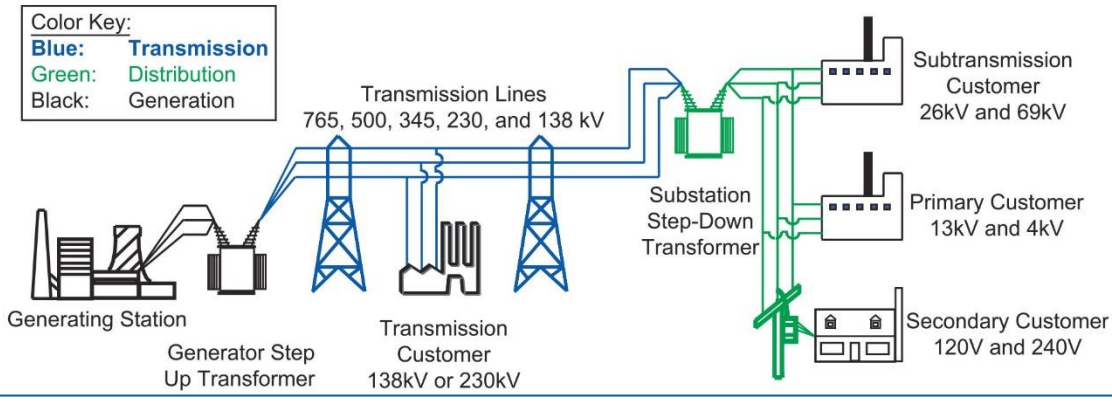


Figure 1 NPS.govElectric Transmission & Distribution, Electrical Power Transmission and Distribution
https://www.nps.gov/subjects/renewableenergy/images/transmission_original.jpg

Not shown is (for fossil fuel-based systems):

- Fuel supply
  - Mining / drilling
  - Refining
  - Delivery

Note that solar and wind power plants do not require the fuel supply infrastructure of fossil-fuel systems. However, the cyclic and unstable nature of solar and wind energy requires one of several methods of supplying power stability. These can include:

Battery storage:	Using backup batteries, typically distributed among end users or at network nodes.
Auxiliary power generation:	Possibly including fossil fuel plants, hydroelectric power, pumped hydroelectric, or other methods.
Large networks:	On the theory that a loss of energy (at night for solar or in low-wind conditions for wind) might be offset with wind or other renewable power types available across the larger grid.

Natural Gas Distribution

Natural gas is included in this discussion as it is a utility used to heat homes and businesses and to supply fuel for power plants.

Fossil fuel refining and distribution is a complex and multi-stage process. Not only does it supply fuel for electricity generation, but it also requires electricity from a grid to run its various processes.

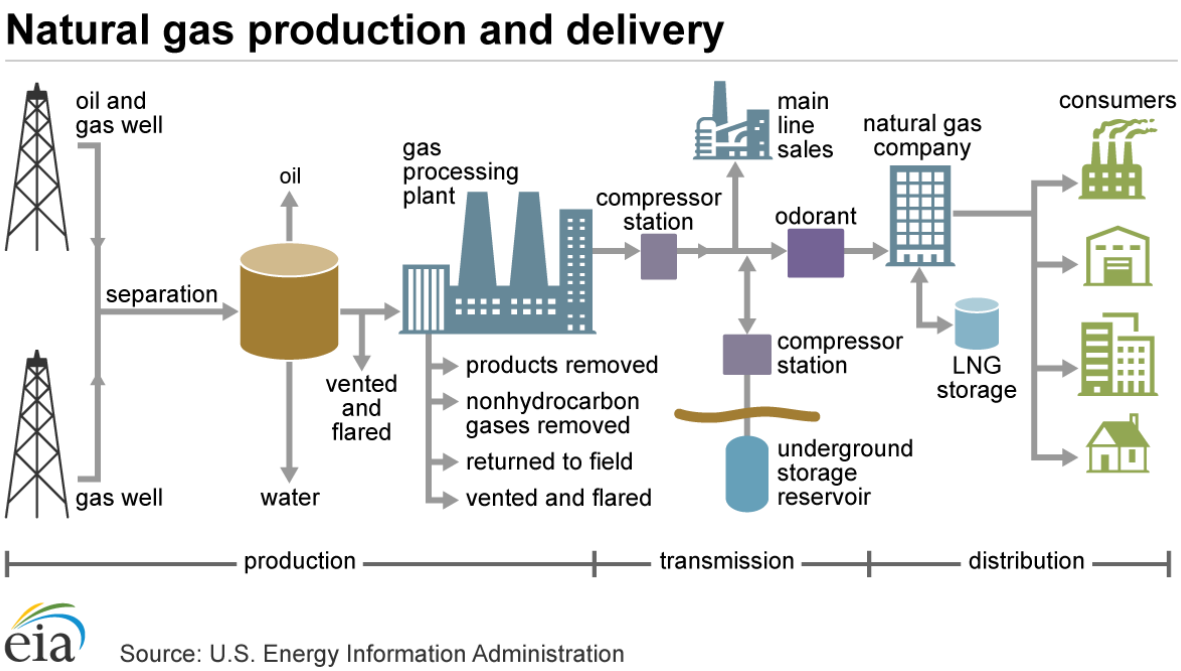


Figure 2 Natural gas explained - Delivery and storage of natural gas US Energy Information Administration
https://www.eia.gov/energyexplained/natural-gas/delivery-and-storage.php

Once natural gas is refined, its distribution infrastructure includes:

- Compressors: To move it through the distribution network.
- Transmission pipelines: Moving gas long distances, typically at 200 to 1,500 PSIG.
- Distribution pipelines: 10 – 200 PSIG, delivering gas from local utilities to end users.
- Storage: Typically underground in played-out wells or salt caverns
- Monitoring and controls

Supply Chain Failures And Effects

Americans expect their utilities to run 100% of the time, without exception. Electric utilities have invested heavily to ensure that reliability. The supply chain for electricity includes backup and redundant power generation capacity, multiple fuel types, interconnecting networks of power lines, spare transformers and switching equipment, the ability to switch between generating sources and the ability to adjust power output to meet demand. For gas it requires natural gas collection systems, refining / processing, and pumping to central distribution points.

When the supply chain for electricity or natural gas fails, the consequences can be disastrous. A failure in the supply chain can lead to the utility going offline, in turn leading to severe consequences for utility customers. Winter Storm Uri in 2021 was, if nothing else, a clear example of the consequences of an inadequately resilient supply chain.

Winter Storm Uri As An Example Of A Supply Chain Failure

A simplified version of the energy supply chain sequence of events during the storm is as follows:[2]

February 8-10	A large cold front moved into Texas. Natural gas plants went offline, largely to protect the wellheads or processing facilities from freezing. At the same time, low wind speeds led wind generators (which had previously provided about 40% of Texas power) to reduce their output. Additionally, wind turbines began to freeze up in the cold. The loss of natural gas prevented natural gas plants from coming online to replace the loss of wind turbine capacity.
February 11	Water in oil and gas wellheads began to freeze. Additionally, the Texas Railroad Commission ordered gas deliveries to be prioritized for homes. Treducing gas availability for electric power plants.
February 13	Cold weather disrupted 22 more gas processing plants, leading to a total of 38 offline or reduced capacity plants (and 45% of Texas natural gas production). This further reduced natural gas electricity production.
February 14:	More wind power plants went offline due to freezing. But as 60% of Texas homes are heated by electricity, the load on the power grid increased.
February 15	From 1:00 AM to about 5:00 AM, the Electric Reliability Council of Texas (ERCOT) told utilities around the state to "shed loads" (turning off power to residents and "non-critical" infrastructure) to prevent complete grid collapse. In the process, several natural gas processing facilities also lost power, further reducing natural gas availability.
February 17	The number of offline natural gas plants peaked.
February 18	ERCOT stopped outages as temperatures rose and power supplies came back online.

