You may delete this page from the document that follows after reading.
It contains plain language about the copyright we've adopted from **Creative Commons**.

It also contains a link to the summary for our copyright license. This summary should be consulted if you intend to copy and redistribute this material in any medium or format, or adapt, remix, transform, or build upon this material.

Click Here for information on the Creative Commons License we've adopted.

From **Creative Commons**:

This is a human-readable summary of (and not a substitute for) the license. Disclaimer.

You are free to:

- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- **Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **NonCommercial** — You may not use the material for commercial purposes.
- **ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

This material is based upon work supported by the National Science Foundation under Grant #1901852. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Introduction to SCADA for Renewables
(A Six Module Course)

Course Learning Objectives

1. **Describe** SCADA system basics and important differences with other control systems
2. **Demonstrate** competency of the key components of a SCADA system and their functions
3. **Describe** the different communication systems used in SCADA
4. **Demonstrate** competency of the role and capabilities of operator interfaces
5. **Demonstrate** competency of implementing SCADA in real world applications, specifically renewable energy applications (install, operation, maintenance)
6. **Identify** emerging technical trends, shifts, and innovations impacting SCADA and its application in the renewable energy sector

Introduction to SCADA for Renewables

Course Outline / Curriculum Learning Modules:

Module 1 SCADA Overview

Module 2 Components and Functionality

Module 3 Basics of SCADA Communications

Module 4 Human/Machine Interface

Module 5 Applications within Renewable Energy Industry

Module 6 Emerging Trends in SCADA for Renewables

Module 6: Emerging Trends in SCADA
Learning Objectives

- **Understand** how various emerging technologies impact RE and SCADA systems
- **Understand s**mart grid architecture
- **Understand** distribution SCADA and advanced applications.
- **Discuss and describe** risks and benefits with advanced SCADA systems.
- **Understand** different types of cyber attacks and risk mitigation frameworks

Introduction

- **Smart grids** are essential to powering the green energy revolution.
  - They take advantage of a range of technological advances, from edge cloud computing and artificial intelligence (AI) to sensors and smart meters, to more smoothly integrate the increasing volume of decentralized and intermittent renewable energy flows.

- However, the more assimilated the energy network becomes with connected Internet of Things (IoT) technology, the greater the risk of cyber attacks.

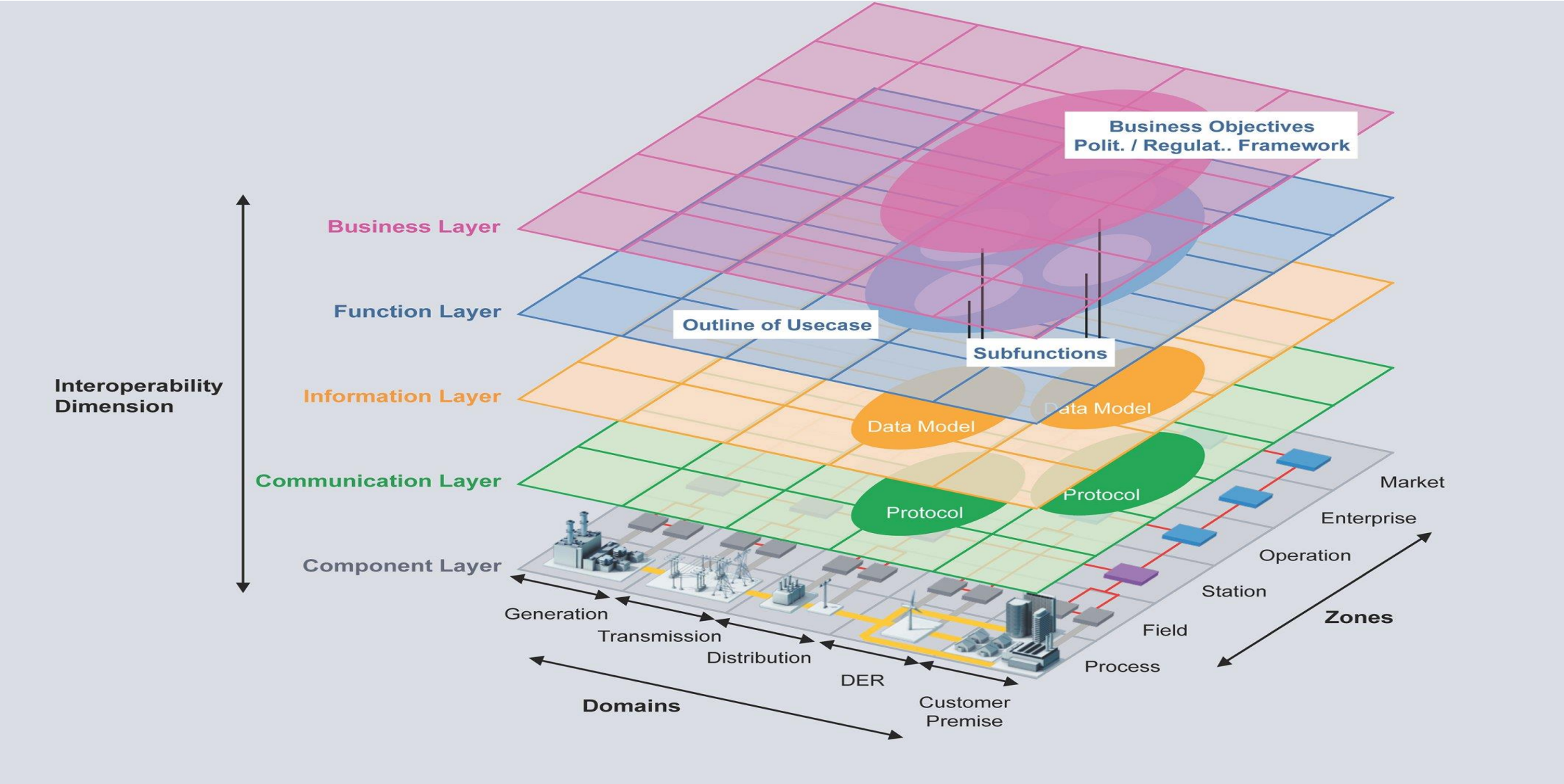
- In particular, the fast data flows needed to pass across highly interconnected communication networks, often facilitated by a mixture of new and legacy infrastructure, can create vulnerabilities in smart grid systems, prompting the urgent need for robust cyber security protection.

- The digitization of the grid, along with renewable energy infrastructure such as solar and wind farms, will serve to enhance the performance, controllability and security of hugely important and strategic assets while building in reliability and resilience.

Smart Grid Architecture (1)

- The backbone system includes SCADA for
  - Generation, transmission and distribution
  - Control centers ●Loads
- A backbone system augmented with "***accessories***", such as
  - Distributed energy resources such as wind and solar
  - Microgrids ●PMUs ●Storage ● Demand response
  - Smart loads and appliances ●Electric vehicles
- The most effective Smart Grid can monitor/control residential home devices and renewable sources that are non-critical during peak power consumption times to reduce power demand and return their function during non-peak hours.

