Pick Your Poison

Navigating a Secure Clean Energy Transition

Aug 2024

DEFCON@policy

Emma M Stewart, PhD

Chief Power Grid Scientist

National and Homeland Security

emma.stewart@inl.gov

@turbo81

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

INL/CON-24-79311

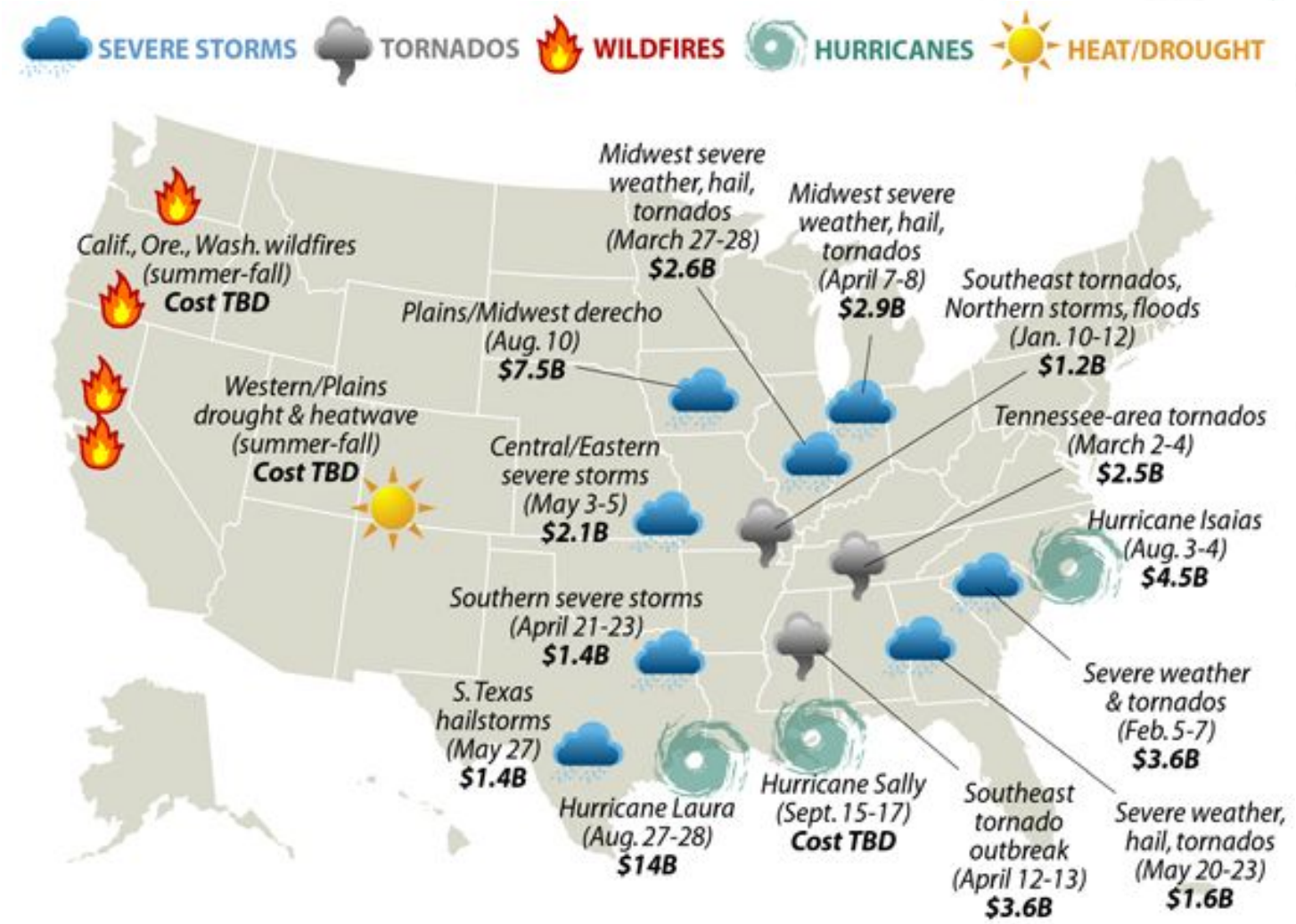
Emma M Stewart

- Actually touching wires: Scottish Power, Scottish and Southern
- Education: MEng, PhD – Electrical, Mechanical, electrochemical Engineering
- SNL/LBNL/LLNL/INL (NL bingo card)
- DNV GL – renewable interconnection
- NRECA – Chief Scientist for 900 utilities
- @turbo81

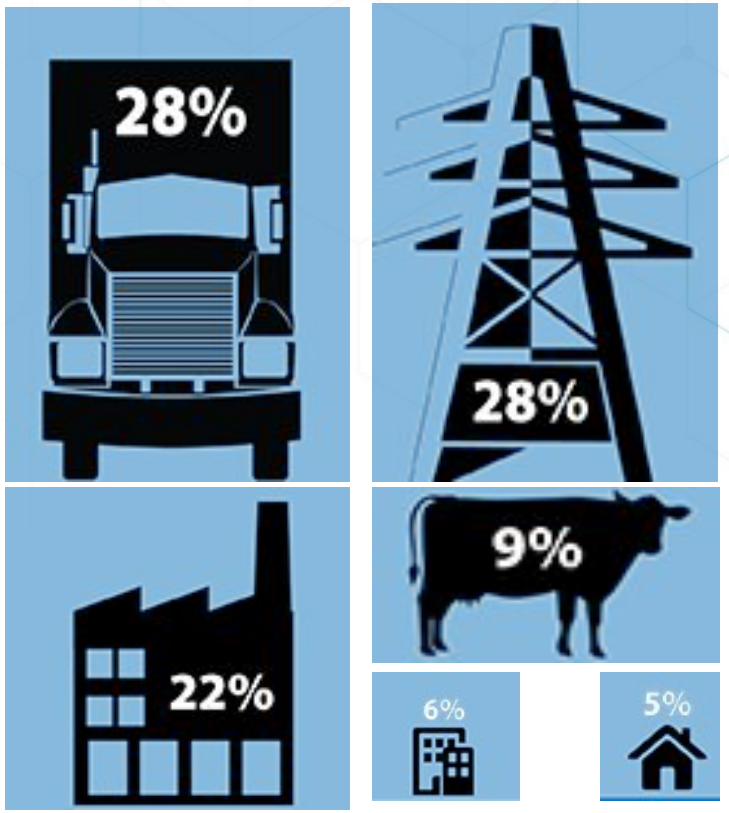
Outline

1. Intro – energy transition & what is means
2. Canon Event
3. Supply Chain for digital components and PRC
4. So?
5. Can we fix it?
   - Banning Products
   - Rip and Replace
   - Regulation
   - Inspections and Right to Repair

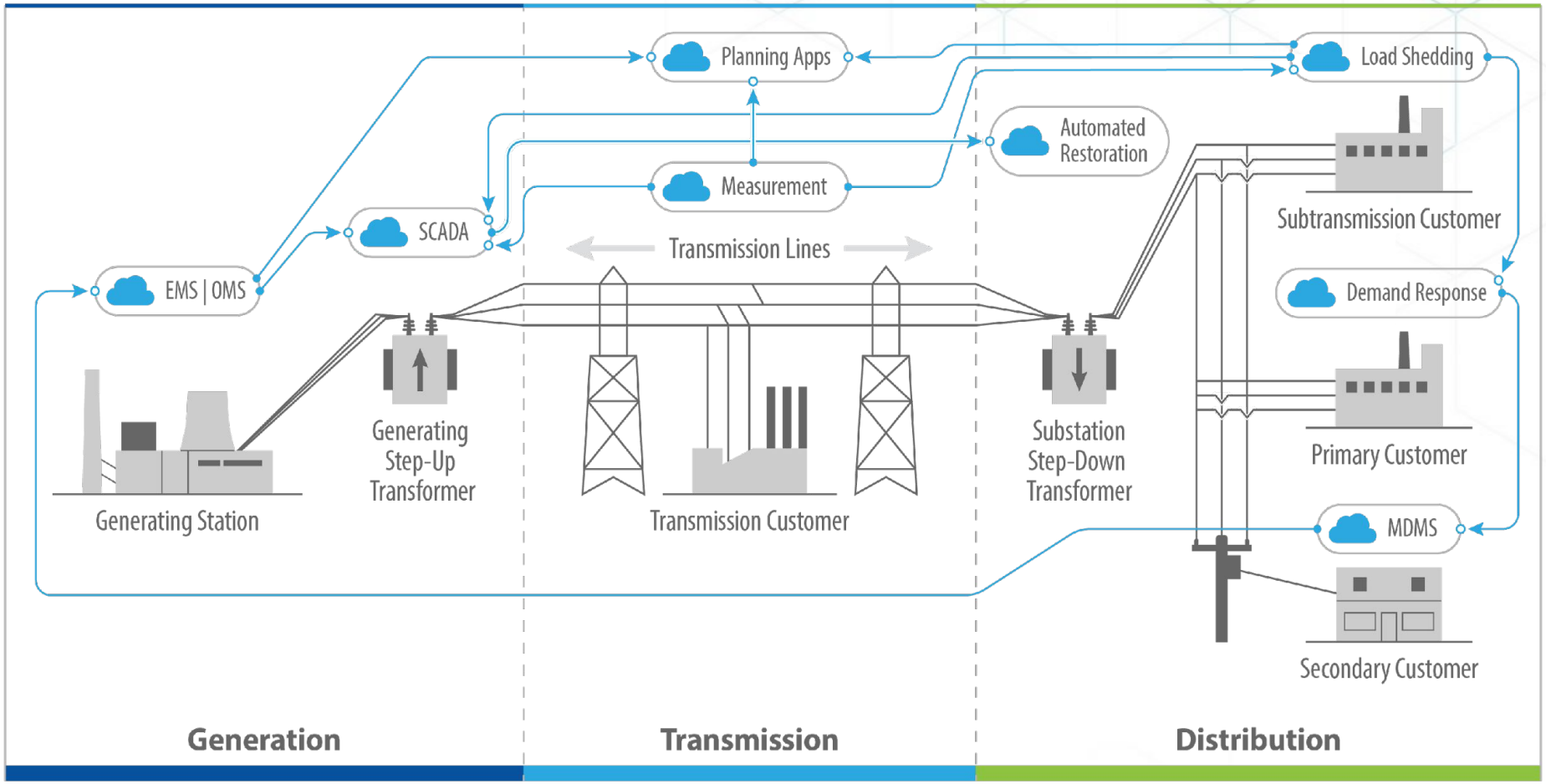
Energy Transition & Climate: Its not getting better

