Telecommunications Industry Association

A FUTURE AT THE EDGE: EDGE DATA CENTER WORKING GROUP SOLUTIONS BRIEF PAPERS

ISSUE 4

January 2020

Physical Security Considerations for Edge Data Centers

BY: John Gallagher (Viakoo)
Xavier Badosa (Schneider Electric)
Dmitry Tsyplakov (HUBER+SUHNER)
Michael Kestigian (Tech Data)
David Knapp (Chatsworth Products)
Ashish Moondra (Chatsworth Products)

OVERVIEW

Security is critical to the success of an Edge Data Center (EDC). Both physical security and cyber security should be considered and addressed when selecting a location and building a new EDC. TIA members came together with cross industry and cross disciple experts to establish the Security Working Group to lay out the physical security considerations and solutions for future Edge Data Centers.

The Security Working Group identified seven areas for initial considerations for the physical security of Edge Data Centers, including:

1. Environmental Risk
2. Physical Protection Risk
3. Power Supply Risk
4. Telecommunication Cabling Risk
5. Access Control Risk
6. Video Surveillance
7. Security Metrics

SCOPE

While physical security and cyber security both need to be addressed, this paper only covers physical security considerations and solutions. As the work of peer teams develops into recommendations, support for relevant measures and metrics to securely support those recommendations can serve as the foundation of an EDC Cyber Security Program. If a particular aspect of an Edge Data Center was not defined, its specifications should be drawn from the TIA-942 document. Public review of this paper is encouraged. The security component of the Edge Data Center program supports, supplements, or at least not constrains any other aspects of an EDC.

I. ENVIRONMENTAL RISKS

Definition

The definition of Environmental Risk adopted by the Security Working Group is as follows:

Concerns related to the ability of the EDC to achieve an intended purpose during changing external conditions. These conditions may arise from:

- naturally occurring sources such as hurricanes, floods, and earthquakes;
- changes in the environment due to adjacent space development;
- changes in the mission of the EDC such as would cause a need for amending its operation; and
- policy changes mandating a change in EDC content which may include maintenance, repair and upgrade procedures necessary to sustain a safe and secure operation.

The main focus for EDC environmental security relates to the first of the four areas above of externally induced change requirements. As Operations, Administration, Maintenance and Automation (OAMA) requirements for EDC operations evolve, and security considerations are woven together with other working group recommendations to form an EDC framework fabric, the other sources of externally induced change requirements will be addressed.

Considerations

The eleven areas of Environmental Risk identified as necessary considerations for Edge Data Center planning include:

- **Temperature**: Extreme temperatures, ranging from -40ºC (-40ºF) to 60ºC (140ºF), affect electronics and mechanical equipment. Design should consider that any external equipment supporting the EDC needs to work at the final location conditions. Designers should take into consideration the implications of global climate change that could impact the working conditions of equipment outside of EDC.

- **Humidity**: The humidity could vary from 0% Relative Humidity (RH) to 100% RH. Most of electronic equipment could support up to 95% RH non-condensing. The issue with low humidity levels is electrostatic discharge (ESD) that it could happen inside EDC and could damage electronic equipment. To avoid ESD risk the humidifier provision could be an option to analyze.

- **Earthquakes**: Seismic activity in the world is categorized in 4 zones, Zone 1 (Low risk) to Zone 4 (highest risk). The importance factor for EDC could be 1 or 1.5 depending on how critical the system is to continue working or not after an earthquake.

- **Solar Flares**: Magnetic fields induce electric currents in a conductor. A large magnetic storm can generate spurious signals and currents. It's quite rare to suffer this kind of event but if any it could affect the regular working conditions of an EDC, affecting data communications mainly.

- **Electro Magnetic Interference (EMI) (RFI)**: Electro Magnetic Interference also called radio-frequency interference (RFI) is when in the radio frequency spectrum, is a disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling, or conduction. Depending on frequency of the source such interference could affect some EDC systems in varying manners. An EDC could experience two types of EMI:

1. **Narrowband EMI or RFI interference** typically emanates from intended transmissions, such as radio and TV stations or mobile phones.