Smart Grid Architecture (2)



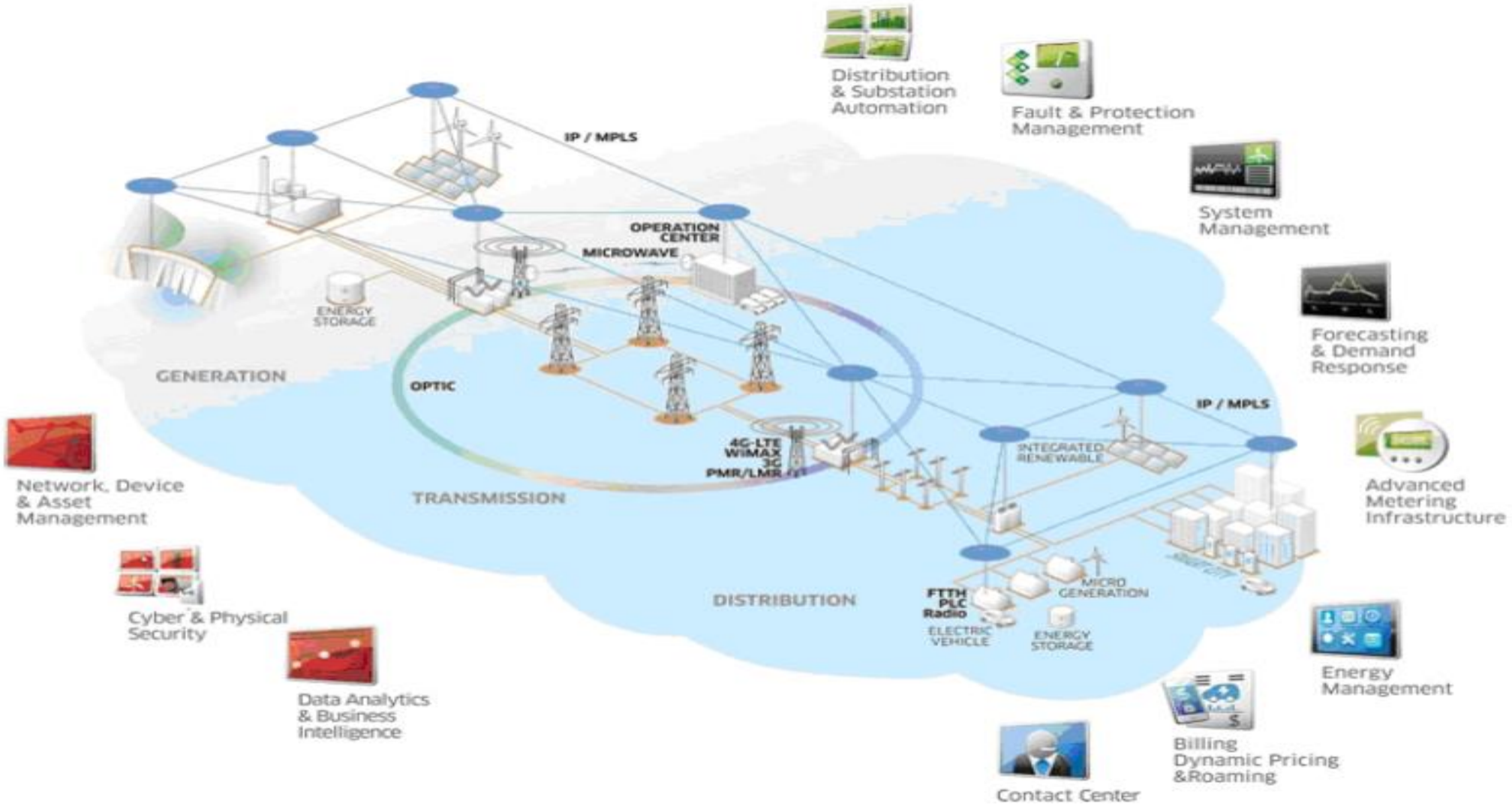
Source: Uslar, M. and Jörn Trefke. “Applying the Smart Grid Architecture Model SGAM to the EV Domain.” *EnviroInfo* (2014).

SCADA/Smart Grid Integration (1)

- SCADA empowers the electricity consumer by interconnecting energy management systems to authorize the customer to manage their own demand of energy and control costs.
- It allows the grid to be self-healing by automatically responding to power quality issues, power outages, and power system faults.
- SCADA optimizes the grid assets by monitoring and optimizing those assets while minimizing operations and maintenance costs.
- The Smart Grid, intelligence and control need to exist along the entire power supply chain.
  - This includes the electricity generation and transmission from beginning to delivery end-points at the customer's side and includes both fixed and mobile devices in the SG architecture.

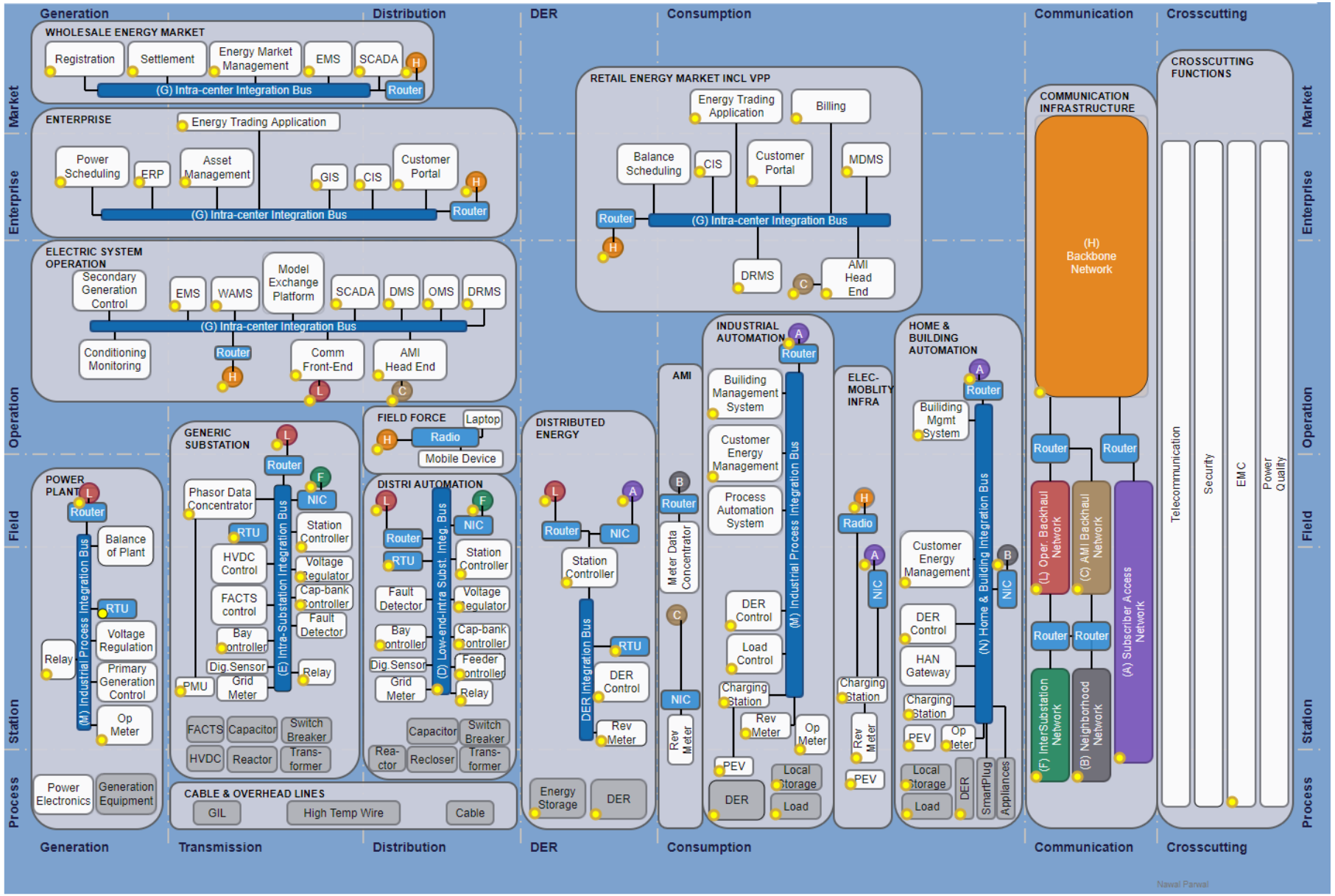
Source: K. Sayed, H.A. Gabbar, Chapter 18 - SCADA and smart energy grid control automation, Editor(s): Hossam A. Gabbar, Smart Energy Grid Engineering, Academic Press, 2017, Pages 481-514, ISBN 9780128053430, https://doi.org/10.1016/B978-0-12-805343-0.00018-8.