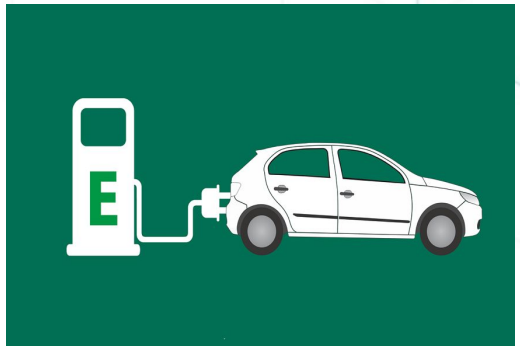


Total US GHG by Sector



The new grid 101





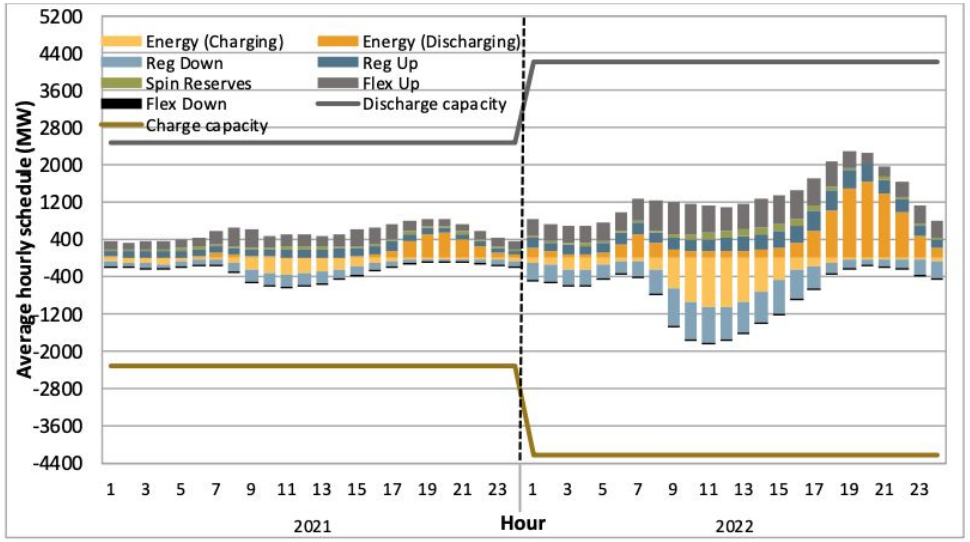
What does Energy Transition Mean: Technology

Big spinning machines with traditional manufacture largely US based

Massive distributed connected solid state machines with largely PRC manufacture

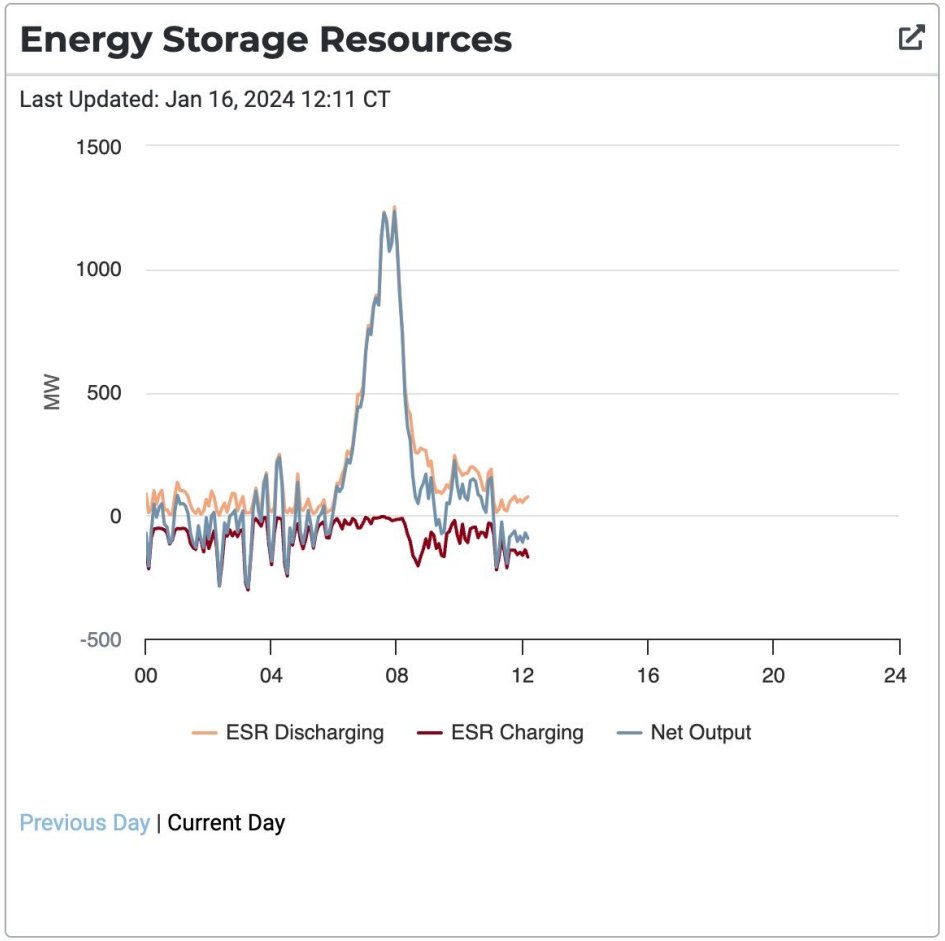
If you like the lights being on today…

MGM has the biggest solar rooftop in the country. The strip is buying 100% renewable energy. Resorts World, convention center etc all served by at least 23% solar and storage



17 emergency dispatches in 2023 in CA

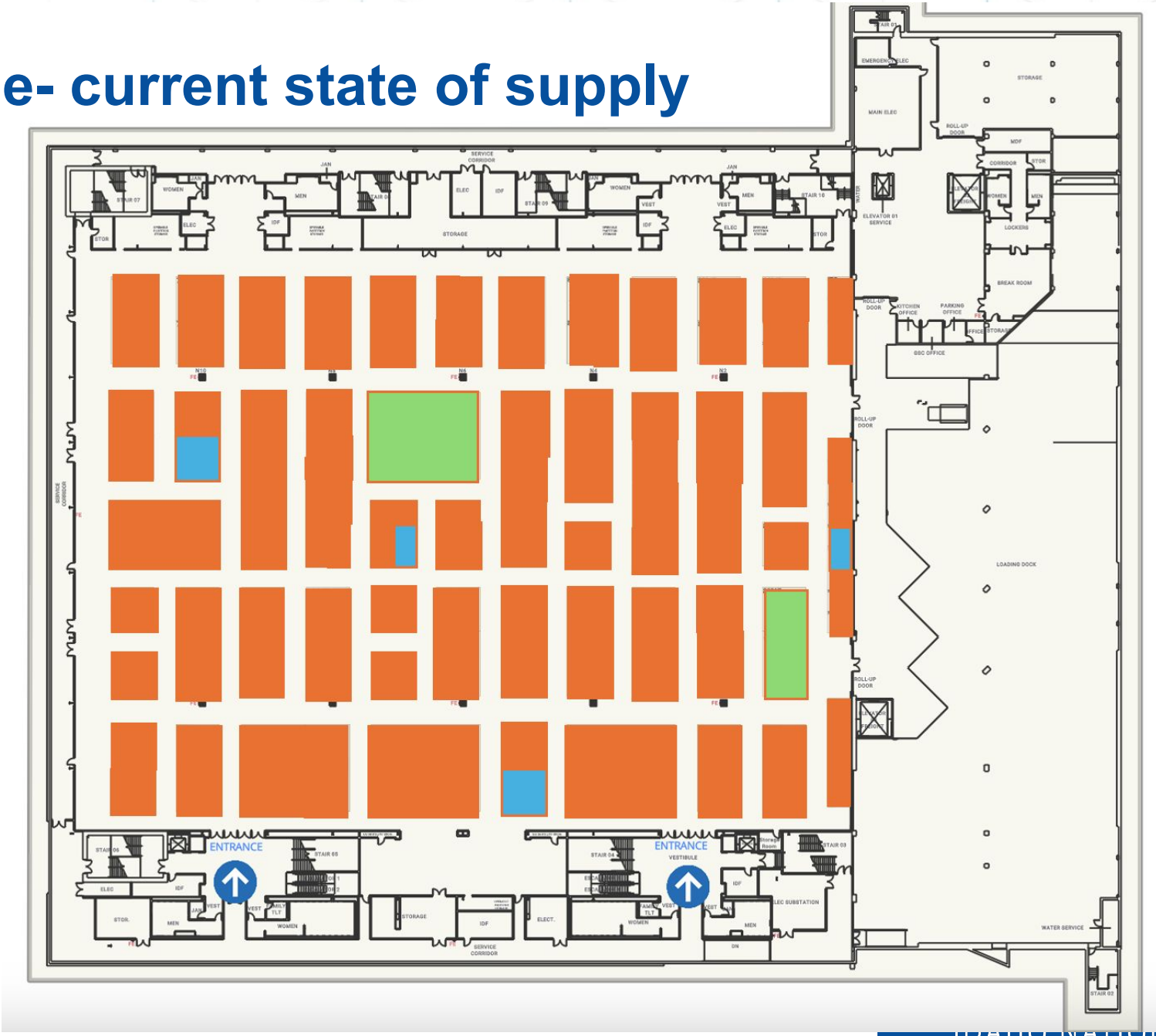
(Ref: CAISO Report on 2022 Heat Event)