[2] The Timeline and Events of the February 2021 Texas Electric Grid Blackouts, University of Texas at Austin Energy Institute, July 2021.
https://energy.utexas.edu/sites/default/files/UTAustin%20%282021%29%20EventsFebruary2021TexasBlackout%20210714.pdf

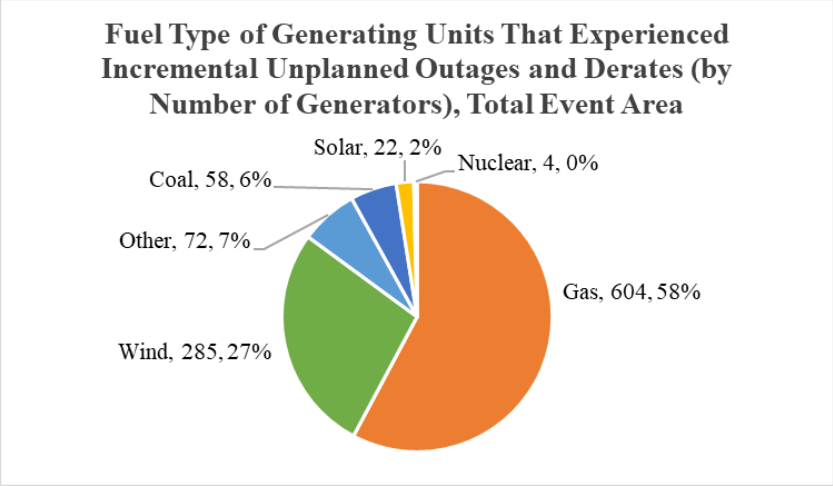
In the end:

- 246 Texans died, primarily due to cold.
- Eleven million Texas residents (69%) lost power, for an average of 42 hours over six days.[3]
- Texans ran water to keep their lines from freezing, even as outside water froze and burst. The resulting drop in water pressure led to bacteria being pulled into the water supply. Between ten and fifteen million Texans lost access to clean water.
- Economic loss estimates ranged from $80 billion to $295 billion USD. Compare this to the two most costly hurricanes in US history, Harvey at $145B or Katrina at $161B. [4,5]
- Texans paid for the losses. While Texans paid less than $9.8 billion for electricity in all of 2020. Texans paid $10.3 billion for electricity on February 16 alone. The Texas Legislature approved the issuance of bonds to repay some of those costs, which would be expected to create a debt obligation of about $200 person in Texas.[6]

Uri Lessons Learned

The entire Texas energy supply chain failed at points. A portion of every generation type, regardless of fuel failed in the cold. Power and wind had the most, but it became clear the Texas energy supply chain:

1. Was not designed for reliable delivery of power and heat to end users.
2. Was not designed to operate temperatures Texas had reason to expect.
3. Was not able to operate even at higher temperatures than it had been designed for.
4. Was not designed taking into account the supply chain vulnerabilities of the various types of generators.



[3] February 2021 Winter Storm-Related Deaths – Texas, Texas Health and Human Services, Dec. 31, 2021, https://www.dshs.texas.gov/news/updates/SMOC_FebWinterStorm_MortalitySurvReport_12-30-21.pdf
[4] Cost of Texas' 2021 Deep Freeze Justifies Weatherization, Dallas Fed Economics, Federal Reserve Bank of Dallas, (Apr. 15, 2021), https://www.dallasfed.org/research/economics/2021/0415
[5] Reliability and Resilience in the Balance, American Society of Civil Engineers, Texas Section, https://www.texasce.org/tce-news/actions-to-get-reliability-and-resilience-in-balance/
[6] The Texas Electric Grid Failure Was a Warm-up, Texas Monthly, By Russell Gold, February 2022, https://www.texasmonthly.com/news-politics/texas-electric-grid-failure-warm-up/

Wind power reliability

Little wind during the storm combined with freezing conditions to lead to 27% of all power losses. Not allowing for this possibility alternatives resulted in a significant portion of overall lost power. Because of the lack of wind and freezing, wind power reliability was the lowest of all energy types during Uri, with a 74% reduction loss in net production capacity.

Natural gas supply chain weakness

The "supply chain" for natural gas was not ruggedized for cold weather. Most processing facilities were not weatherized for several days of very cold temperatures. Plants went offline due to:

Freezing issues or wells being shut down to prevent freezing:	52.2%
Power losses to NG facilities (blackouts and power lines):	18.1%
Freezing and power loss combined:	18.2%

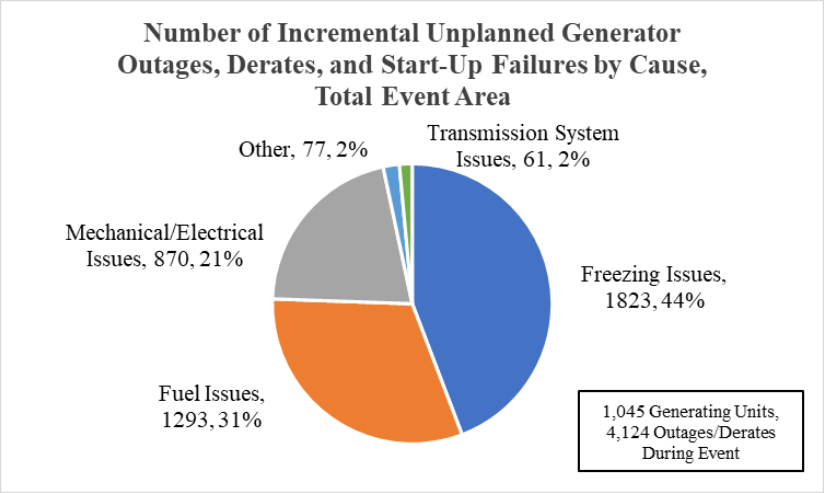
Declines in NG production led to declines in NG power plant electricity output. This in turn led to rolling blackouts and power losses at the gas producers - a "cascading 'death spiral' for gas-fired power plants and their customers"[7].

Last, most natural gas processing facilities had not taken advantage of their ability to receive (as critical infrastructure) priority power from ERCOT. Ironically, natural gas industry groups placed most of the blame for power losses which shut down gas processing and transmission on ERCOT.

Power plant construction

Whether by design or operation, plants were unable to meet their own ambient temperature specifications, , as 81% of freeze-related generating plant "outages occurred at temperatures above the "units' stated ambient design temperature."

The power plants themselves were not ruggedized for freezing conditions. This accounted for 44% of "Freezing Issues", but likely contributed to the 21% "Mechanical / Electrical Issues."



[7]The Texas Railroad Commission's Response (so far) to Winter Storm Uri, Oil and Gas Lawyer Blog, John McFarland, May 2,2022, https://www.oilandgaslawyerblog.com/the-texas-railroad-commissions-response-so-far-to-winter-storm-uri/

Ultimately, the system failed because the energy supply chain was not protected. Given that the disaster cost Texans over $100 billion, protecting that supply chain would likely have much cost less than the resulting damage.

One organization which was prepared for the event was pipeline owner Energy Transfer which winterized their gas distribution equipment. When Uri struck, they had gas available for users. As a result, they posted record profits during the first quarter of 2021. It "chalked up its profits to preparation—it had forked over the money to winterize parts of its facilities, so they remained up and running during the storm."[8] Presumably this might be an incentive for other gas producers to do the same.

Uri Lessons Ignored

Multiple parties documented advance warnings regarding the need for energy supply chain protection. Storms in both 1989 and 2011 led to natural gas flow curtailments due to cold weather. The importance of doing so was documented, at least after the 2011 grid failure. However, legislation passed following the 2011 event only required reports to be prepared about infrastructure security. No legislation required grid suppliers or ERCOT to actually make any physical changes to infrastructure.