SCADA/Smart Grid Integration (2)



Source: K. Sayed, H.A. Gabbar, Chapter 18 - SCADA and smart energy grid control automation, Editor(s): Hossam A. Gabbar, Smart Energy Grid Engineering, Academic Press, 2017, Pages 481-514, ISBN 9780128053430, https://doi.org/10.1016/B978-0-12-805343-0.00018-8.

Advanced SCADA in Smart Grid applications



Source: http://smartgridstandardsmap.com/

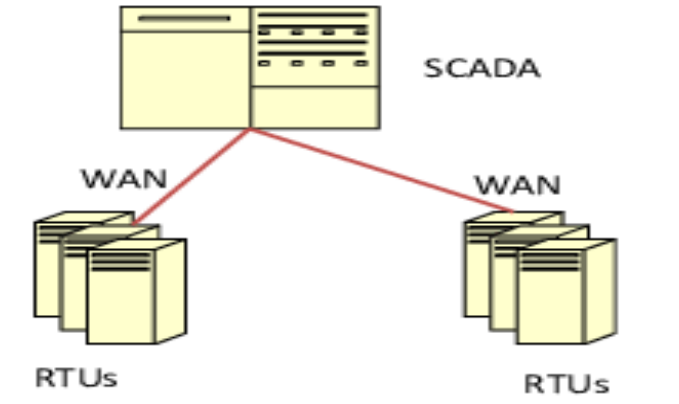
SCADA system – Current Status

- The **SCADA system** is a centralized system that monitors and controls the entire area.
- SCADA architecture is a supervisory system gathers data on the process and sends the commands control to the process.
- SCADA framework is an amalgamation of hardware components and software programs where hardware includes a “Remote Terminal Units (RTU)”, “Master Terminal Unit (MTU)”, actuators and sensors, and software includes “Human Machine Interface (HMI)”, a central database (Historian) and other user software.
- These software provide a communication interface between hardware and software.
- The physical environment is linked to the actuators and sensors which are further connected to RTUs.
- RTUs gather the information and data from the sensors and forward telemetry data to the MTU for observing and controlling the SCADA framework.

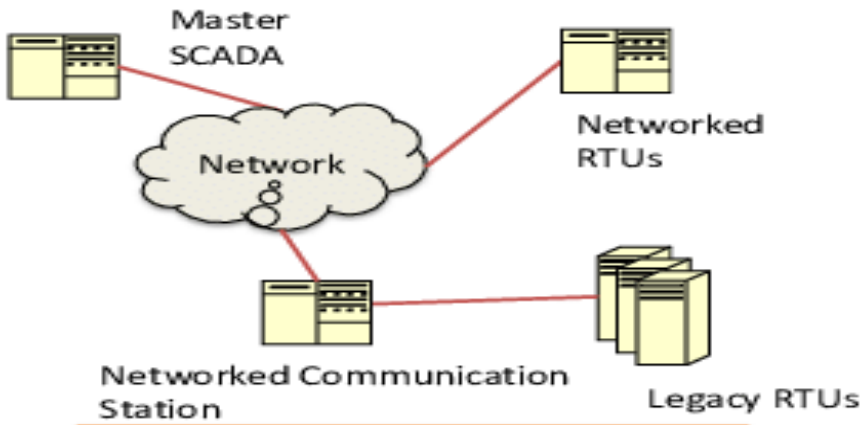
SCADA Network Framework (1)

- Communication network provides communication services between various components in the SCADA network framework.
- The medium utilized can be either wireless or wired. Presently, wireless media is generally utilized as it interfaces geologically circulated areas and less available zones to communicate effortlessly.
- The advancement of communication paradigm is isolated into four primary ages,
  - First era: Monolithic
  - Second era: Distributed
  - Third era: Networked
  - **Fourth era: Internet of things technology.**

SCADA Network Framework (2)



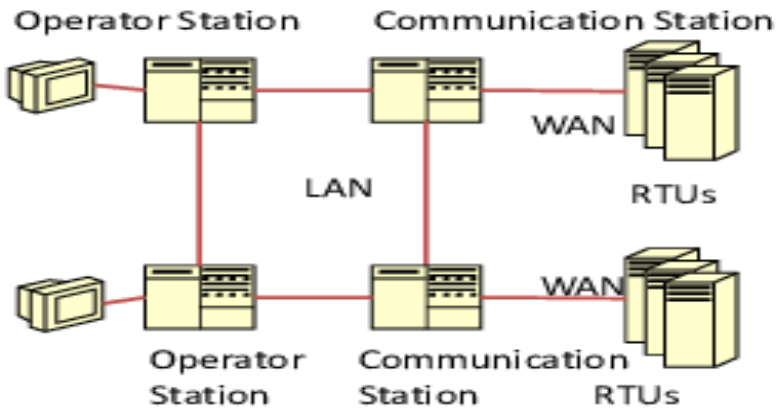
1st generation: "monolithic"



3rd generation: "networked"

1G→2G

- Distributed Processing
- Multiple LAN connected stations
- Real-time information sharing
- Proprietary Protocols
- Cost effectiveness



2nd generation: "distributed"

2G→3G

- Open System Architecture
- Open Protocols
- Mostly WAN Connectivity
- Internet Connectivity

Source: Karnouskos, Stamatis & Colombo, Armando. (2011). Architecting the next generation of service-based SCADA/DCS system of systems. IECON Proceedings (Industrial Electronics Conference). 359 - 364. 10.1109/IECON.2011.6119279.

SCADA Paradigm (1)

- **Monolithic SCADA systems:**
  - refers to those systems which work in an isolated environment and do not have any connectivity to the other systems. The motive of these systems is to work in a solitary way. Large minicomputers were used for SCADA system computing.

- **Distributed SCADA systems:**
  - systems that were inter-connected and confined inside small range network like Local Area Networks (LAN) . This generation distributes the computation overhead on remotely located systems using LAN, i.e., some of the systems work as communications processors.

SCADA Paradigm (2)

- **Networked SCADA systems:**
  - It utilizes networks and web broadly because of the standardization and cost-effective solutions for large-scale systems. This is also referred to as a modern SCADA system. In this design, SCADA systems may be geographically distributed.

- **Fourth generation:**
  - The industries have been utilizing the power of technology to build, monitor and control the systems. Integration of Internet of Things (IoT) innovation and economically accessible cloud computing with SCADA systems has considerably lessened its infrastructure and deployment costs.

Emerging trends in SCADA

- Cloud-based supervisory control and data acquisition (SCADA) systems
- Increased use of analytics
- Subscription/flex licensing: SCADA as a service
- High-performance Human-machine Interface (HMI) and HISTORIAN
  - Allows for pre-attentive processing
  - Provides predictive analytics and regression analysis that will alert your operator days or weeks before a system failure
  - Allows operators to learn from and analyze data without the help of a programmer
- Cellular and 5G
  - seen as reliable backups for primary fiber communication and alternative to traditional radio communications
- Virtualization
  - Reduces capital and operating costs, Allows for system redundancy, Minimizes or eliminates downtime and Simplified data center management

Advanced Smart grid & SCADA Application: Distribution Automation

Distribution Automation technologies and systems can achieve substantial grid impacts and benefits:

- Improvement in location of fault, isolation, and service restoration capabilities
- Improved distribution system resilience to extreme weather events
- More effective equipment monitoring and preventative maintenance that reduces operating costs,
- More efficient use of repair crews and truck rolls that reduces operating costs
- Improved grid integration of selected distributed energy resources (DER) such as thermal storage for commercial and municipal buildings