2. **Broadband EMI or RFI interference** is unintentional radiation from sources such as electric power transmission lines.

- **Chemical Hazards and Pollution**: There are areas like industrial, mining, coast, dumps, and oil rigs where an EDC could have potential risks of corrosion, explosion and failures because of chemical agents in the air. Air treatment and corrosion protection are options to mitigate these risks. For ATEX classified areas with high risk of explosion, a specific design of EDC is mandatory.

- **Wind Load**: EDC should be designed to support wind loads depending on the conditions of the area its being installed. EDC should be able to support wind gusts and static wind loads but should also consider tornadoes and hurricanes depending on the final location.

- **Snow Load**: The location will create different requirements for snow loads. EDC construction should comply with local standards to fulfill the requirements, but the design should consider that EDC enclosure could be free of maintenance, so it could be important to consider a roof slope design.

- **Flooding and Tsunami**: The risk of flooding on EDC should be analyzed depending on the final location. Sites close to rivers, seacoasts, and lakes will be more likely to suffer from this risk.

- **Lightning**: Lightning is a high risk for an EDC since it can cause EMI, fires, electronic damages all due to high over voltages in power lines and the ground.

- **Fire**: Risk of fire on EDC can come from several sources: forests, power lines, buildings, but also it can be generated from the equipment installed inside of EDC. To mitigate the risk, the design of an EDC should consider fire rated enclosures and internal fire detection and suppression systems.

Further development of EDC security solutions will include methods and measures relevant to the components of the EDC Types and Locations Working Group.

II. PHYSICAL PROTECTION RISK

Definition

The definition of Physical Protection Risk adopted by the Security Working Group is as follows:

Concerns relating to seals, locks, embedded information and communication technologies, and the boundary layer encapsulating other EDC contents and the capability to manage and maintain that protection.

In this material, physical protection refers to the mechanical, electro-mechanical and information infrastructure necessary to sustain the required levels of operation. In most cases, industry standards such as TIA-942 or AFIPS (American Federation of Information Processing Societies) programs provide guidance as to what a particular level of operation might require.

Considerations

Physical protection of the environment includes considerations for restricting access to the site and enclosure(s) or facility used to house the EDC. Key considerations include:

- **Physical Access Method***:* A method of securing the site and equipment and of managing locks and keys to individuals who are granted access. Consider methods of securing all access points into the site and enclosure(s). Consider access to the lock system and secure pathways for wiring of electronic lock controls. Availability of replacement components including gates, doors, covers and door/gate/cover/lock hardware if there is a breach. Provision of backup power and separate network connections for electronically monitored or controlled locks to maintain access control if there are other interruptions to remote access or power at the EDC.

- **Enclosure Robustness (ruggedized)**: The selection of the enclosure type, material, construction, to consider tampering by people or animals, or unintentional damage from contact by/with vehicles or construction equipment. Methods of protecting/hiding power and network cables in attached pathways and ingress/egress points. Methods of protecting mechanical piping. Methods of protecting ventilation openings.

- **Protect Against Animals**: In addition to standard and practical physical access and enclosure robustness, a method of preventing animal and insect penetration into any ingress point on the enclosure(s). This may include screen added to openings and periodic inspections of the site, perimeter, enclosure and ingress points.

- **Displacement Prevention**: Use of fences, trenches, berms or other manmade or earthworks to create a perimeter or barrier around the site to prevent access by unauthorized individuals. Secure pathways for data and power cables, preferably diverse and underground. Placement of AC condensing units, generators or other auxiliary equipment within barriers.

- **Flooding and Tsunami**: The risk of flooding on EDC should be analyzed depending on the final location. Sites close to rivers, seacoasts, and lakes will be more likely to suffer from this risk.

- **Signage**: To indicate private property, no trespassing and limited access; warnings regarding potential risks from exposures to electricity, light and radio waves; and to provide contact information for site owners, administrators or management.

- **Remote Monitoring**: Use of technology to remotely monitor, control, and record access attempts to the site and enclosure(s). Consider surveillance cameras, sensors, access controls to monitor the site, all doors and access points to the site and enclosure(s). Defined policy, procedures, training for monitoring and responses to authorized and unauthorized access.

