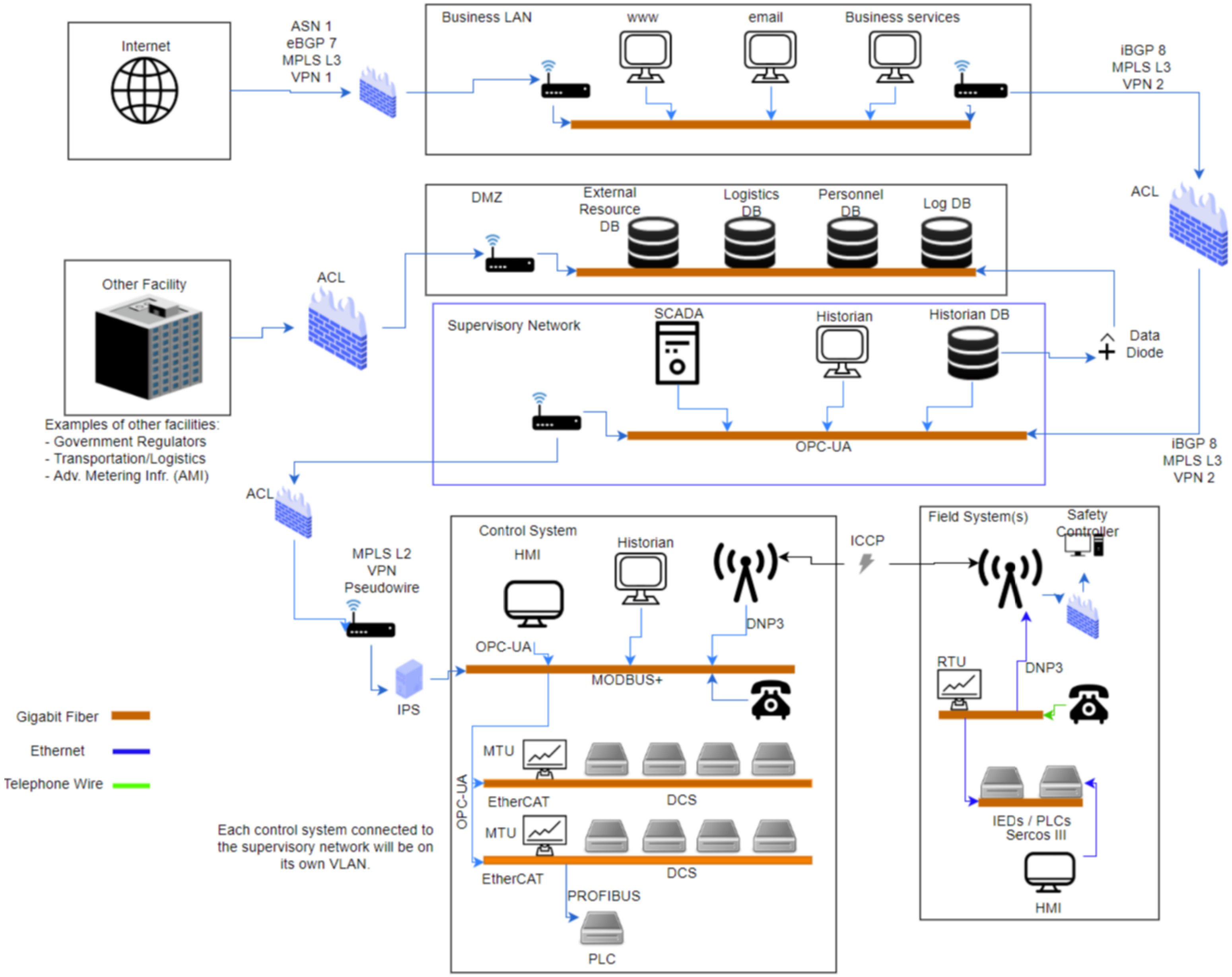
Attack



The image above is the ICS diagram that was created and explained for the Defense portion of this project. Please see the Defense project for explanation.

Stuxnet: Stuxnet is a computer worm that was engineered to work on many different kinds of systems and primarily targets Programmable Logic Controllers, or PLCs. Originally, Stuxnet was injected into an Iranian uranium enrichment plant via a USB drive. The malware spread throughout the system and destroyed the centrifuges by causing them to spin much faster than they were supposed to and for much too long, meanwhile the worm did not allow the system to report any of the anomalous behavior. After the Iran uranium enrichment plant was attacked, Stuxnet mutated itself and has been found in infected systems across the globe, now targeting more than just PLCs.