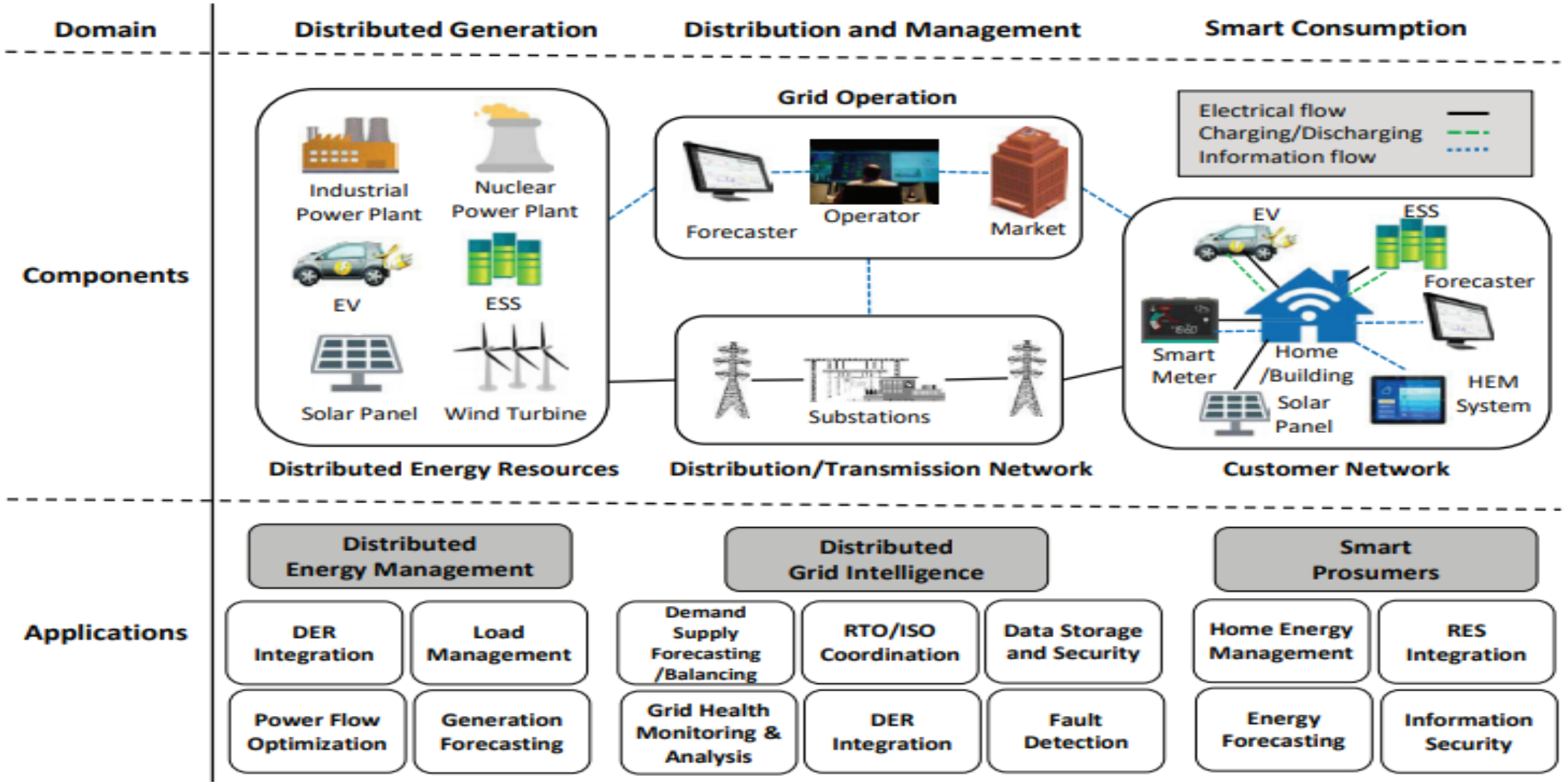
Application of advanced distribution Automation in SCADA

The most important application of the Advanced Distribution Automation is fault diagnosis by monitoring the faults in the grid, then identifying the root cause of the occurred fault and then restoring the system.

Distribution Automation can be grouped into 5 major subgroups:

1. SCADA
2. Integrated volt self var control(IVVC)
3. Equipment health monitoring
4. Fault location , isolation and service restoration(FLSR) systems.
5. Integration of renewable energy sources.

Components and Applications of SCADA in Distribution Automation



Source: Ali, Syed S.; Choi, Bong J. 2020. "State-of-the-Art Artificial Intelligence Techniques for Distributed Smart Grids: A Review" *Electronics* 9, no. 6: 1030. https://doi.org/10.3390/electronics9061030

Improving Power distribution network with SCADA (1)

With customers relying on continuous power supply, electricity distribution authorities need to provide power that meets customer needs by ensuring distribution infrastructure, including substations and transformers, are efficiently managed, operated and maintained.

Automating power distribution networks by installing, or upgrading, a SCADA system is a cost-effective solution to minimize power disruptions and provides greater visibility and improved control of the distribution network.

https://www.greenpowermonitor.com/how-cybersecurity-can-protect-your-renewable-energy-assets/

Improving Power distribution network with SCADA (2)

Minimize disruptions and improve operations:

- SCADA system's function in the power distribution network is to
  - monitor and control distribution sectors,
  - optimize overall network efficiency, and
  - provide greater system reliability and sustainability.

- SCADA does this by
  - Collecting data from the distribution system, most of it originating from substations.
  - Typically, substations are controlled and monitored in real time by Programmable Logic Controllers (PLC) or Remote Telemetry Units (RTU) along with other devices such as circuit breakers and power monitors.
  - Devices that collect data transmit it back to a central SCADA node located at the substation; this node is connected to the main Control Centre.

https://www.greenpowermonitor.com/how-cybersecurity-can-protect-your-renewable-energy-assets/

Improving Power distribution network with SCADA (3)

- **Reducing Manual labour requirements:**

SCADA reduces the need for workers to physically complete the task themselves. This allows workers or operators to undertake specific tasks in a much safer and more efficient manner than if they were to do them manually.

- **Reaping the benefits of SCADA:**

Automation IT covers all aspects of SCADA power control and monitoring, from large distribution transformers and high voltage switchgear through to complete renewable energy power stations, solar farms, wind turbines, gas turbines and reciprocating engines.

Other functions performed by SCADA include:

- Controlling transformer voltage taps to improve network efficiency
- Control and monitoring of sectionalizers and reclosers
- Continuous monitoring and controlling of electrical parameters
- Trending and alarming to alert operators to power supply, quality or safety issues

https://www.greenpowermonitor.com/how-cybersecurity-can-protect-your-renewable-energy-assets/

Benefits of integrating technologies to SCADA (1)

- **Proactive Maintenance:**

Proactive maintenance involves preventive maintenance measures that will allow you to correct the root causes of failures and avoid downtime caused by underlying equipment problems. The main goal of proactive maintenance is to be able to anticipate machine failures and eliminate them before they develop.

- **Quick response to issues:**

A quick response is critical when SCADA system emergencies happen. In fact, depending on the issue, a quick response may be the difference between correcting the situation and a disaster. That's why receiving notifications in a timely manner is so important - emergencies could occur at any time.

- **Automated Controls:**

Having notification flexibility is very important, but sometimes it is not enough. Usually, SCADA systems allow you to remotely control just about any piece of equipment through control relays outputs in your RTU.

Benefits of integrating technologies to SCADA (2)

- **Customized Alerts:**

Your SCADA should be customizable in order to allow you to avoid receiving irrelevant alarms. Getting notifications for every little thing that happens in your network triggers the slippery slope of operator indifference towards all alarms. Another important custom option that is important to have is the need-to-know based alerts.

- **Detailed reporting:**

SCADA systems are always collecting data from your remote equipment and processes. All of this information is usually stored in a central master station. Efficient master stations are able to compile a detailed reporting document about your network equipment.

- **Integration with your current Equipment:**

The result of integrating incompatible devices is that issues are dealt with more quickly and with a better level of consistency. The systems will allow for the integration of your current equipment to best in class SCADA increase efficiency.