- **Coordination with Local Utilities and Agencies**: Defined policy, procedures, training and involvement of local utilities, emergency response and law enforcement regarding site monitoring and access.

- **Inspections**: Periodic inspections, documentation and repair of the site, perimeter, enclosure(s) and ingress point(s) from normal wear or damage caused by trespassers, theft, or vandalism.

Further development of EDC security solutions will include methods and measures relevant to the types components of the EDC Types and Locations Working Group.

III. POWER SUPPLY RISK

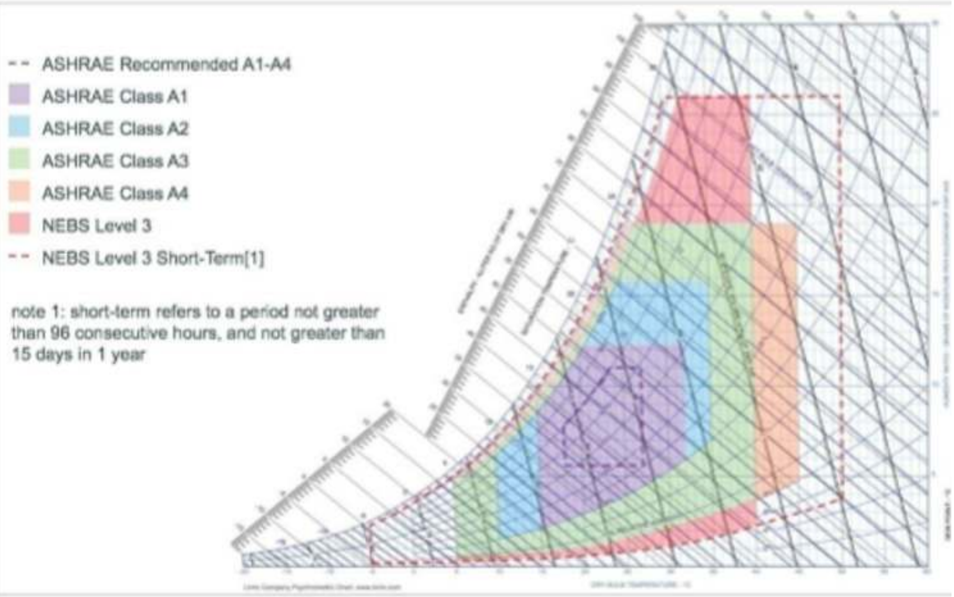
Definition

The definition of Power Supply Risk adopted by the Security Working Group is as follows:

Concerns regarding the state and status of power, power conditioning, and supplemental power solutions deployed to support EDC operation.

Considerations

Edge Data Centers have been proposed in several locations and environmental conditions. The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) Technical Committee has created a widely accepted set of guidelines for optimal temperature and humidity set points in a data center. These guidelines specify both a required and an allowable range of temperature and humidity. ASHRAE 2015 thermal guidelines are presented in the 2016 ASHRAE Data Center Power Equipment Thermal Guidelines and Best Practices.



note 1: short-term refers to a period not greater than 96 consecutive hours, and not greater than 15 days in 1 year

Figure 1. ASHRAE and NEBS Temperature and Humidity Limits

In deciding what type of power system to deploy in support of an Edge Data Center, the overall wattage requirements must be considered. In addition to considerations regarding the amount of power necessary to support a Recover Point Objective and/or a Recovery Time Objective in the advent of a cessation on a primary line of electrical power delivery, the following considerations for power systems and power conditioning systems should be considered:

- Air flow and air conditioning support for the EDC;
- A consideration for hot flow and cold flow data center design;
- Intra-rack heat flow and heat dissipation methods; and
- Cross-rack heat and cooling flow for EDC's with multiple racks.

The design of power distribution units for Edge Data Centers should follow TIA-942 guidelines regarding the placement and availability of electrical receptacles and types, secondary electrical line placement, and the use of uninterruptible power supplies and generators to supplement electrical power during main line outages.

Further development of EDC security solutions will include methods and measurements relevant to the Types, Locations, and the Reliability, Accessibility, Serviceability (RAS) components.