As had occurred in 2011 and during 2021's winter storm Uri, the same thing happened again. On January 22, 2022, a cold front passed through West Texas, and the "temperature in Midland hit a low of 14 degrees before rebounding to 56 the next day. During that brief spell, the gas infrastructure faltered, with production falling by 25 percent".[9]

Under pressure from the Texas legislature, Raiload Commission of Texas (RRC), the state regulator of natural gas production and distribution adopted requirements that Critical Infrastructure natural gas suppliers have their equipment winterized by December 1, 2022. However, as the RRC has not issued guidance on how that will occur, it is questionable as to whether it will be done by the deadlin.

This paper does not discuss the political and economic reasons for the lack of preparation in the Texas natural gas system.

Texans need not feel like they are alone in bad planning. On August 25, 2022, California's legislature passed legislation prohibiting new gasoline cars from being sold in the state by 2035. Six days later (August 31, 2022) the California Independent System Operator (the California version of ERCOT) asked electric vehicle owners not to charge their cars after 4:00 PM as part of a "Flex Alert" to keep the electric grid from being overloaded.

There are, of course other energy supply chain issues (which will be discussed below). However, Winter Storm Uri stands as a textbook example of the importance of protecting the energy supply chain protection and the consequences of failing to do so.

[8] Texas Monthly, 2022
[9] Texas Monthly, 2022

ENERGY SUPPLY CHAIN VULNERABILITIES

During the first half of 2022, discussions of US Energy Supply Chain vulnerabilities primarily revolved around:

1) Cyberattacks, particularly on Operational Technology.
2) Physical attacks.
3) Maintaining system reliability and infrastructure with growing demand.
4) Concerns about relying on unfriendly countries for critical equipment.
5) The effect of Covid on equipment maintenance, new construction, and labor availability.

Whether physical attacks or natural disasters, supply chain failures can strike due to:

Fuel disruption	
Natural gas:	(For power plants, industrial or residential use).
Weather:	Reducing power (solar and wind) availability for power generation.
Generating equipment	Failure or sabotage.
Distribution networks	Failure or sabotage to power lines, substations, transformers and pipelines.
Excess demand	Whether from heating or air-conditioning loads during extreme weather conditions.
Weather	Physical damage / Equipment failure due cold weather.

Other vulnerabilities are discussed below, but the above are those most discussed as of 2022.

Partial List of Energy Supply Chain Vulnerabilities

Fuel	Target Process	Vulner. Point	Targeted Equipment	Result	Cascading Effect
Cyberattack					
NG	Fuel Processing	Control systems	Plant O.T.	Shutdown/damage	Power loss to grid
NG	Fuel Processing	Control systems	Plant O.T.	Shutdown	Space Heat Loss
All	Power Generation	Control systems	Plant O.T.	Shutdown	Power loss to grid
All	Power Generation	Generators	Plant O.T.	Shutdown	Power loss to grid
All	Power Distribution	Control systems	Plant O.T.	Shutdown	Power loss to grid
All	Power Distribution	Business systems	IT Systems	Records loss	Billing, power loss
Physical Attack					
NG	Natural Gas Processing	Process equipment	NG Purification	Eqpt. Damage	Gen. plant fuel loss
NG	Natural Gas Processing	Process equipment	NG Purification	Eqpt. Damage	Space heat loss
NG	Natural Gas Distribution	NG distribution	H.P. Distribution	Eqpt. Damage	Gen. plant fuel loss
NG	Natural Gas Distribution	NG distribution	H.P. Distribution	Eqpt. Damage	Space heat loss
Any*	Power Generation	Generation	Generators	Shutdown	Power loss to grid
Any	Power Generation	Generation	Support Equipment	Shutdown	Power loss to grid
Any	Power Distribution	Power lines	Towers, Wires	Transmission loss	Power loss to grid
Any	Power Distribution	Substations	Transformers, esp. HV	Transmission loss	Power loss to grid
Any	All	EMP detonation	Generation, Control	Shutdown	Grid collapse
Weather					
NG	Inbound Fuel Supply	Gas Stream Freezing	Collection, Processing, Distrib.	Eqpt. Freezing	Gen. plant fuel loss
NG	Inbound Fuel Supply	Gas Stream Freezing	Collection, Processing, Distrib.	Eqpt. Freezing	Space heat loss
NG	Processing	Equipment Freezing	Collection, Processing, Distrib.	Eqpt. Freezing	Space heat loss
All	Power Generation	Support Equipment	Pumps, cooling, etc.	Eqpt. Freezing	Grid power loss
Wind	Power Generation	Wind turbine blades	Generator	Eqpt. Freezing	Grid power loss
All	Power Distribution	Substations, Power Lines	Transmission Loss	Grid power loss	
Wind	Power Generation	Low wind	Generator	Power reduction	
All	Power generation	High electrical demand	Grid frequency drop	Grid power loss	Rolling blackouts
Maintenance					
All	Power Generation	Generating equipment	Power Generation	Shutdown	Grid power loss
All	Power Distribution	Transformers	Power distribution	Transmission loss	Grid power loss
All	Any	Long lead times	Any with long leads	Power reduction	Grid power loss
All	All	Unfriendly suppliers	Any w/ International supply	Shutdown	Grid power loss
All	Power Distribution	Remote hacking	HV Transformers	Shutdown	Grid power loss

* Wind and solar generators are less likely to be directly targeted due to the relatively wide dispersion of the generators.

Operational Technology

A particular vulnerability and growing target of cyberattacks is Operational Technology (OT). This is the hardware and software used to control power plants, refineries, and automated manufacturing, and is used to ensure plants operates reliably, efficiently, and safely. OT in energy infrastructure is a ripe target for ransomware or bad actors wishing to disrupt an economy, and can lead to cascading physical or economic harm and panic.

SCADA (Supervisory Control and Data Acquisition) Systems

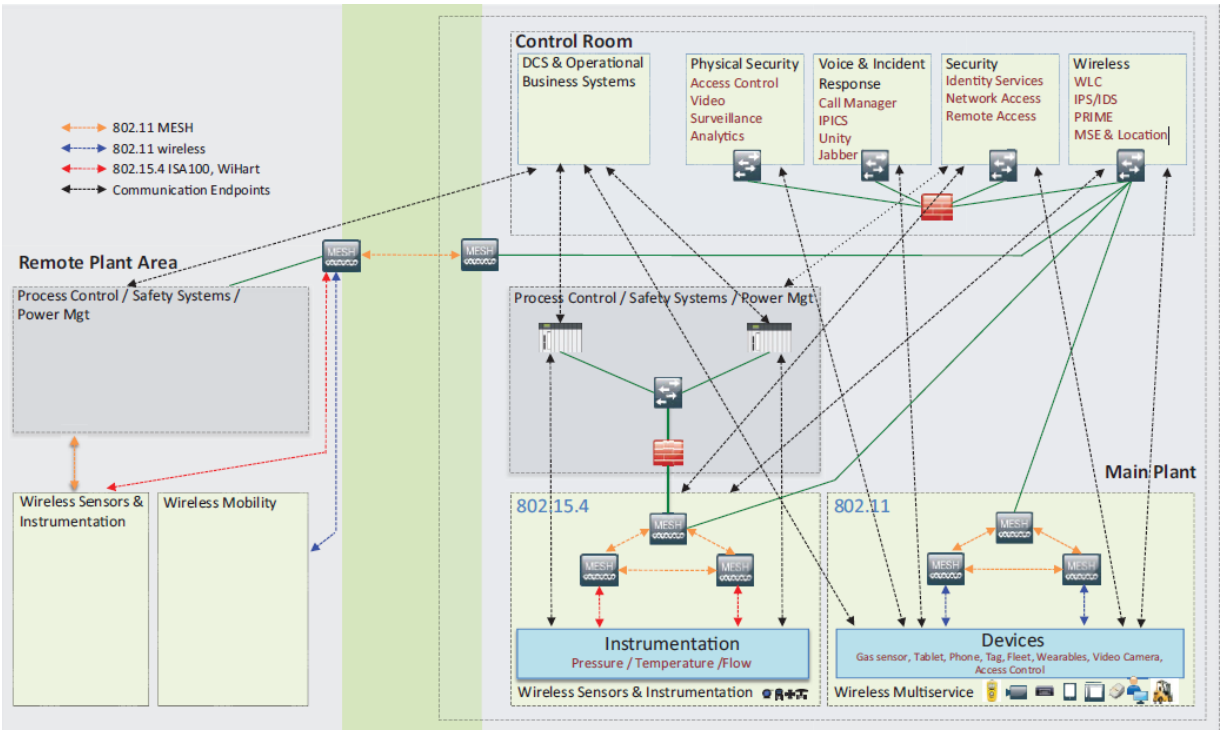
SCADA systems are the heart of operational technology used in refineries, power plants and distribution centers use SCADA systems. A SCADA system is a combination of computers, sensors and other devices that control, monitor and log plant operation.