Batteries save the day in TX (ref: ERCOT)

2023 Surprise- current state of supply

- 95 to 100% of digital components available currently for new generator control systems have a PRC made, owned, derived control or software component



Biggest North American Renewable Conference – show floor (orange = prc company)

Battery Supply Chain in the News – Canon Event

NATIONAL DEFENSE AUTHORIZATION ACT
FOR FISCAL YEAR 2024

cles.
Sec. 154. Prohibition on availability of funds for procurement of certain batteri

April ‘23

Cybersecurity

FBI says Chinese hackers preparing to attack US infrastructure

By Christopher Bing
April 18, 2024 2:12 PM PDT · Updated 4 months ago

Dec ‘24

NEWS

California solar-plus-storage project with world’s largest BESS fully online

By Cameron Murray
January 24, 2024

US & Canada, Americas Grid Scale Business

LinkedIn Twitter Reddit Facebook Email

Now

Duke Energy disconnects CATL batteries from Marine Corps base over security concerns

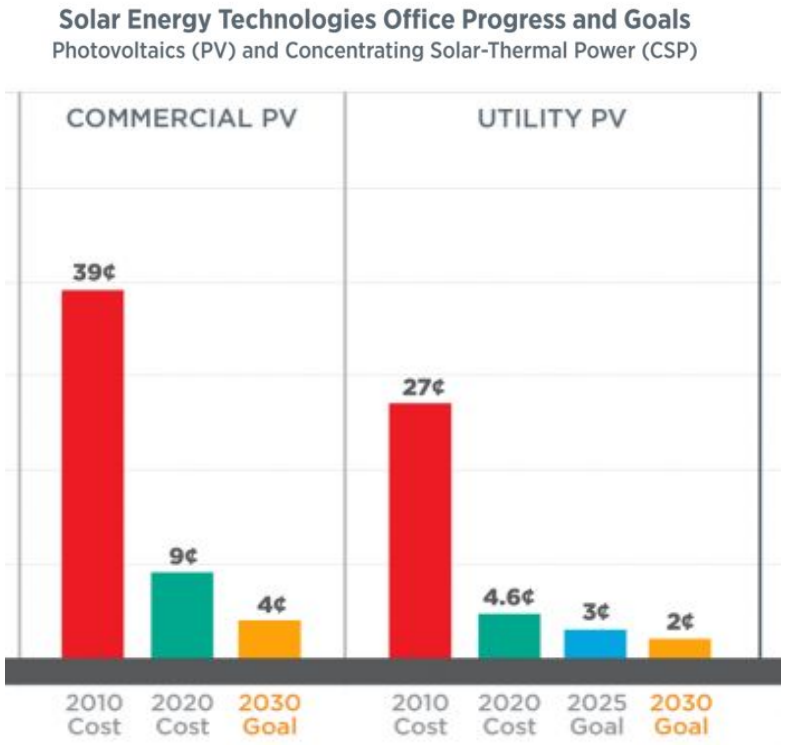
By Michael Martina
December 7, 2023 1:34 AM EST · Updated 8 months ago

Pentagon says it's impossible to ditch Huawei telecom gear — officials beg Congress for waiver from Chinese sanctions

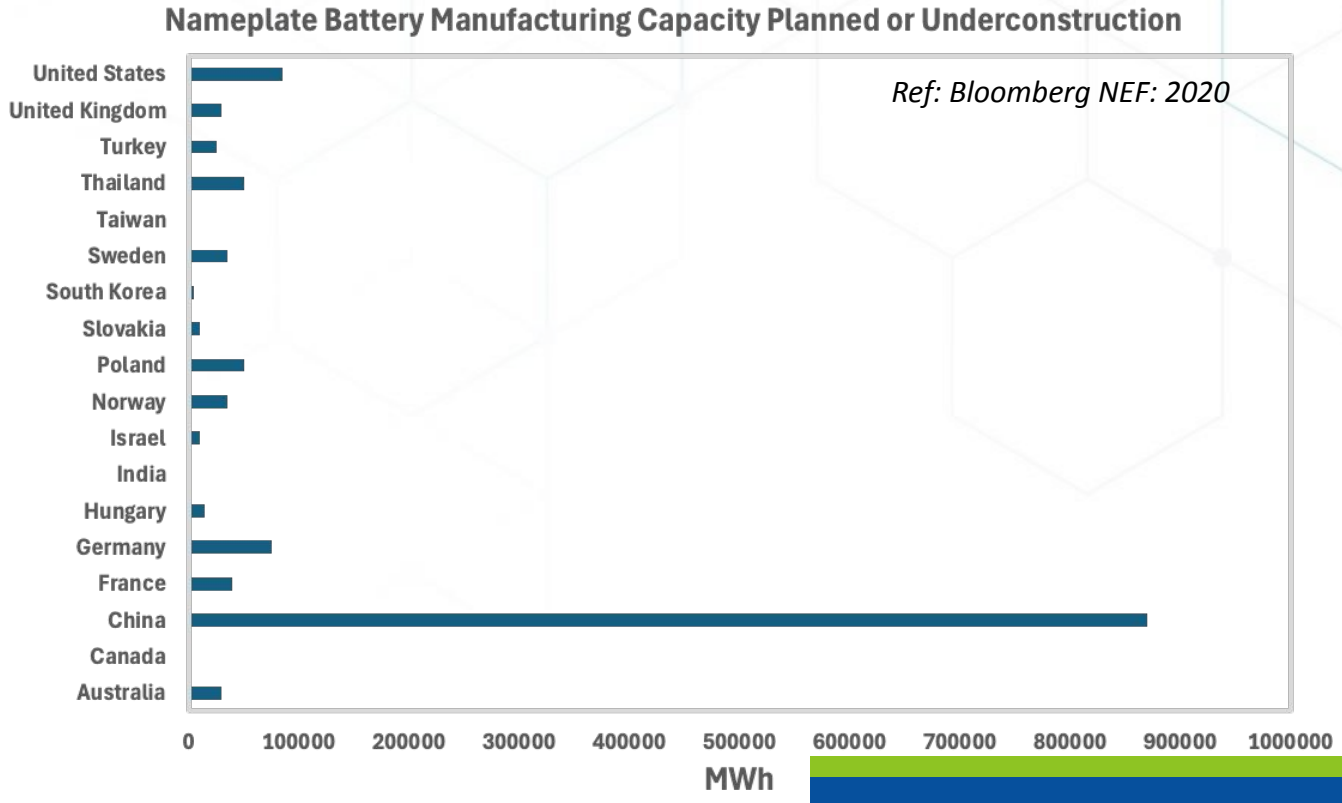
Jeff Butts
July 5, 2024 · 2 min read

How did we get here: Cost and Volume

- Prioritized low cost and volume
- China spent time, made quality performing product
  - Market is flooded