- The HMI in the Control System network would need to be configured to disable the USB port when not needed. Enabling would require approval from higher.
  - After installing required updates via USB, ensure that the installation device had no changes made to it. Could use hashes.
- Implement some type of authentication protocol to prevent exploitation of hardcoded authentication certificates.
- Automated checks on changes in the alert reporting system so that worms such as Stuxnet cannot make the systems destroy themselves without the alert going through to the control center.
- For certain systems with redundancy, reset them to baseline configurations at the end of day.
- Keep all software and OSs up to date.
- Create policies for employees when entering the facility to prevent possible internal threats from being capable of destroying the system.
- If infection is discovered, quarantine them into a sort of honeynet to watch the behavior, if possible.
- Do not use Siemens WinCC on SCADA systems.
- Whitelist the devices that are necessary to each specific system.
- Use authentication between the master and the slaves when using PROFIBUS.
- Encrypt connections that use PROFIBUS.

Dragonfly/HAVEX: Dragonfly is an APT who created a Remote Access Trojan, or RAT, known as HAVEX that targeted organizations within the energy sector. HAVEX attackers creating “watering holes” to attract victims to a malicious website, for example, to make it easier to infect them with their RAT. Additionally, spam and exploit kits were used to deliver the HAVEX malware. The attackers could then retrieve information from connected devices which would be sent back to C2 for analysis.

- Implement email phishing prevention and employee education to prevent successful phishing campaigns. Primarily in the Business LAN.

- Whitelist legitimate executable directories.

- MFA.

BlackEnergy: The trojan known as BlackEnergy was used to create a botnet that the attackers could use for DDoS attacks, cyber espionage, and information destruction attacks. A group of BlackEnergy attackers deployed SCADA-related plugins to ICS and energy markets.

- Administration and access control for network access. Group policies that prevent certain types of vulnerabilities from being exploited.

- Mandate cyber security awareness training.

- A DDoS attack would not cause a dramatic effect on our ICS since they do not require internet access and are connected to subsequent networks via VPNs. It would be more important to prevent very long-term shutdowns so communications can be re-established quickly.

Ukraine Cyber Attack 2015: In 2015, attackers used spear phishing emails, variants of the BlackEnergy 3 malware, and manipulation of the Microsoft Office documents that contained malware. These techniques were used to gain control of the networks within the electrical companies where they gathered credentials and information needed to access the ICS network. The attackers installed tools on the SCADA systems that can automatically control mouse movement which allows them to control the system or shut it down altogether if they decide to do so. Additionally, they set up VPN connections to enter the ICS network, used existing remote access tools within the environment or issued commands directly from a remote station, used UPS systems to impact connected lad with scheduled service outages, and DDoS attacked the telephone lines of the customer service call center.

- Implement machine learning algorithms to detect mouse movement when no CAC inserted.

- Ensure there’s an SLA with the power companies that requires them to provide redundant power systems so that if they get attacked and their primary grid loses power, our system continues to receive power.

- Ensure SLA requires the power company to scan for killdisk.

- Power redundancy such as large generators.
- Protect domain controller.
- If possible, generate our own power – at least for critical components in the ICS.
- Increase authentication for breaker-open commands or anything of that nature.

CRASHOVERRIDE: CRASHOVERRIDE malware consists of an initial backdoor, a loader module, and many payload modules. It was used in the 2016 Ukraine cyber attack in 2016 (not 2015) to disrupt operations at a single transmission level substation. One payload module is the data wiper module. This module clears all registry keys associated with system services, overwrites all ICS configuration files across the hard drives and all mapped network drives, overwrites generic Windows files, and renders the system unusable. Another module name IEC 104 reads config files defining the target (likely an RTU) and action to take, it 'kills' legitimate master process on the victim host and masquerades as the new master, and it enters one of four modes (sequence, range, shift, and persist). These are only a couple of modules used in this attack, but they are perhaps the most destructive parts (dragos.com).

- Since our ICS is not a power grid, the only thing we would need to do to protect ourselves from this malware is generate our own power, if possible, or have redundant power generators in the event the power grid goes down.

TRISIS: TRISIS is a compiled Python script using py2exe compiler which allows TRISIS to execute in an environment without Python being installed on the native host, which would be the case in most ICS environments and Safety Instrumented Systems (SIS). SIS maintains safe conditions if other failures occur and this is what TRISIS aims to attack. It is one of the first attacks meant to result in human injury or death (dragos.com).

- Field systems have a safe shutdown that they can go through as well as redundant systems that can allow them to complete that process.
- Strict authorization on safety controls.
- All controllers should be left in locked cabinets and in program mode.
- Devices in the field system should never be connected directly to the internet other than the safety network.
- Scan any foreign devices before allowing them to connect to the network.
- Check for any and all anomalous changes to the system on a frequent basis.