SCADA systems are a core part of the infrastructure of automated power plants, utilities, refineries, and manufacturing facilities around the world. Proper operation means a safe, productive plant. Improper design and operation can lead to equipment damage, toxic releases, fires, explosions injury and death.

Programmable Logic Controllers (PLCs)

PLCs are industrial computers at the heart of SCADA systems. Specifically designed to control and monitor other equipment, they communicate with and control plant equipment, as well as computers operators will use to monitor the system. For large plants, PLCs will monitor and control thousands of plant devices.

Below is a simplified example of a communications paths used by a refinery SCADA system. [10]



[10] Connected Refineries and Processing Plant, Cisco Reference Document (CRD), CISCO Systems, January 2016, p. 31.

SCADA Vulnerabilities

Unfortunately, PLCs were not originally designed for cybersecurity, and most are built with equipment operation and communication (not security) as their core focus. The same applies to most of the thousands of devices on a plant network, with the possible exception of routers, modems, and wireless access points. Therefore, any device on a network with the ability to communicate with other devices represents a possible source for malware.

The magnitude of this vulnerability can be seen in the sheer numbers of software components in SCADA systems, including:

Firmware Firmware is pre-programmed software built into devices. A simple example is software built into a cell phone that takes an action when users press buttons. Virtually every one of the thousands of plant devices monitoring or controlling processes and communicating with other devices has built-in firmware.

In PLCs, the firmware is programmed by users who then download it to the PLC. This then becomes the device firmware to control equipment and entire plants.

Operating Systems Vendor software provided with a computer that tells a computer how to operate, in what sequence, etc.

Software drivers Software drivers are software used by computers, printers, PLCs and sensors to allow them to communicate with other devices. In SCADA systems, PLC and other device manufacturers will write specific drivers for different networks to allow their devices to communicate with other networked devices.

Applications Software people use to perform tasks. In familiar cases, it includes word processing, spreadsheets or email. In SCADA systems, it includes programs used by operator to control plants, to design screens used by operators to monitor the plant, and to program different alarm conditions.

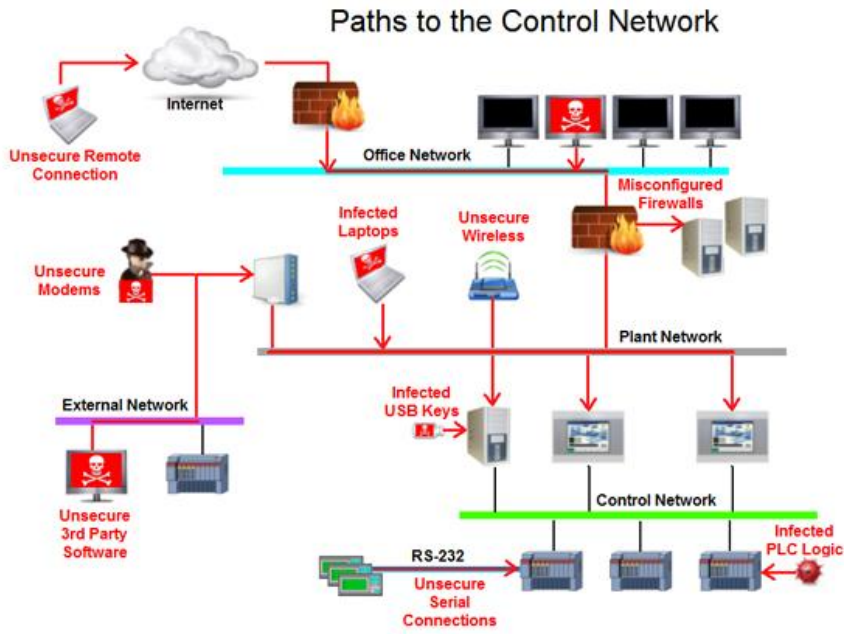
Virtually all hardware and software in a system can be downloaded from various websites. Placing it on the web creates opportunities for attackers to corrupt it even before users download it.

Some devices use multiple types of software, thus multiplying potential vulnerability points. For example, each of the items below include multiple types of software, a few of which are listed:

Device	Firmware	Operating System	Drivers	Application Software
Supervisory Computer	•	•	•	•
PLC	•	•	•	•
Network Communications Hardware	•		•	
Sensor or Control Devices	•		•	•

Noe also that several attacks have been performed on third-party data exchange systems used for billing and other communications.

Below is an illustration of a plant control system and potential "bad actor" access points to it. [11]



PRIMARY TYPES OF ENERGY SUPPLY CHAIN ATTACKS

Attacks on the grid by "bad actors" typically fall into two categories: Cyber and physical attacks. A more recently understood type of attack would be via the components supplied to US industry by foreign unfriendly governments.

Cyberattacks

Cyberattacks attack grid control systems to cause either single-point or wider grid failures. The purpose of these can either be for criminal gain, terrorism or as part of international cyberwarfare. While exceptions exist, cyberattacks generally require the sophistication of international criminal groups or hostile governments.

Data from types of attacks clearly shows that foreign governments are actively planning attacks on American Energy, water and other infrastructure. Reasons for these are typically either for economic reasons (ransomware), to damage the grid (military / terrorism purposes) or both. This document will focus primarily on attacks intending to damage the grid.

Asymmetrical Warfare

Grid attacks are part of "asymmetrical warfare", by which a country attacks its foes with effects reaching far into the morale of the victim's populace. This document will focus primarily on attacks on operational technology.

[11] 6 ways remote HMI/SCADA users can protect plant operations and save money, Controlglobal.com, Kerry L. Sparks, Jun 17, 2015, https://www.controlglobal.com/industrynews/2015/6-ways-remote-hmiscada-users-can-protect-plant-operations-and-save-money/

In addition to damaging a country's ability to prosecute a war, an additional benefit of well-planned cyberattacks could be to decimate a country's will to fight an opponent by:

- Shutting off power possibly for weeks or months, to large sections of a country's population.
- Restricting or eliminating water and sewage service.
- Eliminating internet access to people or businesses.
- Cutting off supplies of natural gas for heating and cooking.
- Cutting off supplies of gasoline for cars.

The demotivating effect this type of attack would have on a population is clear:

> *Why would the US care about what China is doing far away in Asia (or Russia in Europe) if opposing them would mean we don't have electricity, running water, heat in our homes, gas for our cars, or access to news and other information?*

Clear evidence shows that China, Russia and other countries are planning cyberattacks on American electrical grids, water systems and manufacturing as strategic parts of attacks on the United States.

- China has built the ability to remotely control hardware into equipment sold to the United States.
- US security agencies have issued several warnings about Russian attacks on US infrastructure.[12, 13]

Further evidence shows they are actively attempting to penetrate US energy industry Operational Technology. In 2021 cyberattacks on OT, over ¼ of the attacks on industry were on energy-related entities:[14]

Industry	All Industries	Energy
Manufacturing:	61%	-
Oil and Gas:	***11%***	***11%***
Transportation:	10%	-
Utilities:	***10%***	***10%***
Mining:	***7%***	***7%***
		28%

It has become clear that China and Russia are actively focusing on learning how to access CI and disrupt in preparation for future attacks.