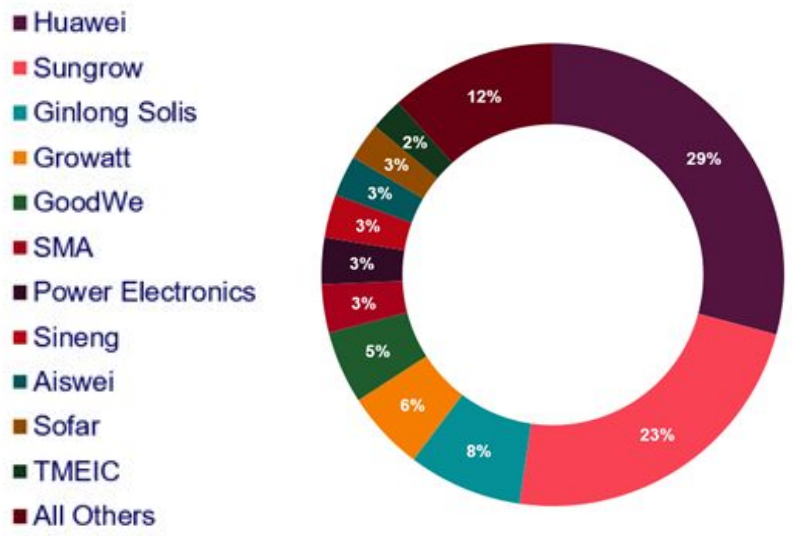
- We just do not build this in the US
  - Might soon – but US investors need a demand signal
- Most of the critical materials are not here



Ref: Bloomberg NEF: 2020

Key Supply Chain Facts and Figures

- **What makes this different to traditional power grid equipment? ….Volume & Regulation**
- **73+ Named Inverter Manufacturers**
- **80+ battery vendors,**
- **Both US integrators and PRC Integrators for PRC equipment exist**
- **Majority of mature solar inverter OEMs also supply EVSE, Small BTM Batteries, Solar Products, BMS**
  - And a lot of this is the same hardware with a different label
- Power Conversion, Inverter Suppliers and BMS – are often the same hardware
- Remote communications/access is needed for maintenance
  - If we don't patch somehow, its just as insecure



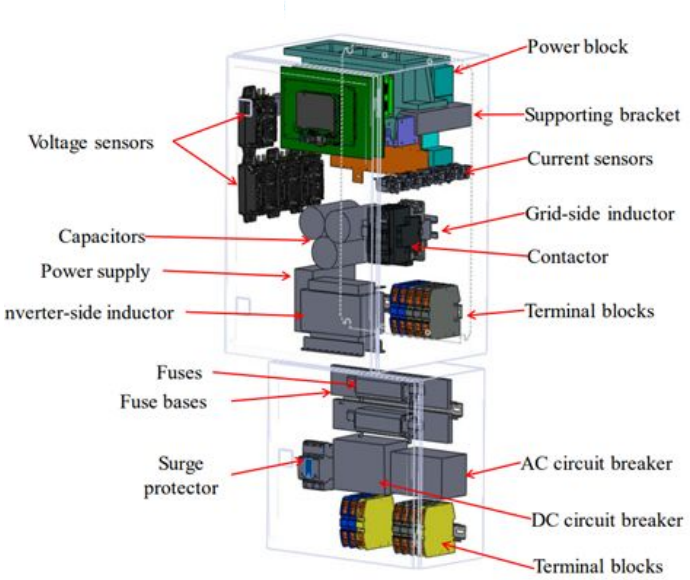


Figure 59. Inverter assembly with supporting components.

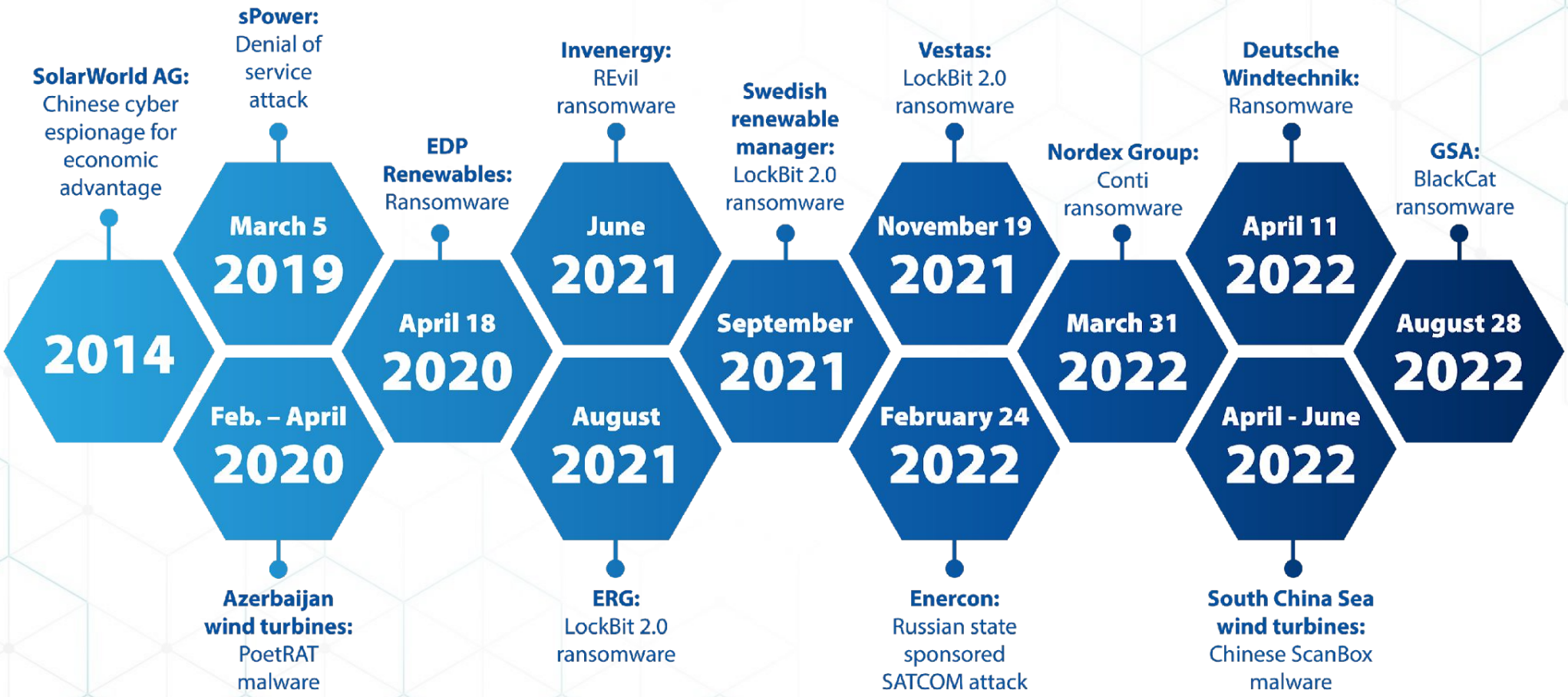
Common Challenges in Procurement & Integration of renewable control systems

1. Failing Chips
2. Persistent Communications
3. Hardcoded Passwords
4. Operation & Maintenance Models
5. White Labeled Products
6. Insecure Apps & Support Software
7. No SBOMS or HBOMs
8. Unknown supply chain ‘Spiderweb’ for integrated systems
9. No PSIRT or vulnerability disclosure/analysis

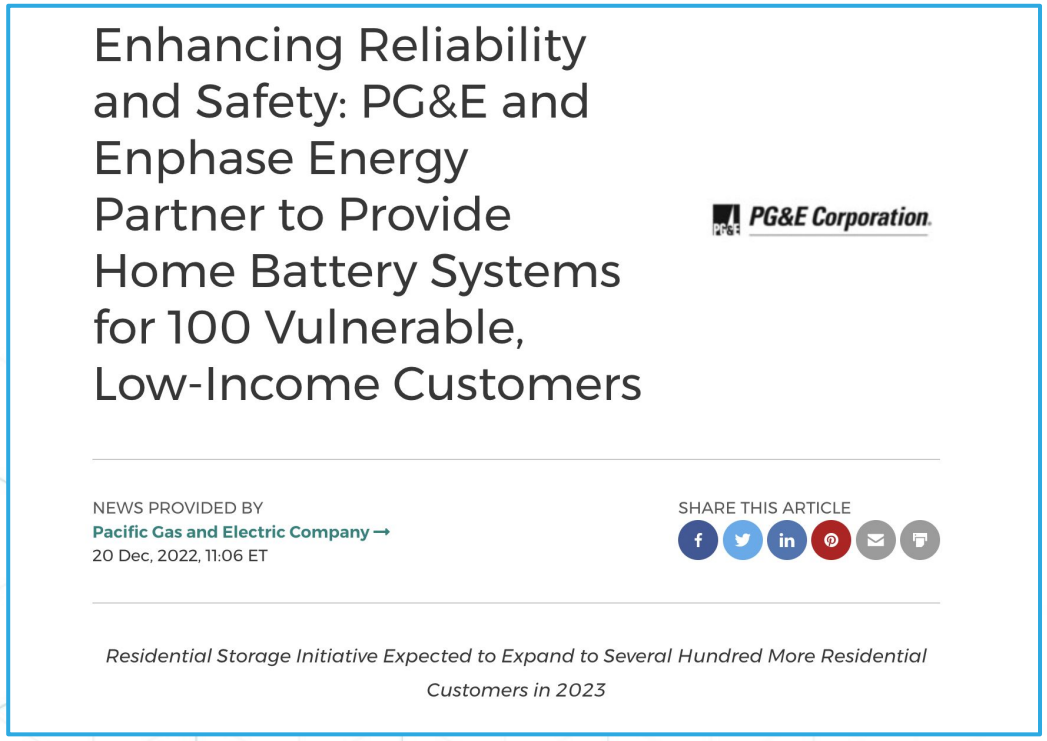
Common Challenges in Procurement & Integration of renewable control systems – PRC++

1. **Failing Chips**
2. **Persistent Comms**
3. **Hardcoded Passwords**
4. **Operation & Maintenance Models**
5. White Labeled Products
6. **Insecure Apps & Support Software**
7. **No trusted SBOMS or HBOMs**
8. Unknown supply chain ‘Spiderweb’ for integrated systems
9. **No PSIRT or vuln disclosure/ analysis**

Renewable Energy is a Target: Clean Energy Related (IT) Events 2014 – 2022



We put the responsibility for securing the grid on the consumer ….