IV. TELECOMMUNICATION CABLING RISK

Definition

The definition of Telecommunication Cabling Risk adopted by the Security Working Group is as follows:

Concerns related to an Edge Data Center's capability to support requisite communication types, synchronization, and throughput as stipulated in its commissioning manifest.

Considerations

In most EDC deployments, communication will be managed through the use of physical cabling which link the systems inside of the EDC to each other and to an external monitoring or management application. The types of cabling which need to be secured within an Edge Data Center are described below:

- **Incoming Cabling:**
  - Fiber and copper cables connecting the EDC to the core DC or another EDC;
  - Splice point, located inside or outside EDC;
  - Connection points, where pre-terminated cables are connecting EDC, located inside or outside of EDC; and
  - Cabling connecting EDC with end-user equipment (e.g. remote radio heads in mobile communication).
- **Cross/interconnect Points**: these are distribution points inside or outside EDC, which may:
  - Interconnect incoming cables to the active equipment within EDC;
  - Cross connect active equipment to another active equipment within EDC; and
  - Connect to other cross/interconnect points.
- **Internal Cabling:**
  - Cables between cross-connect points to the active equipment; and
  - Cables between splice or connection points to the cross-connects.
- **Service Cabling:**
  - These are cables connecting other security and environment elements, e.g. cameras, security locks, sensors that can be both outside and inside the EDC.

The Security Working Group recognizes that EDC deployments will make use of wireless monitoring solutions and Cloud Radio Access Networks in the future and have included a mention of mobile communication to support those developments.

Since 'Incoming Cabling' is one of the most critical and most vulnerable part of cabling infrastructure, the Security Working Group envisions that this function will be a characteristic supported in any assessment methodology pertaining to TIA's EDC collateral.

An example of the type of requirements which might be included in such an assessment are provided in Table 1:

RISK ASSESSMENT	POSSIBLE SOLUTIONS
Cable Failure (accidental or intentional)	
What happens when all incoming cables stopped functioning?	• Re-arrange the data flow to another EDC and send the signal to turn off the EDC (for example by using wireless connection protocols)
What happens when one or several of incoming cables stopped functioning but there is still at least one running channel?	• Switch to the redundant cable, put EDC operations to the alarm mode and follow the recovery plan
Cable Disruption (accidental or intentional)	
What if the incoming cable is facing disruptions?	• Switch EDC to the alarm mode or/and switch to the redundant cable
Is the cable being tapped?	• Observe and monitor eavesdropping possibility • Monitoring and detection of fiber performance at the physical level • End-to-end encryption solutions (working at a higher level)
Service degradation	• Monitoring of alien wavelengths or high -power jamming (out of scope of this paper)
Preventive Measures	
How easy is it to get access to the incoming cable?	• Underground cable laying should prevalent over the aerial • Warning labels, tapes alarming signal cable • Ducts and dedicated cable pathways in case of underground laying
How easy for an intruder or animals to damage the cable?	• Armored cables should prevalent over non-armored
How proper the cable is protected against the environment? (e.g. tornados, earthquakes)	• Redundant cables
Location and security of cable entry	• Inaccessible cable entry should prevalent
How safe is the splice point of incoming cables?	• Splice point inside the EDC space is preferable (but will not be always possible) • In case of external splice point, extra security measures should be taken, starting from a simple lock, up to intrusion detection and burglar alarm;

Table 1: Example Risk Assessment and Solutions Table

The simplest thing that can happen is when, intentionally or by accident, damage is sustained to the incoming cable plant. If there is no redundant cable or if the redundant cable has the same path and suffers the damage simultaneously, this completely paralyzes the operation of the EDC.

The risk assessment of vulnerability of incoming cabling infrastructure should include not just the perimeter of the EDC but also the complete path of the cable, including manholes, tunnels, maintenance holes and diverse distribution points along the path. As such, the analysis of operational capability which forms the reason for an assessment methodology in the TIA framework, would begin with these incoming cables and proceed to other aspects and concerns in the Edge Data Center.

Further development of EDC security solutions will include methods and measures relevant to the types and locations components identified by the Types and Locations Working Group.