[12] Understanding and Mitigating Russian State Sponsored Cyber Threats to U.S. Critical Infrastructure; Critical Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency; January 11, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-011a (A pdf version is available on this page).

[13] Russian government cyber activity targeting energy and other critical infrastructure sectors. Alert (TA18-074A), Department of Homeland Security / Cybersecurity and Infrastructure Protection Agency, March 16, 2018, https://www.cisa.gov/uscert/ncas/alerts/TA18-074A

[14] (identified by IBM Security X-Force), p. 26

Documented Attacks on SCADA Systems and OT

US authorities have documented hundreds of cyberattacks on US electricity, water treatment and other facilities. Following are a few examples:

A US utility had its SCADA system targeted and shutdown for two weeks. They did not lose power as they manually operated their substations during this time. This was similar to the 2015 Russian cyberattack on the Ukrainian power grid.

There have also been several "incidents where utilities in multiple locations had 'loss of monitoring or control' starting at exactly the same time and ending at exactly the same time." This indicated a widespread, multi-prong effort by a sophisticated attacker. One of these attacks resulted in power being lost to 130,000 customers.

- As early as 2012, US authorities documented attacks on US non-military targets by Russian hackers and Chinese hackers controlled by the Chinese army.[15]
- In 2013, Iranian hackers accessed a dam used by the Bowman Dam utility for flood control purposes. It was a reconnaissance test and no other attacks were performed.
- In 2014, Russia unleashed Black Energy2 (malware targeting GE Cimplicity HMI, Siemens WinCC and Advantech/Broadwin deployments) in the US electric grid.
- In 2016, attackers hit the SCADA of a water district (given the fictitious name "Kemuri"). They accessed the valve and flow control application that controls PLCs and altered the number of chemicals entering the water supply. This affected water treatment and production capabilities.
- In April 2020, hackers attacked an Israeli water treatment plant, raising the level of chlorine in the water supply.[16]
- In 2021, ransomware attacks hit SCADA systems at three US water treatment facilities. Actual controls were disrupted in two of the systems while the third struck "only" struck system monitoring.
- In February, 2021, a hacker attacked the Oldsmar, Florida water treatment facility and increased the sodium hydroxide content from 100 parts per million (ppm) to 11,100 ppm. The operator that detected this was able to bring the water content back to normal.[17]
- On May 7, 2021, Colonial Pipeline was hit by a Russian gang which took almost 100 GB of data hostage. The disruption led Colonial to shut down diesel, gasoline and jet fuel deliveries to the east coast of the United States – 45%of all of these fuels consumed on the East Coast.[18]

---

[15] Chinese Hacking Team Caught Taking Over Decoy Water Plant, MIT Technology Review, Tom Simonite, August 2, 2013, https://www.technologyreview.com/2013/08/02/15525/chinese-hacking-team-caught-taking-over-decoy-water-plant/

[16] Throwback Attack: Hackers attempt to flood Israeli water supply with chlorine, Industrial Cybersecurity Pulse, Tyler Wall, May 26, 2022

[17] Oldsmar water treatment facility attack is an example of rising cyber threat, Industrial Cybersecurity Pulse, CHRIS VAVRA, FEBRUARY 9, 2021, https://www.industrialcybersecuritypulse.com/facilities/water-treatment-facility-targeted-by-hackers/

[18] Attacks on critical national infrastructure escalate with Colonial Pipeline hack, Industrial Cybersecurity Pulse, GARY COHEN, MAY 10, 2021, https://www.industrialcybersecuritypulse.com/facilities/attacks-on-critical-national-infrastructure-escalate-with-colonial-pipeline-hack/

- In 2022, Russian programmers employed by the Russian government were indicted in the United States for executing cyberattacks which compromised control systems at US refineries. At least one defendant was involved in the 2015 attack on the Ukrainian electrical grid. [19] Three employed by the Russia's Federal Security Service (FSB) attacked the Wolf Creek nuclear plant in Kansas.[20]

A suspicious explosion on June 8, 2022 at the Freeport Liquid Natural Gas facility in Texas was reported to have been caused by LNG being sent through a pipeline at 917 PSIG (instead of the 90 PSIG for which the line was rated). As of September 2022, speculation persists that the attack came from Russia because it bore similarities to a 2017 Russian attack on a Saudi Arabian refinery where hackers took over the SCADA system of a 3,000 acre refinery. The attack came during Russia's Ukraine invasion, a time when Russia had a financial motive to force Europe to depend on Russian natural gas.

Reconnaissance / deferred action attacks

A significant trend has been attempts by foreign governments to gain access to US networks for later use as part of some type of warfare. From 2015 and on, most attacks have appeared to be reconnaissance for the purpose of learning how to access CI computer networks.[21] This type of exploration takes significant resources. Therefore, it is a strong indication that it is sponsored by hostile foreign governments to use later, possibly in real warfare.

On March 15, 2018, the Department of Homeland Security issued an alert that the Russian government engineered a series of cyberattacks targeting American and European nuclear power plants and water and electric systems. It was reported these attacks could allow Russia to sabotage or shut down power plants at will.[22]

"Analyzing data from 2021, X-Force observed attackers conducting massive reconnaissance campaigns searching for exploitable communications in industrial networks."[23]

This appears to be an intentional focus on manufacturing and energy supply chain attacks.
Attacks on Operational Technology continue. The IBM 2022 X-Force Threat Intelligence Report showed a 2,204% increase in attacks on the computer port used for control of Modbus (a PLC communications protocol). These were primarily "massive reconnaissance campaigns searching for exploitable communications in industrial networks. [24]

---

[19] Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide, Justice News, United States Department of Justice, March 24, 2022, https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

[20] Russian Agents Charged With Targeting US Nuclear Plant, Saudi Oil Refinery, Voice of America News, March 24, 2022, https://www.voanews.com/a/russian-agents-charged-with-targeting-us-nuclear-plant-saudi-oil-refinery-/6501013.html

[21] Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, CISA, March 16, 2018, https://www.cisa.gov/uscert/ncas/alerts/TA18-074A#revisions

[22] Perloth N, Sanger D (2018) Cyberattacks put Russian fingers on the switch at power plants, U.S. says. The New York Times Available at https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

[23] X-Force Threat Intelligence Index 2022, IBM Security, p. 24

[24] X-Force Threat Intelligence Index 2022, IBM Security, P. 24

Physical attacks On the Energy Supply Chain

Physical attacks attempt to directly damage facilities and equipment at targets such as refineries, power plants, substations, transmission lines, and water purification or sewage treatment plants. The US has already experienced multiple incidents of this type, and they can be expected to continue. Physical attackers of US infrastructure to date who have been identified have typically been disgruntled employees, eco-terrorists and racial extremists attempting to start race wars. Their attempts have been to either strike single targets or, if attempting to take down the electric grid, multiple targets simultaneously.

Some attacks are aimed at individual points on the grid. With increasing availability of information and attacker sophistication, others can be targeted at multiple locations in an attempt to take down a wider area or an entire grid.

Point Attacks

Point attacks can strike at individual points in energy supply chains. These can include attacks on natural gas refineries, power plants, substations and transformers, and power lines.

Electrical substations are a particular target because attacks there can affect not only downstream customers but, if properly timed, can take down other substations and potentially, an entire grid.