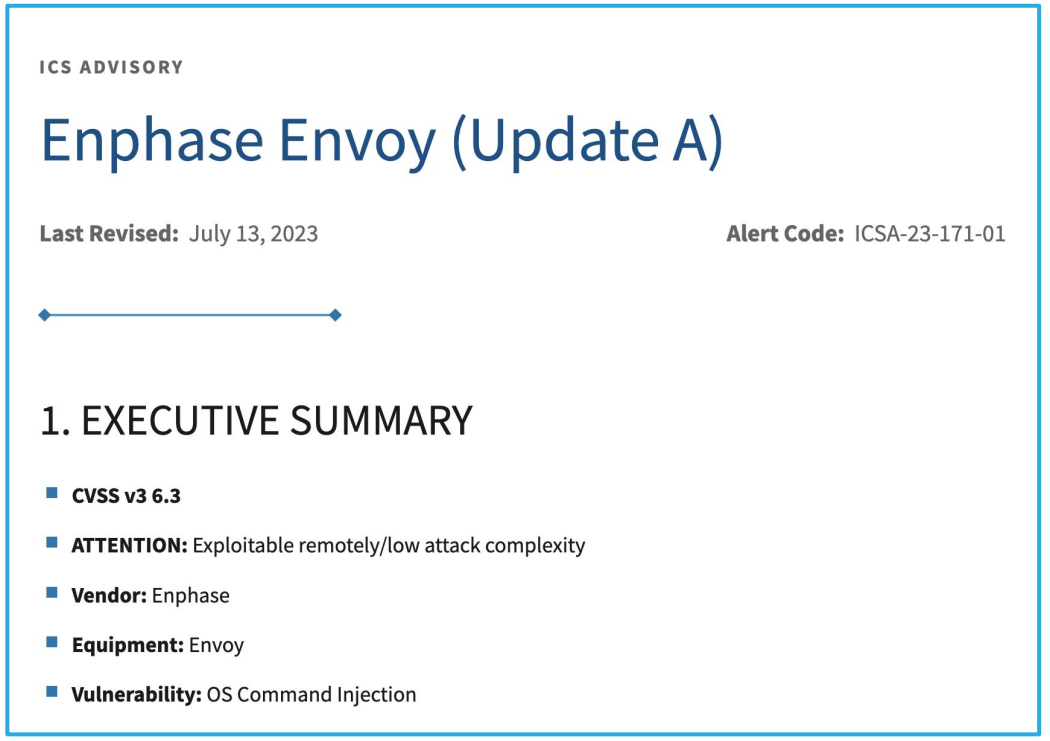
Enhancing Reliability and Safety: PG&E and Enphase Energy Partner to Provide Home Battery Systems for 100 Vulnerable, Low-Income Customers

PG&E Corporation

NEWS PROVIDED BY
Pacific Gas and Electric Company →
20 Dec, 2022, 11:06 ET

SHARE THIS ARTICLE

Residential Storage Initiative Expected to Expand to Several Hundred More Residential Customers in 2023



ICS ADVISORY

Enphase Envoy (Update A)

Last Revised: July 13, 2023

Alert Code: ICSA-23-171-01

1. EXECUTIVE SUMMARY

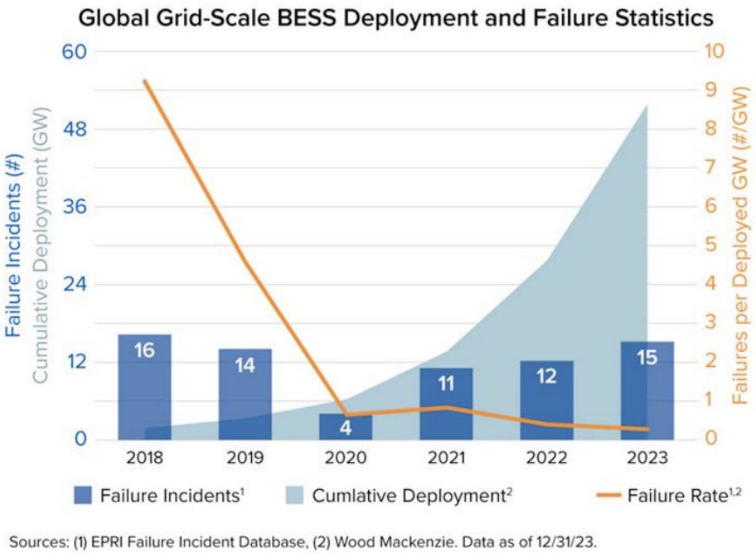
- **CVSS v3 6.3**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Enphase
- **Equipment:** Envoy
- **Vulnerability:** OS Command Injection

The OT/ICS landscape for supply chain attack in inverters – looks more like this

- Common (and useful) feature
- Mass firmware pushes to devices
- Software related grid events have happened, they weren't cyber attacks
- But mass pushes been used to hot fix issues

Technically… some of what makes them a risk is also a benefit, and quality is increasing

- CAISO and WECC 2022-2023:
  - Poor commissioning, bad data, miscoded inverter behavior led to grid event with IBR/BESS
  - Fixed with software and policy changes



Sources: (1) EPRI Failure Incident Database, (2) Wood Mackenzie. Data as of 12/31/23.

bess

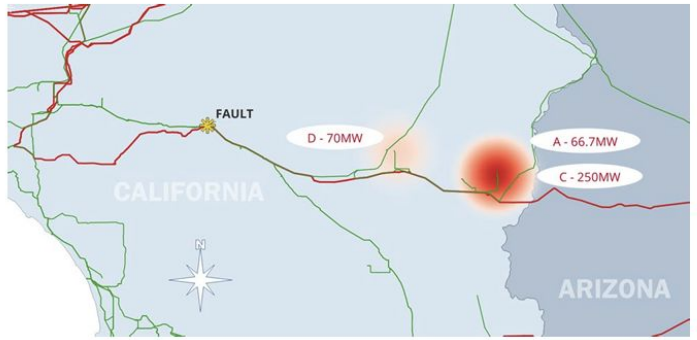


Figure 1.1: Map of the Fault Location and Affected IBR Facilities—March 9, 2022

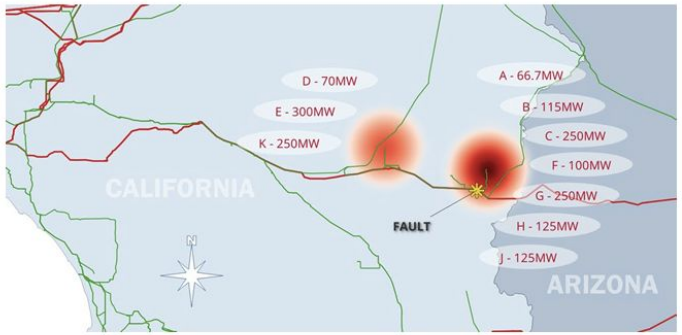


Figure 1.2: Map of the Fault Location and Affected IBR Facilities—April 6, 2022

So what?