Risk while integrating technologies into SCADA RE systems (1)

- The need for a powerful and collaborative risk management framework for SCADA systems has become urgent to identify, evaluate, and treat various types of risks targeting SCADA systems. All possible scenarios that may happen and affect the system either directly or indirectly should be well described according to a set of parameters. Some of them are:
- Giving a detailed level of identifying the risks and classifying them based on the nature of the risk agents, their action's motivation, and the penetration tools/techniques that can be used to cause a risk on a SCADA system.
- Providing all possible components that formulate a SCADA system and state all known vulnerabilities that can be used by attackers to perform the attack.

Risk while integrating technologies into SCADA RE systems (2)

- Mapping between risks, vulnerabilities, and system components by linking each risk with all possible vulnerabilities of system's components that an attack agent can utilize to achieve the risk goals. A description of the estimated impact on that component as a result of an attack is also missing.

- Description of the interdependency among threats that can be used to present the possible attack path scenarios. The main point in this work depends on the hierarchal based method. The relation among related parameters is converted into matrices, which are linked synchronously to construct an augmented matrix with six dimensions, which is analyzed.

Cyber Threats (1)

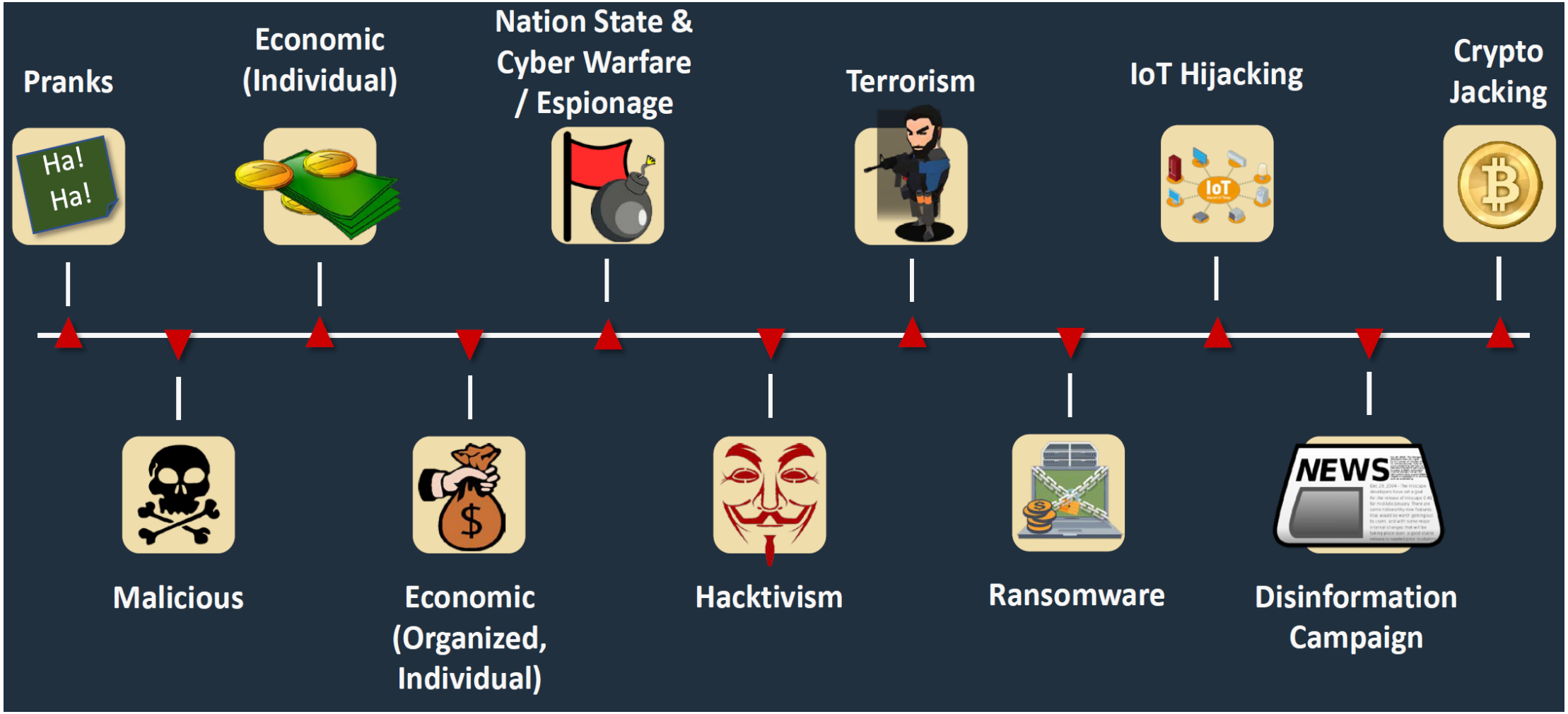
- There are several technical threats that could affect to the digital infrastructure because of the need to connect remotely.
- This involves unencrypted connections, technical known vulnerabilities and exposures from systems on site that could enable malwares, backdoors and many other techniques to affect to current or future behavior of digital components.
- Or even worse botnets and advanced persistent threats could disrupt normal operation and affect to the energy assets as well.

Cyber Threats (2)

- Internal technical threats because of unsafe network designs, communication protocols chosen, software dependencies , lack of patch management policy or simply information risks because of bad human habits can make useless any cyber protection.

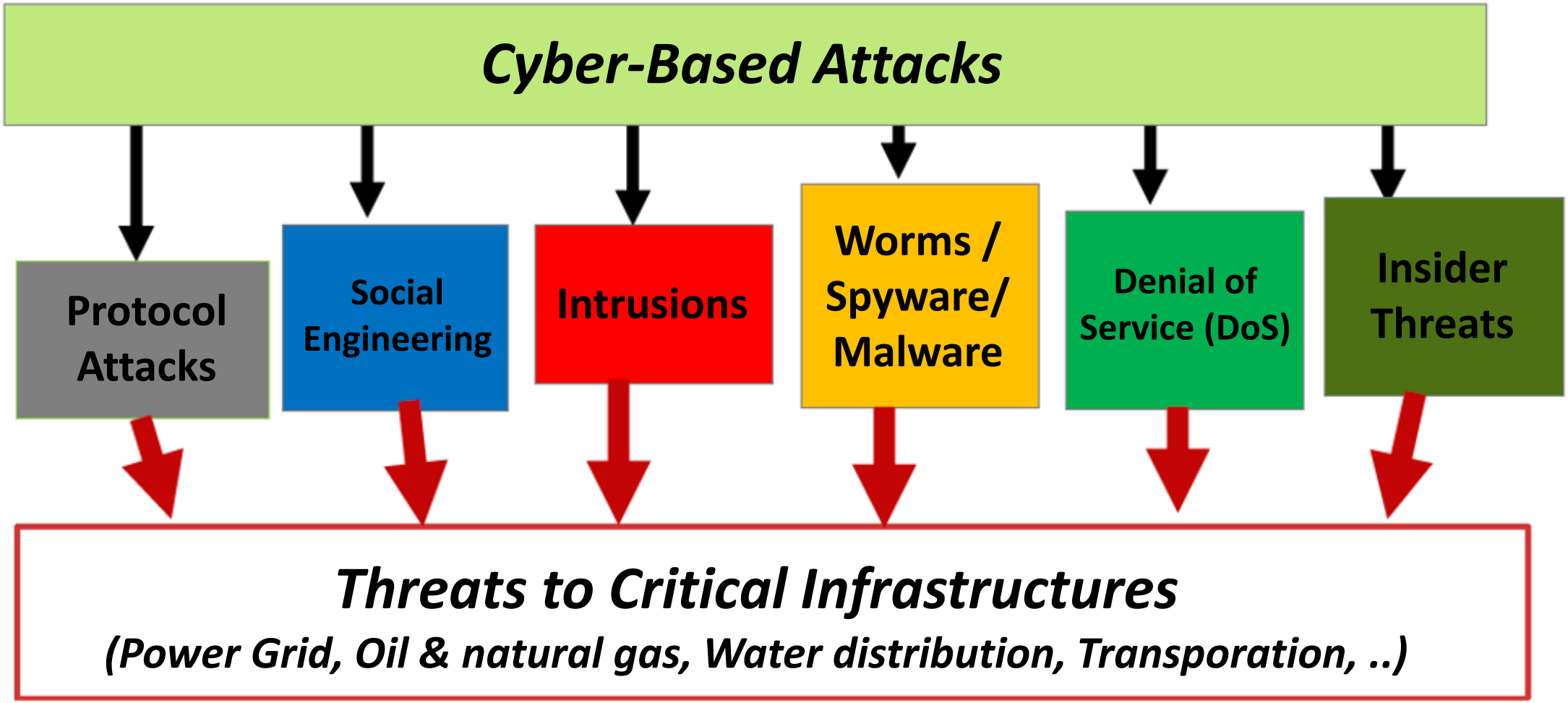
- It is well known that a system is only as strong as the weakest link, and this involves people as well, so social engineering needs to be considered as an important threat too.