Attackers seem to know this. In 2022, a CBS interview discussed physical attacks on US electric infrastructure. Specifically, they noted that:

- On April 16, 2013, as many as six gunmen attacked PG&E's Metcalf Power near Silicon Valley. Had they knocked it offline, power to all of Silicon Valley would have been cut off.
- In 2016, an eco-terrorist in Utah shot up a large transformer, triggering a blackout. He said he'd planned to hit five substations in one day to shut down the West Coast.
- In 2020, the FBI uncovered a white supremacist plot called "lights out" to simultaneously attack substations around the country.[25]

Multiple-Point Grid Takedown Attacks

- The widely distributed and exposed nature of the US electrical grid makes it difficult to defend against attack. Therefore, responses to single-point attacks have typically focused on repairing damage and rerouting power to make up for individually lost plants, substations, or transmission lines. The American electrical grid is designed to withstand the loss of individual components without losing the entire network.

Causing more damage to the grid than operators can respond to can take down the entire network. Attacks on several plants or substations could have this effect, especially if simultaneous. US researchers have posited that simultaneous attacks on as few as 20 US transmission centers could take out an entire grid area.

[25] Vulnerable U.S. electric grid facing threats from Russia and domestic terrorists
CBS News, 60 Minutes, Bill Whitaker, February 27, 2022, https://www.cbsnews.com/news/america-electric-grid-60-minutes-2022-02-27/

A possible (though quite limited) example of simultaneous physical attacks occurred in Austin County, TX and Los Angeles County, CA on 9/11/2021 at 8:32 AM. They were reported by the NERC as a "Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems." No attackers were identified, but the simultaneous attacks at exactly the same time on the 20th anniversary of 9/11/2001, appear to indicate an intentional multiple-point grid attack.

High Altitude Electromagnetic Pulse (HEMP)

One multiple-point attack would be to detonate a nuclear weapon at altitude can create a HEMP and damage or take down an entire electrical network at once. This type of event can affect circuit boards, computers, and commercial equipment, all the way up to distribution line transformers and power lines.

As noted above, most bulk power systems (large networks) are designed to withstand a single-point failure or a series of them, if spaced out over time. A HEMP at altitude can hit large areas and their power plants simultaneously, propagating at the speed of light. Per one estimate, this could "expose the entire electrical grid east of the Mississippi River to a severe HEMP transient within one power cycle (1/60th of a second)." [26]

Other countries (again, primarily China and Russia) are putting a great deal of effort into EMP devices. Possible motivations for this strategy include:

- Disable American infrastructure while preserving it for later use by the aggressor.
- Disable an American response to aggression.
- Disable an American response to aggression while also warning the US against a full nuclear response by saying the equivalent of "We could have done worse. Don't push us."

Supply Chain Equipment Attacks

On May 27, 2020 the Wall Street Journal reported that a Chinese built transformer was seized by the government and diverted by the federal government to Sandia National Laboratories.[27] In another case, Cybersecurity Controls Expert, Joseph Weiss noted that "Government and public utility procurement rules often push organizations into buying equipment due to price and without regard to origin or risk… *When the Chinese transformer was delivered to a US utility, the site acceptance testing identified electronics that should NOT have been part of the transformer – hardware backdoors.*"[28]

Because China is the only country supplying this type of equipment, it makes the US vulnerable to potential Chinese attempts to shut down the US power grid.[29]

---

[26] High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, North American Electric Reliability Corporation, June 2010, p. 80.

[27] U.S. Seizure of Chinese-Built Transformer Raises Specter of Closer Scrutiny, Wall Street Journal, Rebecca Smith, 5/27/2020, https://www.wsj.com/articles/u-s-seizure-of-chinese-built-transformer-raises-specter-of-closer-scrutiny-11590598710

[28] Emergency Executive Order 13920 – Response to a real nation-state cyberattack against the US grid, Controlglobal.com, Joe Weiss, Mon, 05/11/2020, https://www.controlglobal.com/blogs/unfettered/emergency-executive-order-13920-response-to-a-real-nation-state-cyberattack-against-the-us-grid/

[29] Executive order boots "foreign adversaries" from US electric grid over security concerns, CSO Online, Cynthia Brumfield, May 20, 2020 https://www.csoonline.com/article/3544299/executive-order-boots-foreign-adversaries-from-us-electric-grid-over-security-concerns.html

OTHER ENERGY SUPPLY CHAIN WEAKNESSES

Generation and Transmission Equipment

Generation capacity in the energy supply chain is currently stretched thin in the United States. Efforts to improve it are ongoing, especially with respect to renewables, but are hampered by a lack of:

1) Generation equipment (primarily solar and wind).
2) Power transformers and substations.
3) Grid connections.
4) Manufacturing, installation, and maintenance labor.

The primary supply chain for much clean energy equipment such as photovoltaic cells, batteries and some wind turbine equipment is the People's Republic of China. Therefore, the supply chain is not only vulnerable to disruption if China decides to cut it off but is also, as mentioned previously, subject to modifications making that equipment more susceptible to cyberattack.

Electric utilities are experiencing shortages and/or high costs for distribution transformers, wire, smart meters, skilled labor, and maintenance equipment due to the ongoing economic impacts from the COVID-19 pandemic. Per the American Public Power Association, "Delayed investments and expanding lead times for new equipment caused by a lack of materials and labor will continue to compound the problem—possibly for years to come.[30] Per multiple sources, supply chain problems are preventing renewable energy projects from being completed.

As a result, the Department of Energy in 2022 stated a need for domestic raw material mining and processing, manufacturing capabilities, and workers in both utilities and their support networks.[31] Whether this will pass environmental regulatory and lawsuit muster has yet to be determined.

Increasing Demand

The Texas population is growing, as is the electrical demand per household with the move away from natural gas heating. Electric generating capacity has not kept up with demand. For example:

Per a June 2022 Reuters article, combined with coal plant shutdowns and reduced hydropower availability, demand led to electric utilities burning record amounts of natural gas to generate electricity. Per the article, this resulted in their having difficulty rebuilding stockpiles for winter 2023.[32]

The year after the winter storm Uri disaster, six Texas power plants went offline in May 2022 due to high demand.[33] In the summer of 2022, rolling blackouts and warnings of blackouts continued in the state.

---

[30] Critical Infrastructure and Supply Chain Constraints, American Public Power Association, June 2022, https://www.publicpower.org/policy/critical-infrastructure-and-supply-chain-constraints-0

[31] America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition, Department of Energy, February 24, 2022, p. ix.

[32] U.S. power companies face supply-chain crisis this summer, Scott Disavino, June 29,2022, https://www.reuters.com/business/energy/us-power-companies-face-supply-chain-crisis-this-summer-2022-06-29/

[33] Texas grid operator calls for power conservation as temperatures, prices soar, Reuters, Gary Macwilliams, May 13,2022, https://www.reuters.com/world/us/texas-grid-operator-calls-power-conservation-over-weekend-2022-05-13/

Maintenance

Per a May 2022 Forbes magazine article[34], the petrochemical supply chain was stretched even before Covid and the Ukraine war. Driving factors included:

- Investor profit demands led oil and gas companies to forgo investing in building resilience (maintenance) in their hydrocarbon supply chains. As a result, Oilfield Equipment and Services (OFES) companies downsized to remain competitive. In this post-Covid environment, they are having difficulty attracting labor for maintenance and production tasks.
- Few OFES companies have digital platforms to balance inventory, optimize work crews and maximize purchasing efficiency. Many use sole source supplier contracts which prevent them from finding alternative equipment sources when their supplier cannot guarantee delivery dates.
- In addition to demand shifting away from petrochemicals and toward clean energy, the pandemic led to a shortage of well casing steel and fabrication capability.