- We are dependent on these products for energy security currently
- There is some bad bad, intrusive comms, hard coded passwords, questionable software
- Overconcentration of PRC products - everywhere
- Global issue – cyber event could have global consequence – supply chain attack wouldn't just be here
- We have zero control over the supply chain for these products – private businesses and market control

Potential Impacts of Attacks on Batteries - Loss of visibility

- Loss of status monitoring
- Loss of capacity monitoring
- Loss of activation or inactivation control
- Loss of physical access alarms

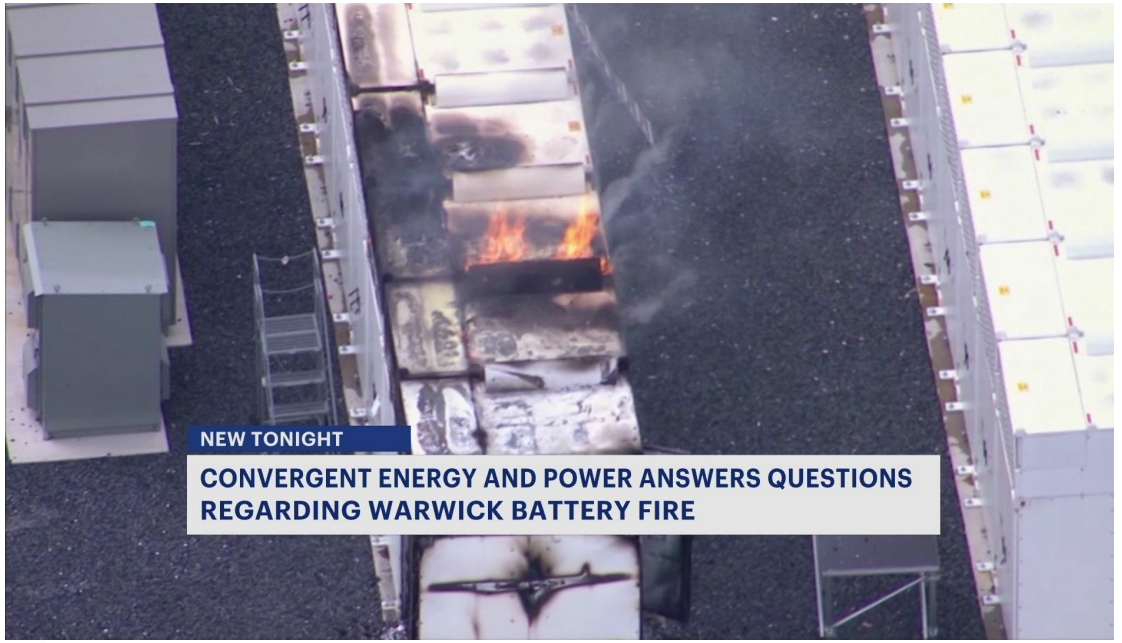
Likelihood vs Difficulty:
Single Site - Low
Mass Event – More likely, medium difficulty
Communications attack only

Examples of this actual events:

- Attack against the ViaSat KA-SAT network (2019)
  - Russian state-sponsored actors in attack coordinated with invasion of Ukraine
  - DoS caused by an attacker exploiting a VPN appliance misconfiguration
    - Allowed for rewriting of flash on customer modems
    - Required replacement devices
- Caused loss of remote monitoring of 5,800 ENERCON wind turbines

Potential Impacts of Attacks on Batteries - Asset Health, Site Damage, Environment

- Site (uncontrolled) Fire
- Loss of preventative/proactive disconnect
- Damage to Battery Components & Site
- Damage to Battery Site Capacity
- Environmental Discharge / Damage



Likelihood vs Difficulty:
Single Site - Medium
Mass Event – Less Likely, Very Difficult
Firmware and Communications, plus other coordinated infrastructure impact

Potential Impacts of Attacks on Batteries - Electric Grid/Bulk Impact

- Loss of Control (doing the opposite)
- Power system stability & ancillary services
- Emergency Dispatch failure/loss of load
- Reputational damage
- Uncontrolled re-energization
- Loss of life
- Financial Loss

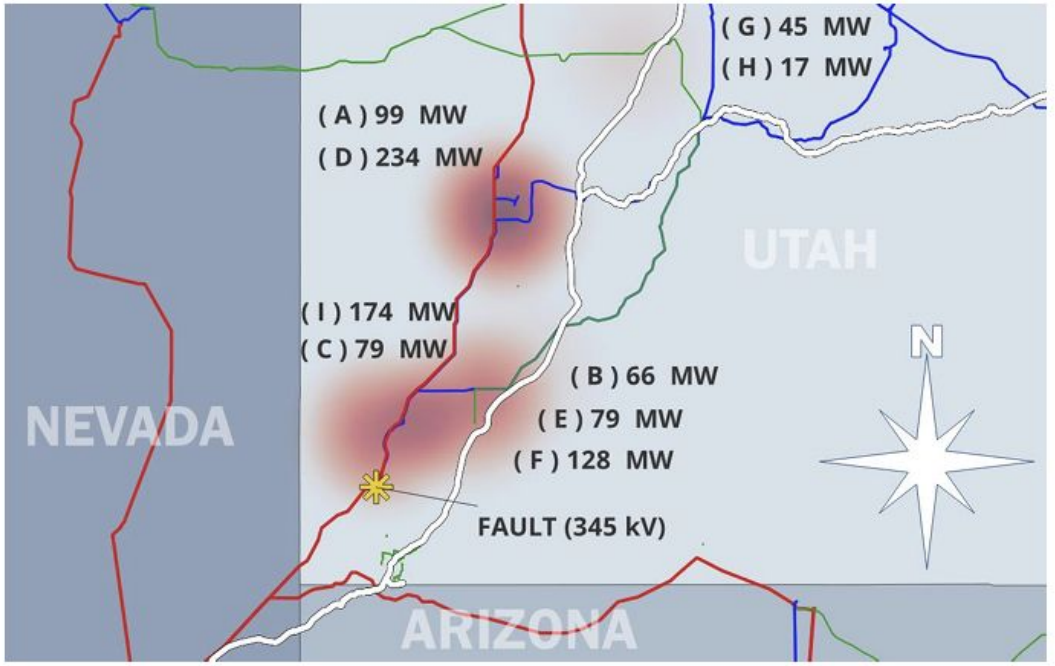


Figure I.3: Map of Fault Location and Affected Solar PV Facilities

Utah IBR
Misop 2022

Likelihood vs Difficulty:
Single Site - Medium
Mass Event – Less Likely, Very Difficult
Firmware and Communications, plus other coordinated infrastructure impact, and power electronics synchronization

OK… so can we fix it? Options….

Option 1: Ban the companies

We are going down this path

Business News › News › International › World News › US lawmakers call to add China's CATL, Gotion to import ban list, WSJ reports

US lawmakers call to add China's CATL, Gotion to import ban list, WSJ reports

Reuters • Last Updated: Jun 08, 2024, 01:20:00 AM IST

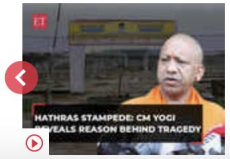
FOLLOW US SHARE FONT SIZE SAVE PRINT COMMENT

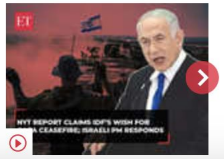
Synopsis
Republican lawmakers are urging the addition of Chinese battery companies CATL and Gotion High Tech to an import ban list, alleging their supply chains use forced labor. CATL and Gotion are linked to Ford and Volkswagen respectively. The lawmakers want them added to the entity list under the Uyghur Forced Labor Prevention Act, which restricts imports tied to alleged genocide in China's Xinjiang region. CATL and Gotion deny the allegations. Volkswagen says it has no evidence of human rights violations.

Chinese battery companies CATL and Gotion High Tech should be added immediately to an import ban list, a group of Republican lawmakers said, alleging their supply chains use forced labour, the Wall Street Journal reported.

The lawmakers called for CATL and Gotion, which have ties to Ford and Volkswagen respectively, to be added to

Videos





The Ban Process Has Started…

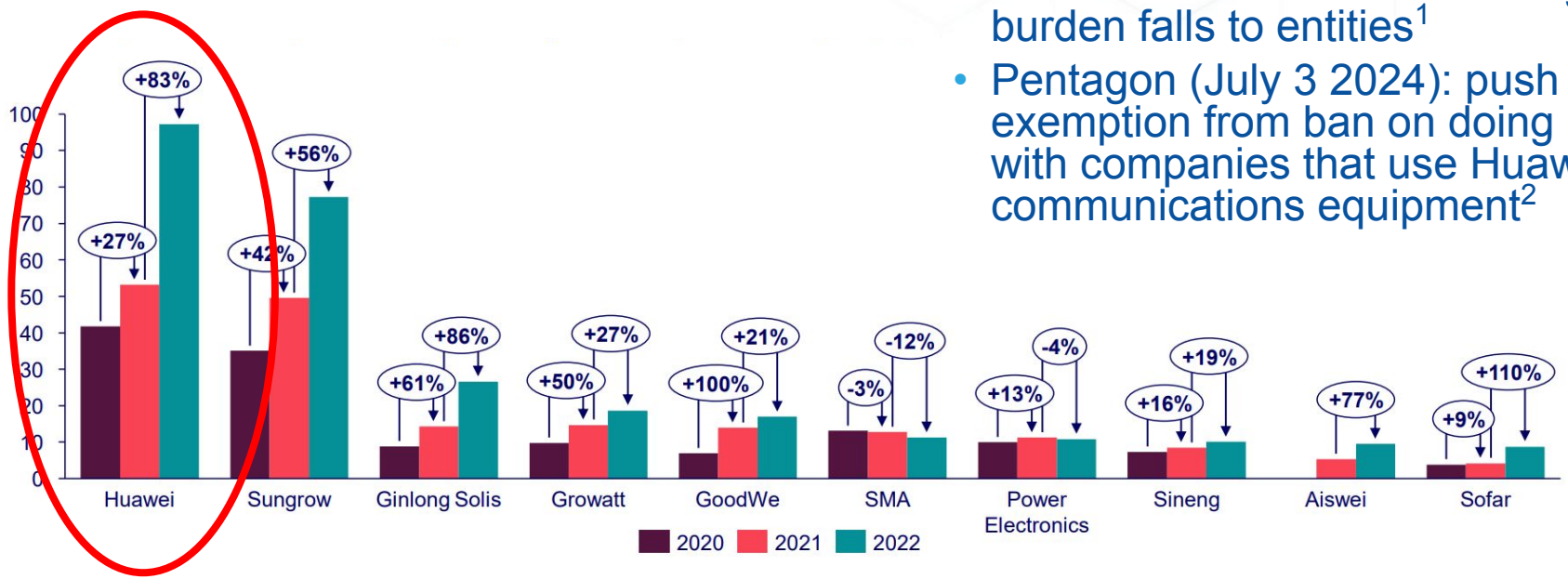
FY24 NDAA, Section 154: Prohibition on Availability of Funds for Procurement of Certain Batteries