- If the safety control devices are ever unexpectedly switched into program mode, an alarm should sound.

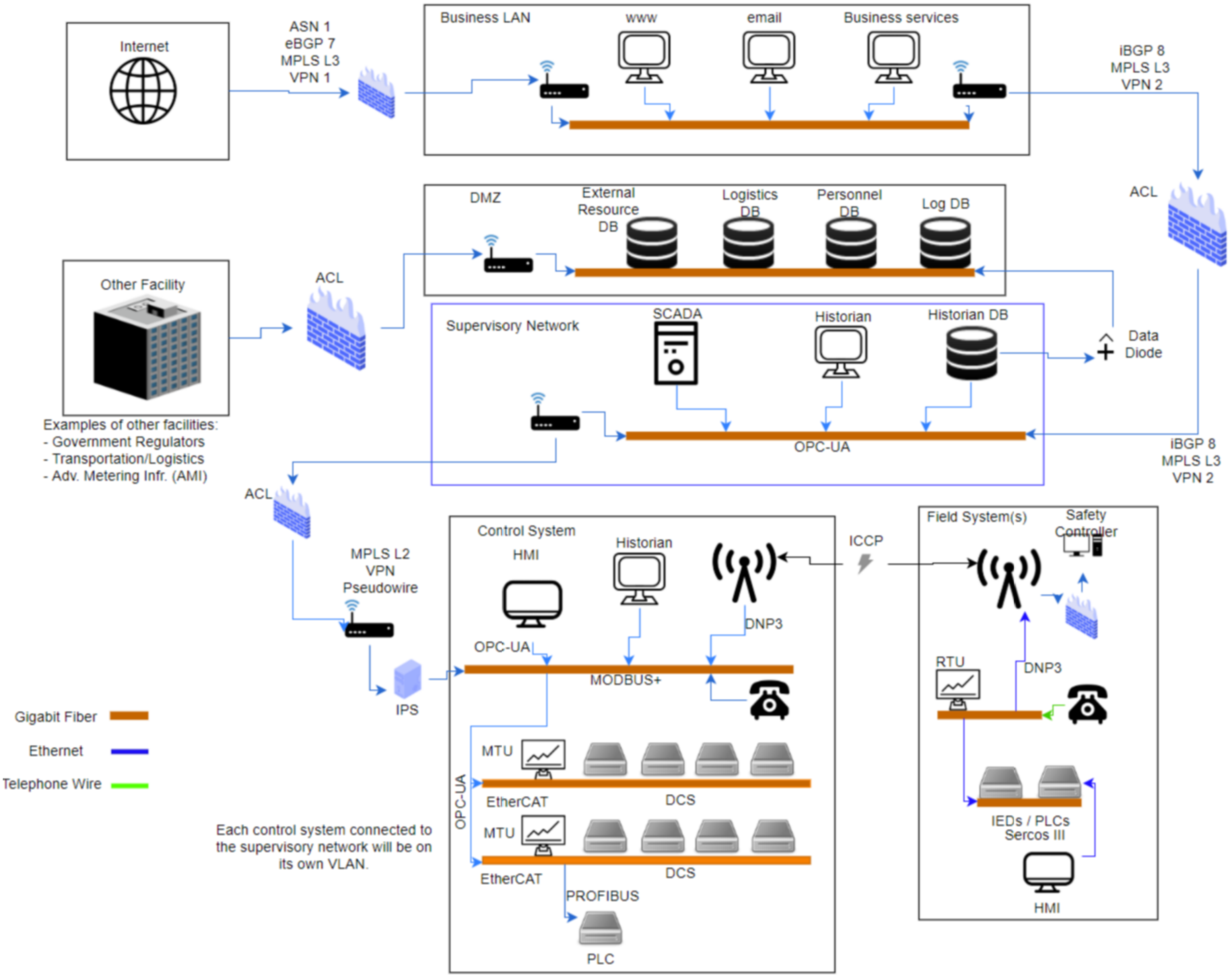
Insider Threat: An insider threat is someone who has access to internal networks, whether it is physical access, or remote access, and is trusted by the owner of the network. However, an insider threat does not necessarily mean that the person intends to do harm to the network. This could be someone who is socially engineered into believing that what he's doing is okay - perhaps by receiving an email that seems to be from his boss who tells him to download a file and install it on several different systems. Insider threats can also be malicious attackers that intend to infiltrate the company that owns the network so they can attack it from within or spy for another entity.