The situation faced by utilities overall was well reflected in a June 2022 statement by Buddy Hasten, president and CEO of Arkansas Electric Cooperative Corp: "Many utilities were forced to deplete their warehouses and staging yards to meet construction demand or handle repairs while manufacturing was stalled. This has eroded the traditional reserve inventory of critical infrastructure. Given the supply chain constraints, there are long lead times making it almost impossible for utilities to restock to normal levels of inventory for storm seasons,"[35]

High Voltage DC Transformers

HV (high voltage) transformers—transmitting voltages of greater than 100 kV make it possible to send electricity over great distances to substations. They are a weak link in the American infrastructure, primarily because of long lead times and because China is the largest supplier in the world. The Federal Energy Regulatory Commission (FERC) has identified 30 of these nationwide as being critical. It has been postulated that simultaneous loss of just nine, in various combinations, could cripple the network and cause a cascading failure, resulting in a "coast-to coast blackout." [36]

As of 2014, high voltage transformers constituted less than 3% of transformers in U.S. power substations but carried 60%-70% of the nation's electricity.

Pandemic

If an event more severe than Covid-19 occurred, it would potentially make a large portion of the utility workforce unavailable to work. Likewise, utilities may not be able to share personnel across power grids. This lack of specially trained operators would cause the overall system to be less reliable, less resilient, and more susceptible to other attacks.[37]

Environmental issues

---

[34] The Energy Industry's Supply Chain Dilemma: Collective Pain Calls For Collective Action, Forbes Magazine, Muqsit Ashraf, May 9, 2022, https://www.forbes.com/sites/muqsitashraf/2022/05/09/the-energy-industrys-supply-chain-dilemma-collective-pain-calls-for-collective-action/?sh=17733a18d123

[35] Tiger Team: Electric Co-op Leaders Join Effort to Ease Supply Chain Problems, National Rural Electric Cooperative Association, July 8, 2022, Derrill Holly

[36] Physical security of the U.S. power grid: high-voltage transformer substations. Congressional Research Service, June 7, 2014, p. 6 https://fas.org/sgp/crs/homesec/R43604.pdf

[37] High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, North American Electric Reliability Corporation, U.S. Department of Energy, June 2010, https://www.energy.gov/ceser/downloads/high-impact-low-frequency-risk-north-american-bulk-power-system-june-2010

As mentioned above, the move toward green energy is greatly disrupting the energy supply chain as:

- Fossil fuel refineries and power plants continue to shut down.
- As was seen in winter storm Uri, the rapid expansion of green (wind) energy has the potential to make grid operators think more power is available than might be the case. The result is a grid more vulnerable than is appreciated. While this will most likely be resolved in the long term, it has led to short term failures to serve Texas well.
- As renewable power generation comes online, the demand is reducing the available supply of high voltage transformers for system maintenance, updates or repair.
- Lawsuits over fossil fuel pipelines contributes uncertainty to the future of fossil fuel expansion.

FRAMING A RESILIENCE MESSAGE TO THE ENERGY INDUSTRY

Texas Culture

The Texas spirit is truly unique with respect to the rest of the country. It can be described as combining patriotism, independence and a preference for minimal government interference in people's lives.

The goal of this section is to describe what approaches might work best in helping Texas business understand the importance of protecting critical infrastructure. What follows is in no way intended as a criticism of Texas, its people or state politics. They are what they are and should be accepted as such.

An example of this Texas culture can be seen in a blog post quoting former Governor (and Energy Secretary) Rick Perry's during Winter Storm Uri.[38] After comments over the previous days blaming wind power for the power outages, Governor Perry was described as saying:

> "Technology – not regulation" is how the governor believes Texas can ensure its grid can weather the next storm.
>
> "We've got to have diversity, we've got to have resiliency, and we've got to have a baseload that we can absolutely count on no matter what happens out there," Gov. Perry said.
>
> "Those watching on the left may see the situation in Texas as an opportunity to expand their top-down, radical proposals. Two phrases come to mind: don't mess with Texas, and don't let a crisis go to waste."

Again, this should not be considered as criticism, but a framework to understand the "target customer"

Framing a Resilience Message

With respect to protection against foreign attacks, Texas can reasonably be expected to strongly support infrastructure protection. On the other hand:

- Whether in Texas or other states, businesspeople are typically highly suspicious of governmental institutions, and don't appreciate being told what they "should" do.
- Approaching resilience from a "global warming" perspective is unlikely to be well received.
- Likewise, telling companies (particularly privately held ones) to spend money on winterizing natural gas systems will result in pushback.

Ideally, a message persuading companies to act on CI protection would benefit most by appealing to patriotism, duty to the state and the company, preventing future regulation and the bottom line.

That said, there is no guarantee that companies will spend money on CI protection. But creating messages that demonstrate concern for the company and the people of Texas will be much better received than those telling people to change for reasons with which they don't agree.

[38] "The American Story – What's Up in Texas, on February 17, 2021 https://www.republicanleader.gov/whats-up-in-texas/

Winter Storm Uri As a Reference Point

After Uri, the Texas Railroad Commission (TRC) proposed rules making it optional for natural gas suppliers to winterize their facilities. In that case, the state legislature stepped in to force a more aggressive plan.

But regardless, motivating change will work better with a "carrot" approach than a "stick" approach.

Possible message concepts in approaching energy Critical Infrastructure companies might include:

Profit — As noted previously, Energy Transfer made record profits during Uri and "chalked up its profits to preparation" by winterizing. They profited through preparation (leveraging both the ability to produce and to take advantage of high spot gas prices), an appealing message.

Patriotism — Being able to allow Texas to keep running and protecting the people of Texas would be what is often called in sales "the sizzle on the steak". Doing well by doing good can be a psychological motivator to change.

Pride: — Many Texans are resistant to the idea of green energy. A campaign showing their support of Texas independence (including independence from green energy) would be well received.

Shame — Fear and shame, (particularly the fear of being singled out or being the one who missed an opportunity) is a major driver in the actions of mid and upper-level managers. As a corollary to a "patriotism" message, it may be a useful tool in marketing. However, this is a strategy best if carefully used and in a very limited manner.

Last, if Critical Infrastructure companies cannot be motivated to CI Protection requirements (weather, cyber-protection physical attacks, etc.), then a legislative approach may be necessary

Ultimately, the most likely solution will be a combination of all of these strategies, combined with:

- Research on who the decision makers and influencers might be.
- "Marketing" messages written to show them the benefits of improved resilience, and costs of unpreparedness.

Treatment of Large Vs. Small Businesses

Based on the idea that it is important to reach both large and small businesses, this paper assumes:

1. There is a need for a "marketing message" about the importance of protecting Critical Industries, to be addressed to those industries.
2. Large businesses (with more than 100 employees and/or $6 million in annual gross receipts are more likely to have their staff to help with supply chain planning than small businesses.
3. Small businesses (defined under Texas law as independently owned and operated, having fewer than 100 employees or less than $6 million in annual gross receipts) are less likely to have access to those resources or even understand what resources are necessary.
4. Creating a "marketing message" will be most effective if it understands the different needs, concerns and psychology of large and small businesses.

In the case of small businesses, they may not be as familiar with CI protection, and would therefore benefit more from a message offering assistance on how to protect their company. As (per below) power generators tend to be larger companies, the petrochemical extraction and natural gas processing businesses have more small companies. Presumably the smaller companies with less resources would be most likely to benefit from CI protection information.

Table 4: Texas CI Businesses and sizes

			Number of companies by employee count		
NAICS	NAICS Description	Total Est.	<100	100-499	500+
211120	Crude Petroleum Extraction	1,990	85%	4%	12%
211130	Natural Gas Extraction	451	52%	7%	40%
212111	Bituminous Coal and Lignite Surface Mining	17	12%	0%	88%
213111	Drilling Oil and Gas Wells	804	68%	5%	28%
213112	Support Activities for Oil and Gas Operations	4,047	77%	9%	14%
221112	Fossil Fuel Electric Power Generation	163	10%	6%	84%
221113	Nuclear Electric Power Generation	8	13%	0%	88%
221114	Solar Electric Power Generation	22	64%	0%	36%
221115	Wind Electric Power Generation	80	18%	0%	83%
221117	Biomass Electric Power Generation	3	100%	0%	0%
221121	Electric Bulk Power Transmission and Control	45	11%	0%	89%
221122	Electric Power Distribution	720	23%	13%	64%
221210	Natural Gas Distribution	272	21%	3%	76%
324110	Petroleum Refineries	36	25%	11%	64%
335311	Power, Distribution, and Specialty Transformer Mfg	21	52%	0%	48%
486110	Pipeline Transportation of Crude Oil	181	7%	0%	93%
486210	Pipeline Transportation of Natural Gas	435	9%	0%	91%
486910	Pipeline Transportation of Refined Petroleum Prod.	149	5%	5%	90%
488310	Port and Harbor Operations	31	77%	0%	23%
488320	Marine Cargo Handling	60	45%	20%	35%

CONCLUSION

There are many challenges ahead in protecting Texas Critical Infrastructure. Whether from other countries or natural disasters, there are numerous threats to Texas energy infrastructure.