Option 2: Rip and Replace

History: The Secure and Trusted Telecommunications Networks Act – Rip and Replace Huawei & ZTE

- Can't buy it
- Funding for small rural entities to replace it

- Cost to remove was estimated at around $4B, primarily from small rural entities
- Current State: Shortfall in budget of $3B, burden falls to entities[1]
- Pentagon (July 3 2024): push for exemption from ban on doing business with companies that use Huawei communications equipment[2]

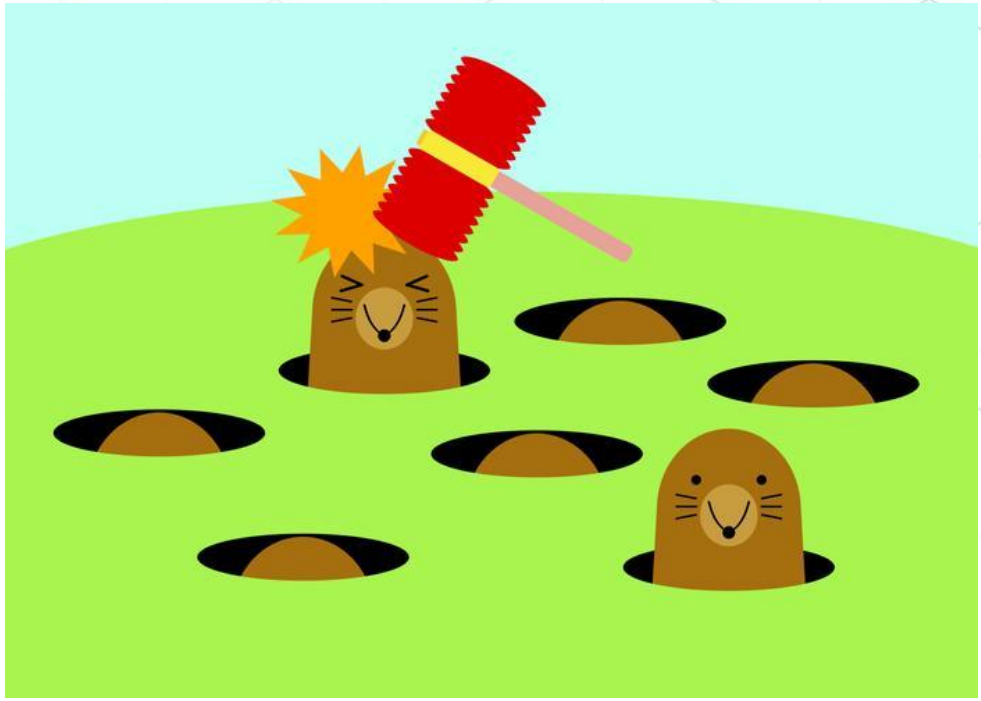


2022's Top 10 vendor shipments and percentage increase, 2020-2022 (GW, %)

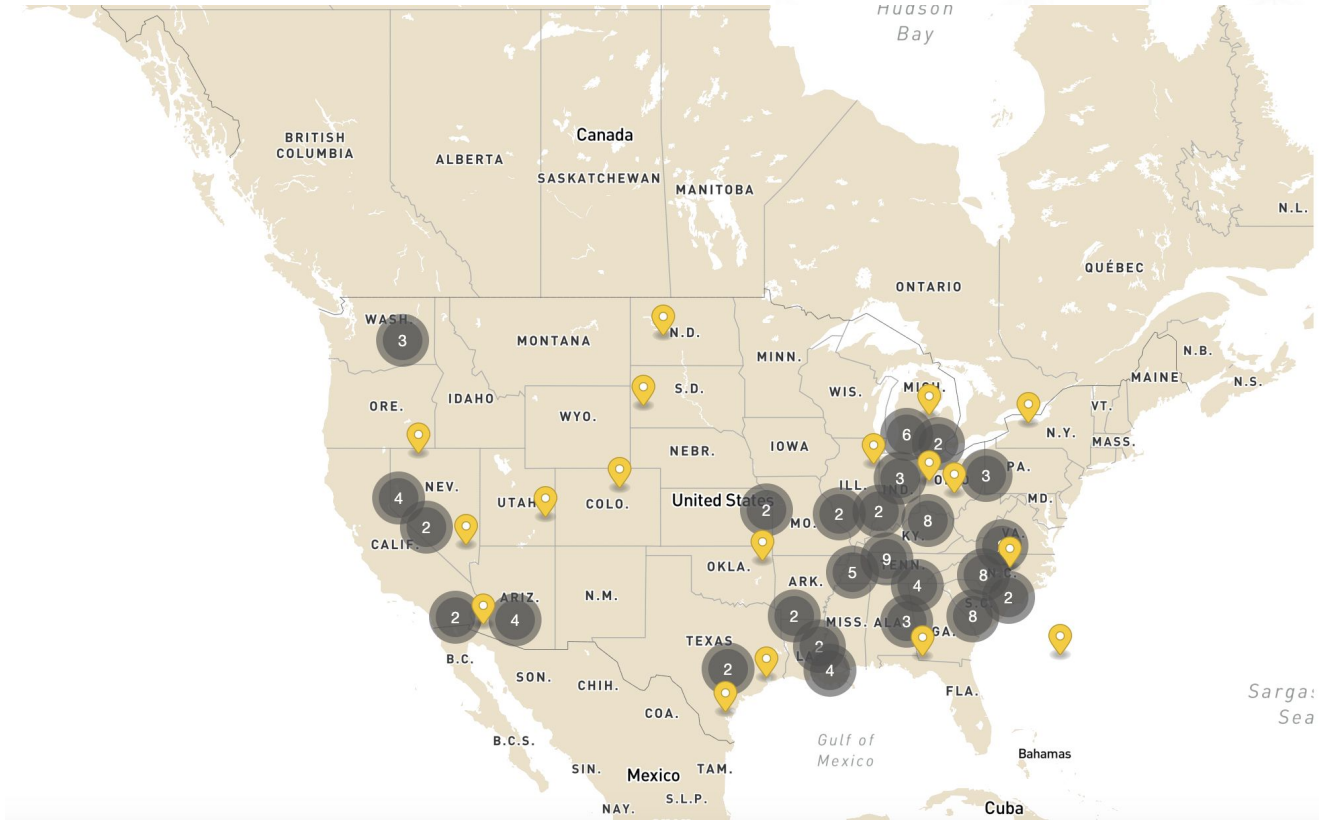
1. https://www.washingtonpost.com/technology/2024/05/02/huawei-rip-remove-order-threatens-service/
2. https://www.bloomberg.com/news/articles/2024-07-03/pentagon-has-a-huawei-dilemma-congress-doesn-t-want-to-solve

Rip and Replace – now?

- $4B, 4 years to replace one US state's batteries alone
- There are over 70 options currently for Chinese Made BESS
  - Average time from launch to integration is ~1 year
  - Whack a mole forever more
- Batteries do have a fire issue
  - Most common name in fire's recently in the US – doesn't use these vendors
  - Those are real events – environment and people have been hurt
  - But they aren't on the list…



There is progress: Investment is happening (but it will take a while)

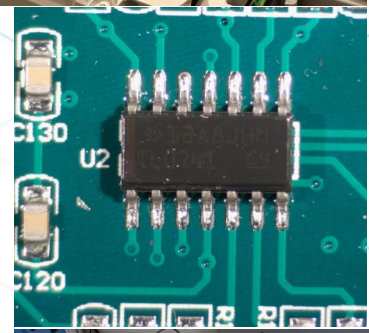


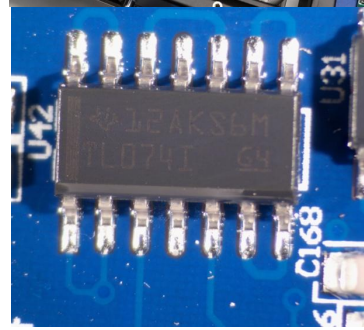
CHIPS for AMERICA

Nov 2023 – U.S. Department of Energy (DOE) announced up to $3.5 billion from the Infrastructure Law to boost domestic production of advanced batteries and battery materials nationwide

https://www.energy.gov/invest

Option 3: Authority and Ability to Inspect /Repair





- Develop the right to inspect and repair the devices and systems
  - And remove bits
  - Contract & policy issue – not tech
- Analyzing the Hardware and Software
  - Create SBOMs, HBOMS
  - Vulnerability Assessments & reporting
  - Firmware escrow before delivery
- Accountability and responsibility for critical infrastructure components lays on the buyer, not the seller
- Actual vulnerability analysis and PSIRT teams for US integrators could be enabled and solve the issues
- Batteries and power electronics also come with some safety issues
- Consumer Electronics made progress
  - But not in energy…

Option 3: Inspection, assessment and evaluation

- **Deterrence** – we will inspect your stuff
- **For safety and performance** – the industry have standards and labs
- ….but we let companies test their own products
- **For cybersecurity & supply chain**– we do not have mature standards and labs
- Safety and Warranty implications
- Contract protections for smaller entities are harsh and protect China
- But… they will do it to us (Steal IP) – acceptable risk trade off?