- Mantraps where important ICS components exist.
- Extensive employee background checks.
- Physical security.
- 802.1x authentication to prevent insiders from connecting unauthorized devices to the internal network.
- Detailed logs and data visualization software (such as Splunk or ELK stack) that can monitor connections and network events.
- Cyber security training mandatory for all employees.
- Thorough and secure reporting system for employees to report suspicious behavior.

Mandatory vacations, separation of duties, access control.

Defense

The ICS diagram above represents a typical ICS topological architecture. Before applying the various famous attacks, we attempted to design a realistic and secure network. We attempted to not add any sort of specific authorization or authentication policy, control insider threat mechanisms, too much system redundancy, or assumed machine learning. Our focus was strictly how to design a secure network flow with separation. The following topic describes our initial



sub layers. The attack portion of the assignment describes our additional security policies, SLAs, and system control mechanisms. Our model is based off of a typical petroleum plant.

Internet Layer

This layer encompasses the general global web available to our employees at the business level LAN. Our assumption with the firewall separating the internet and business LAN was that our organization had some ASN, communicated with an ISP using BGP, and followed standard MPLS with a layer 3 VPN. We may assume that the business LAN uses OSPF to share routing information within the enterprise.

Business LAN Layer

This layer represents the various routers, computers, and IoTs associated with business operations within the IT infrastructure. Our standard servers are located here and the LAN may be connected to several DMZs other than that described below. Those DMZs would be separated by the business LAN and may be available services for any given customer to access like an online purchasing system.We may assume that the business LAN follows secure IT practices.

DMZ Layer

The DMZ layer for the ICS system is actually not connected to the business LAN, but the Supervisory Network layer. We chose this specific layout because the DMZ purpose is to provide necessary entities access control data information via a one-way data diode leading from the supervisory network up. This information may be accessed by governments for reporting and compliance purposes, transportation services for logistics, and AMI for the power company. These network connections are direct ethernet VPNs. They are not directly connected to the internet and SLAs are required by participating parties. Our available logs are also stored here.

Supervisory Network Layer

The supervisory network connects to the DMZ via data diode and the business LAN separated by a strict ACL firewall. There is no business LAN direct control over SCADA system equipment, only communication, no master switch. To limit spear phishing vulnerabilities, staff are trained on cyber security best practices and information sharing from the business LAN down must be multi-authenticated. We discuss more deeply in our attack paper. The supervisory network communicates over BGP and on a separate MPLS layer 3 VPN than that used by the enterprise. The historian at this level aggregates information from the control system layer and sorts need-to-know information to be forwarded to the DMZ via the data diode. The devices within this layer run Windows OPC-UA as best practice. As described more in depth within the attack paper, better authentication will be added to these protocols and unnecessary RPC ports will be closed.

Control System Layer

The control system layer connects to the supervisory layer where the SCADA system may control devices at a lower level. These networks are separated by a strict ACL firewall and an IPS system which lies behind the control system gateway router which runs a separate form previous VPNs, MPLS L2 VPN. This decrease in encryption volume is best for the layer 2 protocol that will eventually send information to the supervisory network. All other connections in this layer are encrypted on a need-be basis and rely on VLANs instead. The HMI connection runs OPC-UA, but it is connected to the general device network via fiber ethernet running Modbus+. The MTU connection to the DCS system uses etherCat which is why we included an IPS system. There are redundant DCS systems to ensure our critical systems run in the event of restart, shutdown, or update. The PLC profibus connection is a monitoring device that connects to the DCS and is therefore non-essential and encrypted with authentication. We may assume that this site has a spare generator and sturdy power supply in the event power is cut. This network connects over DNP3 to an antenna to communicate wirelessly to a remote oil rig.

Field Systems Layer

The field system communicates with the control system wirelessly over ICCP. The RTU connects to the antenna via DNP3. In the event of emergencies or general communications, a phone system is installed. The RTUs communicate with the PLC/IED devices over modbus+. PLC-to-HMI setups run OPC-UA assuming that all HMIs are Windows OS. PLCs and IEDs communicate with each other over Sercos III. A strict firewall separates the emergency safety control systems from this network. The attack paper details this methodology further in an attempt to prevent TRISIS attacks. There is likely an emergency generator on board.

Conclusion

It is important to note that OT devices are non-routable and thus rely on certain IT routers to move data across the networks. This diagram fails to highlight where enclaves are utilized, but it may be assumed that devices follow a reliability and efficiency model within like-device enclaves, but utilize authentication services between enclaves. The separation between devices via theoretical switched lines of wire within the diagram give a general idea where some enclaves may exist, such as the separation of DCS and the HMIs. For the purposes of simplicity within our reports we do not highlight the detailed processing and scanning mechanisms that would be applied upon the various ICS protocols to ensure packet information is correct. However, we did consider this information in where and how we decided to wire specific devices.