Those hurdles include a lack of awareness, the cost to upgrade protection, a desire to be left alone to run a business the way someone wants to, political reluctance and others. Whether those hurdles can be overcome will be of critical importance to the health of both the people and economy of Texas.

APPENDIX 1 Energy Sector Resource Web Sites

Cyber Texas Department of Transportation	https://www.txdot.gov/inside-txdot/division/information-technology/Cybersecurity/cybersecurity-resources.html
FCC Cyberplanner	https://www.fcc.gov/cyberplanner
Small Business Administration	https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity
Shields Up, CISA	https://www.cisa.gov/shields-up
U.S. Department of Energy	https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf
Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/ict-supply-chain-library https://www.cisa.gov/supply-chain-compromise https://www.cisa.gov/stopransomware

APPENDIX 2: NAICS DEFINITIONS

211120 Crude Petroleum Extraction
Establishments primarily engaged in (1) the exploration, development, and/or the production of petroleum from wells in which the hydrocarbons will initially flow or can be produced using normal or enhanced drilling and extraction techniques or (2) the production of crude petroleum from surface shales or tar sands or from reservoirs in which the hydrocarbons are semisolids. Establishments in this industry operate oil wells on their own account or for others on a contract or fee basis.

211130 Natural Gas Extraction
Establishments primarily engaged in (1) the exploration, development, and/or the production of natural gas from wells in which the hydrocarbons will initially flow or can be produced using normal or enhanced drilling and extraction techniques or (2) the recovery of liquid hydrocarbons from oil and gas field gases. Establishments primarily engaged in sulfur recovery from natural gas are included in this industry.

212111 Bituminous Coal and Lignite Surface Mining
This U.S. industry comprises establishments primarily engaged in one or more of the following: (1) surface mining of bituminous coal and lignite; (2) developing bituminous coal and lignite surface mine sites; (3) surface mining and beneficiating (e.g., cleaning, washing, screening, and sizing) of bituminous coal; or (4) beneficiating (e.g., cleaning, washing, screening, and sizing coal), but not mining, bituminous coal.

213111 Drilling Oil and Gas Wells
This U.S. industry comprises establishments primarily engaged in drilling oil and gas wells for others on a contract or fee basis. This industry includes contractors that specialize in spudding in, drilling in, redrilling, and directional drilling.

213112 Support Activities for Oil and Gas Operations
This U.S. industry comprises establishments primarily engaged in performing support activities on a contract or fee basis for oil and gas operations (except site preparation and related construction activities). Services included are exploration (except geophysical surveying and mapping); excavating slush pits and cellars, well surveying; running, cutting, and pulling casings, tubes, and rods; cementing wells, shooting wells; perforating well casings; acidizing and chemically treating wells; and cleaning out, bailing, and swabbing wells.

221112 Fossil Fuel Electric Power Generation
This U.S. industry comprises establishments primarily engaged in operating fossil fuel powered electric power generation facilities. These facilities use fossil fuels, such as coal, oil, or gas, in internal combustion or combustion turbine conventional steam process to produce electric energy. The electric energy produced in these establishments is provided to electric power transmission systems or to electric power distribution systems.

221113 Nuclear Electric Power Generation
This U.S. industry comprises establishments primarily engaged in operating nuclear electric power generation facilities. These facilities use nuclear power to produce electric energy. The electric energy produced in these establishments is provided to electric power transmission systems or to electric power distribution systems.

221114 Solar Electric Power Generation
This U.S. industry comprises establishments primarily engaged in operating solar electric power generation facilities. These facilities use energy from the sun to produce electric energy. The electric energy produced in these establishments is provided to electric power transmission systems or to electric power distribution systems.

221115 Wind Electric Power Generation
This U.S. industry comprises establishments primarily engaged in operating wind electric power generation facilities. These facilities use wind power to drive a turbine and produce electric energy. The electric energy produced in these establishments is provided to electric power transmission systems or to electric power distribution systems.

221117 Biomass Electric Power Generation
This U.S. industry comprises establishments primarily engaged in operating biomass electric power generation facilities. These facilities use biomass (e.g., wood, waste, alcohol fuels) to produce electric energy. The electric energy produced in these establishments is provided to electric power transmission systems or to electric power distribution systems.

221121 Electric Bulk Power Transmission and Control
This U.S. industry comprises establishments primarily engaged in operating electric power transmission systems and/or controlling (i.e., regulating voltages) the transmission of electricity from the generating source to distribution centers or other electric utilities. The transmission system includes lines and transformer stations.

221122 Electric Power Distribution
This U.S. industry comprises electric power establishments primarily engaged in either (1) operating electric power distribution systems (i.e., consisting of lines, poles, meters, and wiring) or (2) operating as electric power brokers or agents that arrange the sale of electricity via power distribution systems operated by others.

221210 Natural Gas Distribution
This industry comprises: (1) establishments primarily engaged in operating gas distribution systems (e.g., mains, meters); (2) establishments known as gas marketers that buy gas from the well and sell it to a distribution system; (3) establishments known as gas brokers or agents that arrange the sale of gas over gas distribution systems operated by others; and (4) establishments primarily engaged in transmitting and distributing gas to final consumers.

324110 Petroleum Refineries
Establishments primarily engaged in refining crude petroleum into refined petroleum. Petroleum refining involves one or more of the following activities: (1) fractionation; (2) straight distillation of crude oil; and (3) cracking.

335311 Power, Distribution, and Specialty Transformer Manufacturing
This U.S. industry comprises establishments primarily engaged in manufacturing power, distribution, and specialty transformers (except electronic components). Industrial-type and consumer-type transformers in this industry vary (e.g., step up or step down) voltage but do not convert alternating to direct or direct to alternating current. Illustrative Examples:

Distribution transformers, electric, manufacturing, Fluorescent ballasts (i.e., transformers) manufacturing, Substation transformers, electric power distribution, manufacturing, Transmission and distribution voltage regulators manufacturing. *(Included as a possible resource for high-voltage DC transformers, currently supplied primarily from China.)*

486110 Pipeline Transportation of Crude Oil
Establishments primarily engaged in the pipeline transportation of crude oil.

486210 Pipeline Transportation of Natural Gas
Establishments primarily engaged in the pipeline transportation of natural gas from processing plants to local distribution systems. This industry includes the storage of natural gas because the storage is usually done by the pipeline establishment and because a pipeline is inherently a network in which all the nodes are interdependent.

486910 Pipeline Transportation of Refined Petroleum Products
Establishments primarily engaged in the pipeline transportation of refined petroleum products.

488310 Port and Harbor Operations
Establishments primarily engaged in operating ports, harbors (including docking and pier facilities), or canals. *Included in consideration of allowing import and export of petroleum-based fuels to and from Texas.*

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Lynn, S. (2022). **Texas Critical Infrastructure Supply Chain Protection: Reaching the Energy Industry** (Report No. IHS/CR-2022-2031). The Sam Houston State University Institute for Homeland Security. https://ihsonline.org/Research/Technical-Papers/Texas-Critical-Infrastructure-Supply-Chain-Protection-Reaching-the-Energy-Industry