Cybercrime Evolution



Source: Cybersecurity at Texas Tech, Sam Segran, 2018

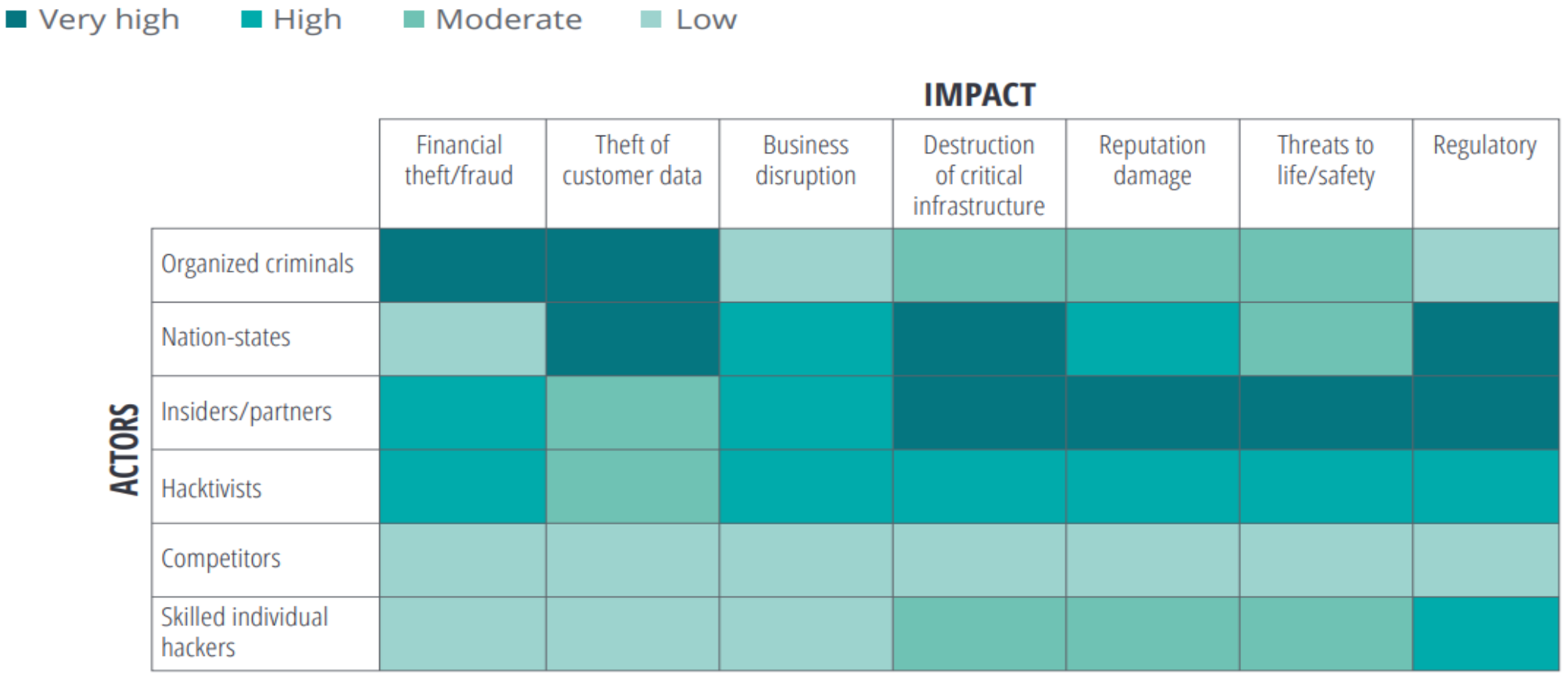
Cyber Threat for Critical Infrastructure



Source: Cyber-Physical Security for the Smart Grid, GIAN Course, IIT Bombay (Manimaran Govindarasu), March 2018

Cyber threat: Actors & Impact in electric power sector

The cyberthreat profile for the US electric power sector is highest from three key actors



Source: Deloitte analysis.

Types of Cyber Threats (1)

- **Malware** :means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer

- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Source: http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf

Types of Cyber Threats (2)

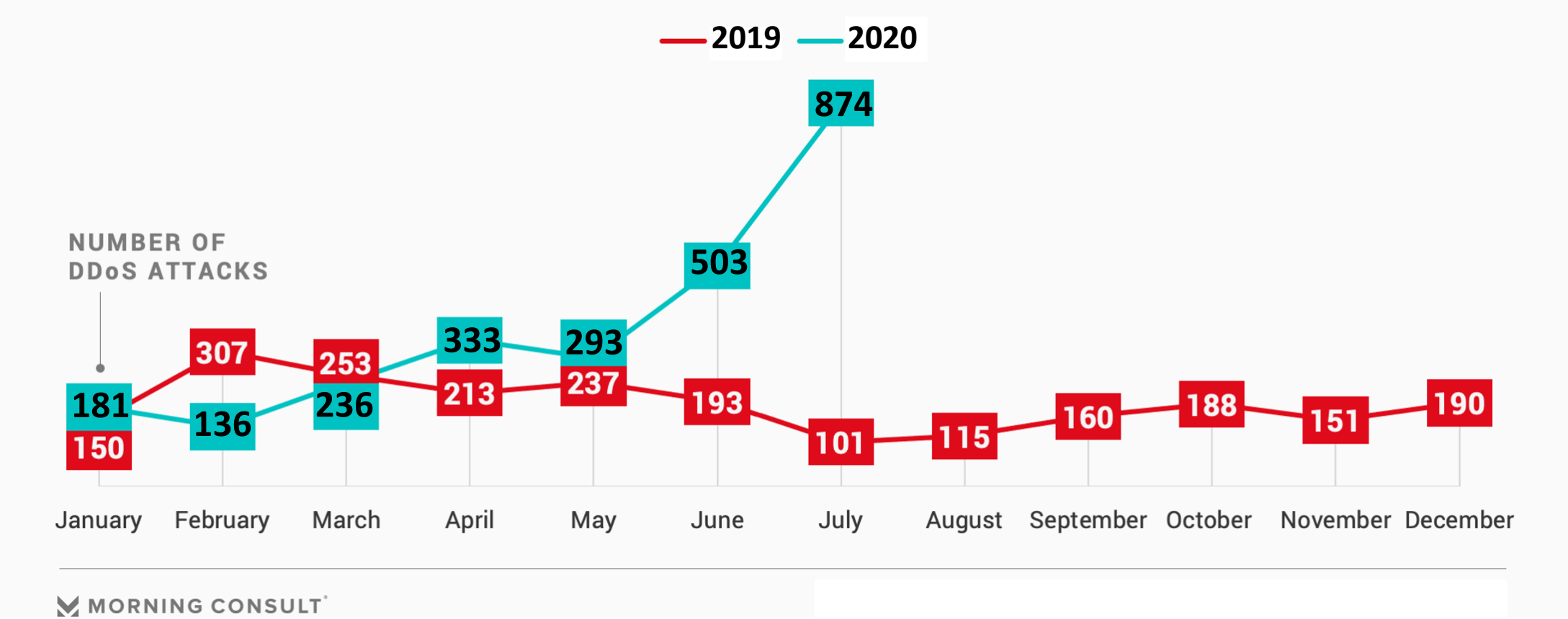
- **SQL injection:** An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.
- **Phishing** : is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information.
- Full list of significant cyber incidents in US since 2006:

https://csis-website-prod.s3.amazonaws.com/s3fs-public/210326_Significant_Cyber_Events.pdf?ZKJIdGVXdQd2vXW.gFEcFQs2Ay7cDiqt