UL Solutions and CATL Join Forces to Advance Battery Energy Storage System and EV Battery Safety and Performance

Inverters Vulnerabilities – a maturing industry, but only in the US

Contec SolarView

- **CVE-2023-27512:** use of hard-coded credentials may allow remote authenticated attacker to login with administrative privilege

Fronius

- **CVE-2019-19228:** Solar inverter allows attackers to bypass authentication because the password is stored in a plaintext file

Enphase

- **CVE-2020-25752:** Hardcoded web-panel login passwords for the installer and Enphase accounts. Users are unable to change these passwords

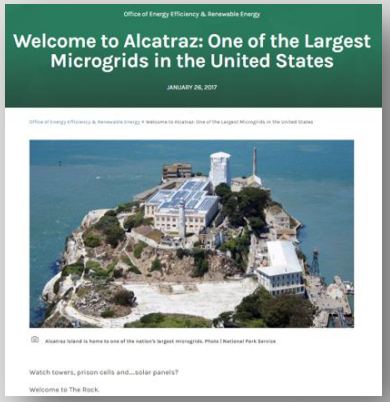
Contract teeth: Configuration, Design Requirements & Supply Chain

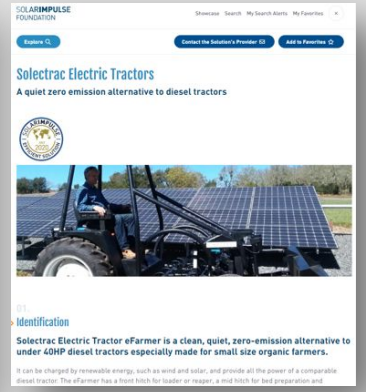
Better configurations could mitigate ~70 to 80% of the biggest consequences

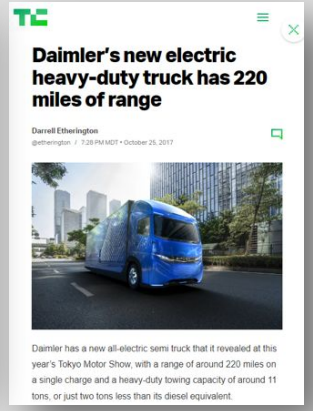
- Strong password requirements
- Firewall and Firmware DMZs
- Don’t put it on the internet
- US Based O&M
- Monitor it
- External sensing for highest consequence scenarios

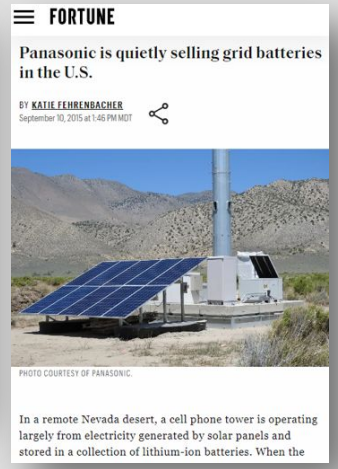
Option 4: Regulate

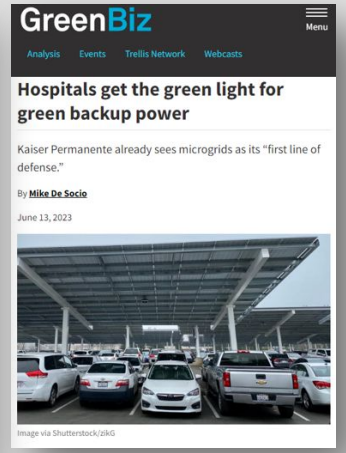
How? Who is in charge of clean energy security?





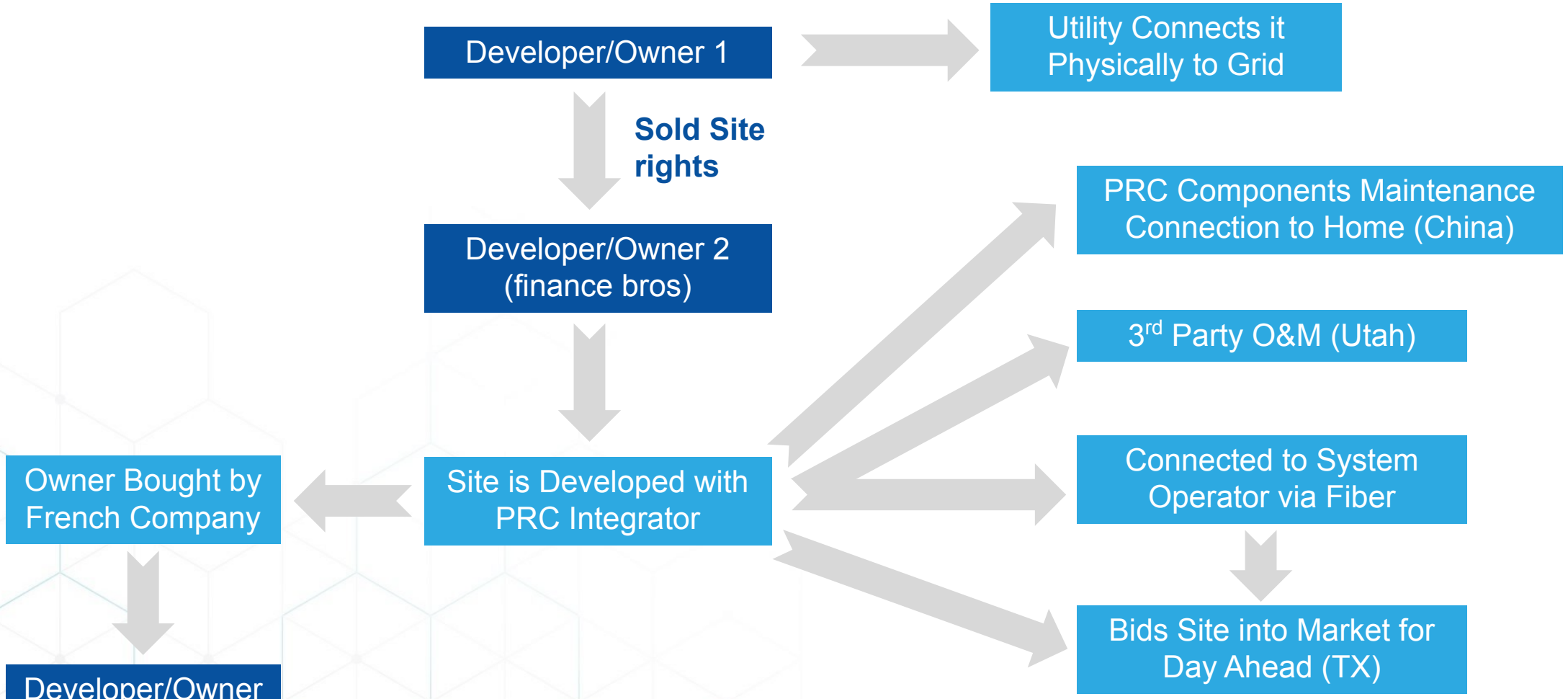






Source: GAO analysis of Presidential Policy Directive-21. | GAO-23-105806

Regulate: Who?



What if..

CVSS 10 vulnerability… is identified and published for all Sunsplat inverters in the aggregators pool

Brick would cost aggregator ~$26M to fix/replace

They can push the firmware, comms are maintained, but risk: reboot takes 10 mins, 5 mins to reconnect

Emergency Mass Push… everything bricks

Who is locally responsible → **its determined the devices need a local reboot**

Incident Communications between who? Aggregator? Distribution Muni? Law Enforcement? → **Is the Distribution utility responsible now to fix locally? (fuses popped with step load increase)**

What would be expected of the equipment provider to support? → **Someone died because of the distribution loss: Who is responsible/liable?**

What regulatory or legal requirements could fix this?

Summary

- The adoption of renewable energy sources is increasing across all critical infrastructure sectors, such as hospitals, communication systems, water, transportation, military installations, and even retail stores.
- The presence of adversarial entity suppliers in the renewable energy supply chain is a significant concern, but not going away
- We can fix this, both in the short and long term
- Policy and Technical mitigations need to align

1. Force inspection and assessment
2. Rationalize regulation and oversight around the “new school”
3. Configure it right….
4. We can safely integrate this equipment, we don’t have a choice, we need the right structure and services to do it (we just need to use them)

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.