**Concept of correlation**:

Assume that an agency has focused its system development and critical infrastructure data collection efforts on separate engineering management systems for different types of assets and is working on the integration of these systems. In this case, the agency focused on the data collection for two types of assets: water treatment and natural gas delivery management facilities.

**Question**:

Identify what type of critical infrastructure data collection is needed for pavement and storm water management facilities.

**Instructions**:

* Need minimum 400 words
* Need 3 APA references
* No plagiarism please
* Need 3 Responses (150 words each) (Use uploaded document for responses)

**Initial post 1**:

Although it’s difficult to follow, it appears the question is about what type of data is needed for pavement and storm water management facilities. An agency, presumably in charge of data collection for critical infrastructure sectors, has already done some data collection on water treatment and natural gas delivery facilities; therefore, the former types of data will be more beneficial than the latter. Pavement, with respect to utilities, seems to have more to do with maintaining roads, sidewalks, etc. In either case, based on our reading from Amoroso (2013), it appears that there is no national collection process today (p.192). It’s also important that we collect only the types of data that are necessary to perform a proper review of the threats so that we can implement some decent countermeasures. Having far too much data, especially at the national level, would cause us to run out of storage space and slow down the entire process of securing the enterprise networks. Amoroso (2013) suggests using data sampling and including system data such as device utilization and common applications.

It seems that more data is probably needed for storm water management, as it can create an immediate health and safety issue. If stormwater runs freely across certain areas, it could cause a serious, life-threatening flood. Sensor data should be reviewed to make sure it’s not being compromised, although this is a difficult thing to accomplish. A security information and event management (SIEM) system could be put in place to aggregate the data from numerous PCs, servers, and sensors (if possible), and this data could even be fed into a larger network of SIEM appliances at the national level. Typical TCP or UDP traffic, audit logs of access events (especially failures), and events such as seemingly normal power fluctuations could all be included in this type of event. For pavement utilities, including roads and bridges, etc., it’s important to consider supply chain implications, as well. The materials required to pave a roadway or rebuild a bridge are extensive, so it’s important to consider some type of security or analysis of the supply chain to ensure that materials are delivered on time and in the right location.

There are tons of laws and regulations at the state, local, and federal level regarding storm water. The City of Colorado Springs (very near to where I live) has been facing federal fines for violating various laws when it comes to the stormwater treatment policies of the city. Our state has a stormwater management program known as the Colorado Discharge Permitting System (CDPS), which regulates stormwater discharges. Municipal Separate Storm Sewer Systems (MS4s) are also part of this system. The State of Colorado follows the NIST framework for developing cyber security plans, so most of the items involving audits will fit. The Colorado standards for audit logs include successful and failed logon attempts, privilege escalation, logins from known malicious locations, brute force attacks, etc. Utilizing these types of standards would be a great way to pull the necessary data together from the disparate sources.

**Initial post 2**:

Water treatment plants and Gas delivery management facilities are anticipated targets to disarm a nation. Very often we see issues like natural resource scarcity because of overuse or wastage. But this is not the only concern, increased digitalization and unmanned processes are opening channels of vulnerabilities. In my previous discussion I briefly described about ICS (Industrial Control systems) which are highly dependent on SCADA operating systems. All small, medium and large-scale plans need to connect to the central system for operational activities. Once these are done there should be a security-frameworks needs to be developed in conjunction with NIST to protect these SCADA systems. These SCADA systems needs to be protected by Network and security architecture to avoid breaches and unauthorized authentications. Water sector is one among the sixteen critical infrastructures which needs protection from threats.

Advanced persistent threats are most common on critical infrastructures like water treatment and gas delivery facilities. The major goal is to destabilize the environment, steal information, analyze the operational activities and bring them down. A single access can result in exfiltration of crucial information. IP networks are different than SCADA networks. SCADA network communication is serial based and use low frequencies for communication with peer autonomous systems. It is technically not possible to integrate IP network and SCADA network. All these could lead to vulnerabilities and loop holes. Hence, we need correlation in networks. It is important to separate network configurations and automation networks with some known conjunctions. In many gas plants to reduce the amount of CO2 emissions most of the facilities follow something called “Electrification” where they need to shut down power supply to certain units, and that proceeds as an operational procedure. With recent innovation such areas are digitalized. Unmanned operations will be followed. This is a potential vulnerability with high risk of intrusion. The SCADA networks are programmed to suit the operational process. It is important to isolate networks to make sure targeted attacks don’t affect other environments. Because lack of communication would result in complete shutdown of the production.

All SCADA networks connected need to communicate with other locations where the IP network is enforced. The communication of SCADA networks end to end should be encrypted using VPN tunnels. This avoids unnecessary exfiltration of data as VPN tunnels are by far best ways to communicate when in remote locations. Also, encryption preserves he integrity of the ICS systems. The most important of all is a developing vision and strategy for cyber culture. Employees must be trained of potential cyber issues and best practices when they operate infrastructure. Network had to be secured starting from perimeter to various zones inside the network. Physical and digital access should be limited to multi factor authentication techniques. ICS network should never be exposed to the external environment and should remain as an internal zone with IP network over it as protection. SCADA network uses a lot of transmitters, receivers, boosters to signal transmissions. Usage of digital devices in the environment can disturb the network and mislead the information. Strict awareness of digital appliance usage with banners are quite needed. Network Intrusion prevention systems should be used at the perimeter to stop unauthorized large packets. Usage of thumb drive or other networks inside should be avoided. Every network should be thoroughly audited with infrastructure teams to be compliant of various industrial frameworks.

Unified strategy for formulating policies and frameworks is much needed with growing threats. IOT can also be a very good solution for data driven networks. When it comes to renewable resources there are multiple ways to generate and so are the risks. IOT devices are easy to build and integrate with a common control system. A heat sensor in a boiler can be built with a raspberry pi chip and be given an IP to communicate with an application loaded on a known workstation. Any failure will be localized and doesn’t spread to other environments. We can use IPv6 addresses which are abundant in IP network world. This gives uniqueness to a device with a unique physical address. A possible show stopper is – extensive network utilization and maintenance. Comfort comes with an effort. When we are building a network of that scale proper security design with multiple teams working on each attribute is needed. Continuous operational activity needs maintenance. Operators should operate, maintain and recover any control system as they cannot be protected 100% from cyber-attacks. All power plants, gas plants, or water plants share one common feature – tailored operational activities. This is a boon as operators know how to mitigate a problem and a bane because a tailored approach can be easily be broken by cyber threats and interrupt any secure system.

**Initial post 3**:

Rainfall intensity and rainfall patterns data is a critical infrastructure data to stormwater management facilities as it determines the quantity of water that will be discharged at any given time and for a given duration of time. Sizing data is one type of data is one of the critical infrastructure data. Those data determines how much the stormwater facility can hold and include incremental void space, height, the discharge rate of effluent, and shape. Sizing data must be regulated to meet regulatory approval to avoid overflows and collapse of the stormwater storage facility.

Footprint data is another type of critical infrastructure data as it includes stage storage data and discharge rate data. Footprint data also include detention, infiltration and inverts data such as infiltration rate, minimum cover, loading ration, connection height and dewatering time which affect drainage efficiency and thus modifications can lead to overflows and thus collapse of stormwater storage and collection facilities (Stormtank, 2019). Cover depth data is another critical infrastructure data as it impacts structural performance. It includes data such as cover depth and cover material, which are all used to determine the allowed maximum load distribution (Guo & Urbonas, 2008).