Source: http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf

Utilities Worldwide Menaced by Cyberattacks As Pandemic Stretch Into the Summer Months

Distributed denial of service attacks on utilities around the globe increased almost seven-fold compared to the year-ago period, NETSCOUT data shows



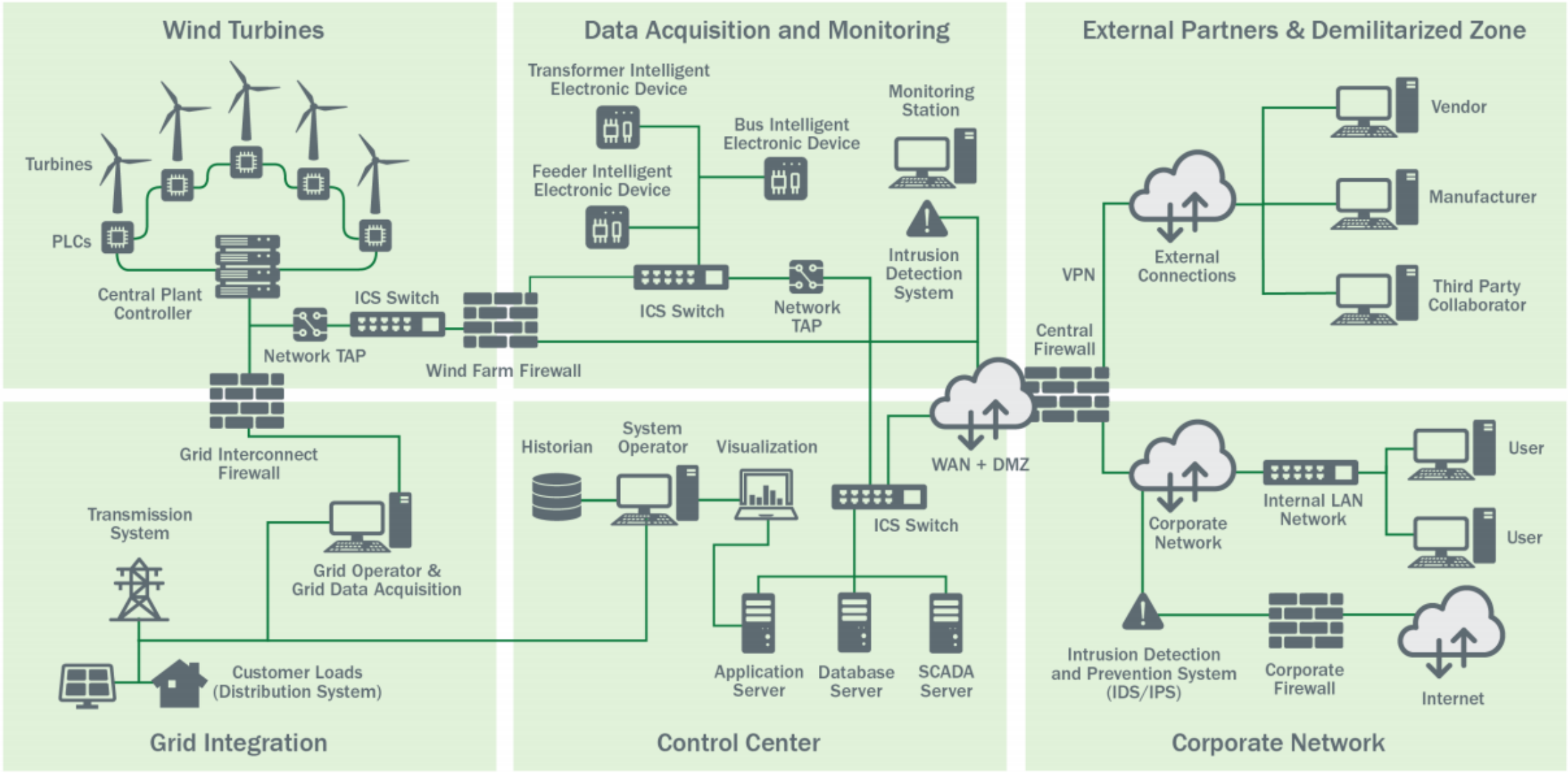
Source: NETSCOUT's Cyber Threat Horizon tracker, accessed Aug. 27, 2020.

Best practices approach on Cyber security at Project/Component level (1)

- Each control with physical or cyber access presents an intrusion point.
- Access must be controlled, and data integrity must be maintained at each accessible point.
- Examples of components: Wind farm reference architecture with secure best practice approaches like Network Segmentation, Zoning, Monitoring, and Intrusion Detection and Prevention System (IDS/IPS) for control and SCADA environment.

Source: US DOE Report, Roadmap for Wind Cybersecurity, July 2020

Best practices approach on Cyber security at Project/Component level (2)



Source: US DOE Report, Roadmap for Wind Cybersecurity, July 2020

Tools for Cyber security (1)

- **Network threat monitoring:**

Network monitoring tools that randomly check data samples to see if traffic is going to suspicious locations in and around a network can identify and stop an attack like this in its respective tracks.

- compare the data flow samples to an in-house extensive threat library and
- decipher suspicious patterns and
- potential security gaps that may be early indicators of a compromise, network problem or misconfiguration.

Tools for Cyber security (2)

- **Managed Security Analysis:**

Advanced analytics of systems can help single out potential attacks early, providing confidence as the digital footprint of the utility and grid expands.

- single out critical threat data and help organizations act before there is a serious impact on operations.
- incident data can be quickly generated for analysis through a simple portal, with actionable information from logs or events made available so the most imminent threats can be escalated for action.

Tools for Cyber security (3)

- **Mobile Security:**

Operators and engineers out in the field are increasingly making use of tablets and other mobile devices that, if not managed, can also be vulnerable entry points for attackers. Mobile security allows businesses to secure employee and associate devices, whether they're at their desks, in the field or nearly anywhere in between.

- **Cyber risk monitoring:**

Cyber risk monitoring can provide an easy 360-degree view of the overall security landscape, make regular risk assessments and benchmark specific security information. The technology will provide regular updates in clear language, making it easier to manage and understand. This can help businesses identify security gaps and ultimately develop a focused action plan so money can be spent where it's needed most.

Tools for Cyber security

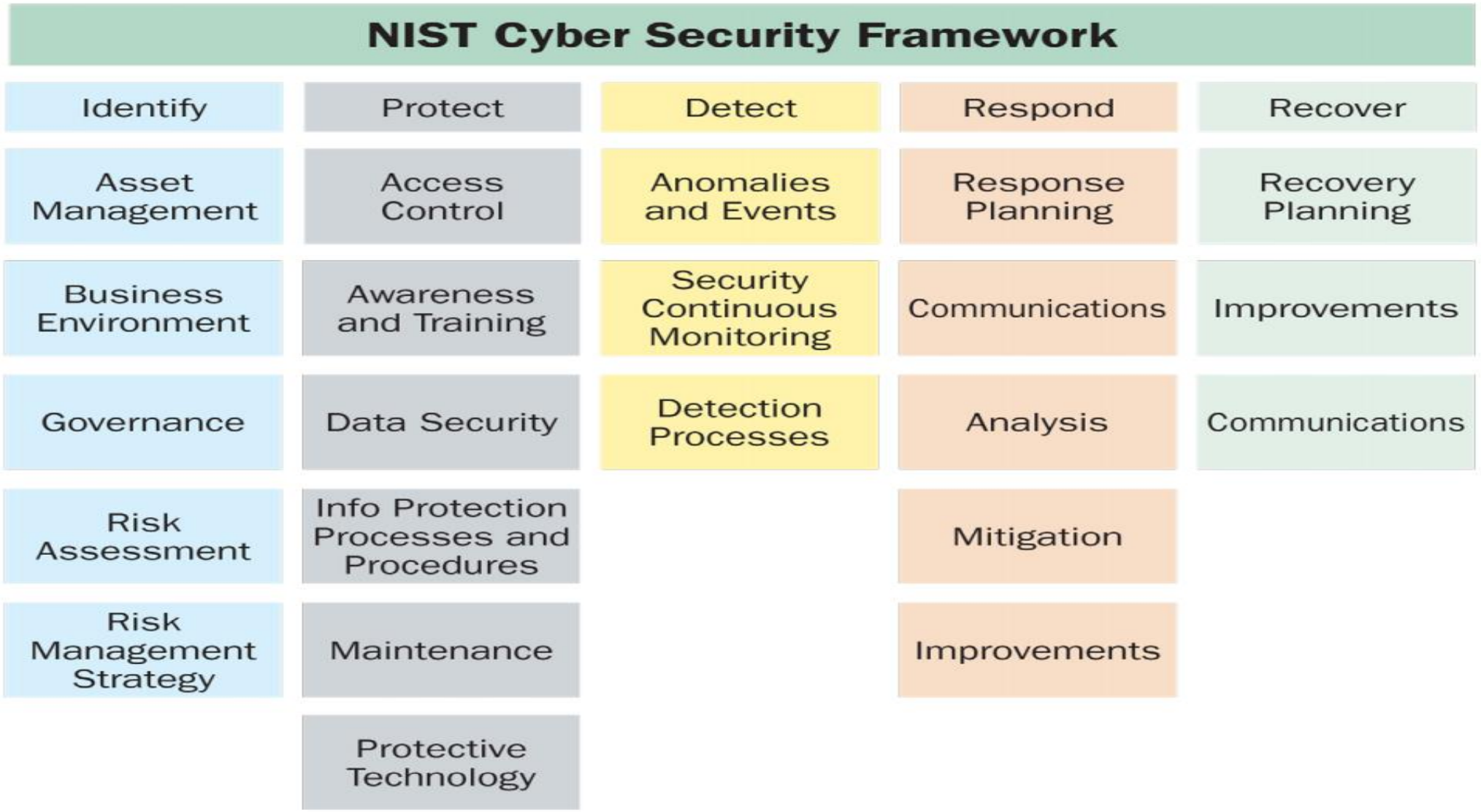
- **Smart energy Cyber Security:**

These are intelligent and robust solutions to keep smart energy and smart grids secure and operational. Together these solutions provide flexibility and scalability when it comes to cyber security management, which is key for an industry that is critical to national infrastructure but also undergoing dramatic and rapid changes.

Points to Consider to develop a cyber security Plan

- Industry needs to adopt cybersecurity best practices and develop a risk management culture; cybersecurity regulations are important, but because there is a delay in developing and implementing them, regulations lag behind evolving threats.
- It is important to rapidly share information about cyber threats while respecting privacy guidelines.
- Good cybersecurity requires skilled teams to understand baseline operations, detect and respond to anomalous cyber activity, reduce the “dwell time” of cyber attackers, and implement layered cyber defenses.
- The is a need to understand and increase system resilience to avoid prolonged outages and better recover from cyber attacks.
- In the future, utilize advanced cybersecurity technologies, international approaches to cybersecurity, and machine-to-machine information sharing so the response to cyber incidents takes place in milliseconds—not months.

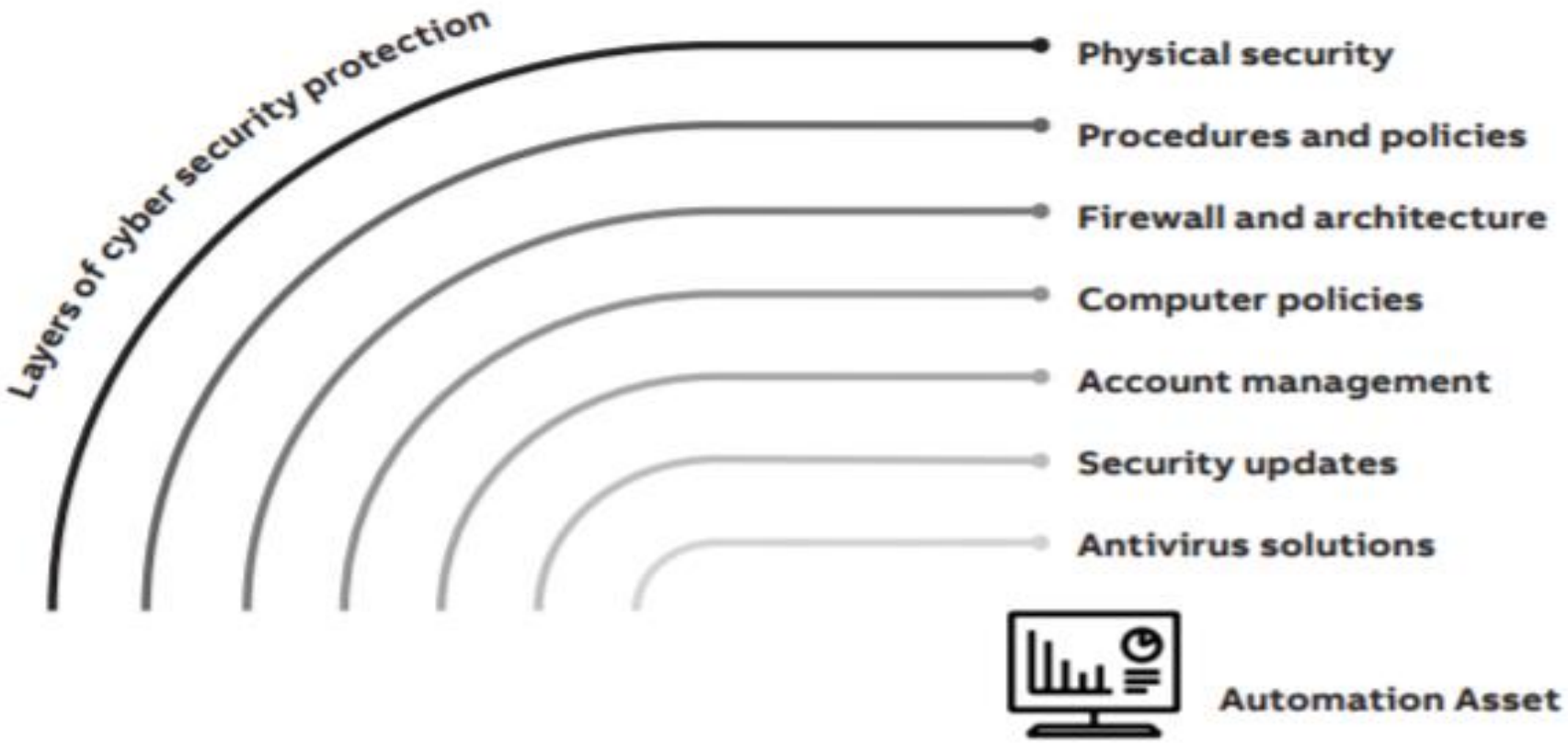
NIST Cybersecurity Framework



Source: US DOE Report, Roadmap for Wind Cybersecurity, July 2020

Defense In Depth Strategy

To Minimize the impact of these attacks, it is important to have multiple layers of cyber security protection.



Source: https://energyinformatics.springeropen.com/track/pdf/10.1186/s42162-019-0083-1.pdf

QUESTIONS?