V. ACCESS CONTROL RISK

Definition

The definition of Access Control Risk adopted by the Security Working Group is as follows:

Concerns related to the capability of the EDC to ensure that gaining control to, or of, assets is authorized and restricted based on organizational requirements.

Considerations

As the discussion of Edge Data Center security has moved through the first four sections of this paper, Access Control Risk provides the point at which confidential, approved, and authorized EDC physical entry or cyber security supported management is provisioned.

- **Tier 1:** Key-based, manually recorded log on entry (examples of what types of EDC this applies)
- **Tier 2:** Electronic access, automated recording of entry/exit. Cloud-based third-party allowed.
- **Tier 3:** Electronic access, integrated with identity management system, automated recording of entry/exit. No third-party cloud-based systems.
- **Tier 4:** Electronic access, dual-factor authentication (e.g. video verification, biometrics), automated logging of entry/exit/location. No third-party cloud-based systems.

In the methodology for providing assignations of risk tiers, the Security Working Group provides the reader with a concept which was developed to support the EDC gap analysis work which served as a pre-amble to TIA TR-42's discussions. It was uncovered, through discussions within the group, that many standards agencies and industry affiliated organizations had already provided tiered frameworks which could be leveraged to support an EDC framework. One such example was the use of the ASHRAE temperature and humidity tiers used above to describe power management systems in an EDC context.

Given the breadth and depth of these works, the Security Working Group believes that if there is sufficient interest on the part of the public, TIA members, and the telecommunication industry, that a tiered EDC framework could be developed through the aggregation of work already published.

VI. VIDEO SURVEILLANCE

Definition

The definition of Video Surveillance capability adopted by the Security Working Group is as follows:

Concerns relating to environmental effects, actual or attempted intrusion, or permissioned access to the EDC managed through the use of electronically captured images or data streams.

Considerations

Video surveillance has become an important part of many security solutions, and in the case of EDC security, serves as the first 'layered application' to support Access Control methodologies. A tiered approach for Video Surveillance capability in the context of an Edge Data Center might be represented as below:

- **Tier 1:** IP-based video surveillance of outside/perimeter with recorded video stored offsite for limited retention period.
- **Tier 2:** IP-based video surveillance of outside/perimeter, cyber-security protocols manually implemented. Retention period longer than 30 days.

- **Tier 3:** IP-based video surveillance of both outside and inside of enclosure. Cyber-security protocols to NIST/CIS framework automatically applied. Retention period of 90 days or longer.
- **Tier 4:** IP-based video surveillance of outside and inside of enclosure, Cyber-security protocols to NIST/CIS framework automatically applied. Yearly testing for vulnerabilities. Retention period of 180 days or longer.

Due to the rise of video surveillance as a security measure, it is believed that providing a mechanism for establishing the use of such a technology in the context of privacy, organizational compliance, and governance is an area which could benefit from future developments by TIA and the Security Working Group.

VII. SECURITY METRICS

Definition

The definition of Security Metrics adopted by the Security Working Group is as follows:

Concerns regarding the acquisition and reporting of measurements traceable to specific EDC assets.

Considertaions

Originally, the Security Working Group was focused on physical security and cyber security and how to recommend risk management procedures for both types. As the group's efforts developed, the reliance on TIA-942 standard as a baseline led to the discussion of how to support physical security first, and then extend into more cyber security considerations in later versions. These efforts could best be directed toward increasing the reliance on the TIA-942 standards, rather than draw attention toward cyber security considerations at this time.

The physical security metrics for the EDC framework would derive from the sensors, machines, and software which support the six security attributes, listed above. EDC developers and users can obtain sufficient information to keep the EDC compliant with its commissioned manifest through the use of monitoring and administration tools which can render the data available into an 'EDC dashboard' organized through the use of operation, administration, management, and automation techniques recommended by the OAMA team developing that material.

The physical security components of the EDC dashboard would serve as examples for how cyber security considerations would be introduced to the dashboard through the use of future versions of this documentation.

Examples of Metrics

- **Video Surveillance:**
  - Video Uptime
  - Video Retention Met
  - All cameras accounted for
  - % of devices with current firmware
  - Scanned for cyber threats
  - Private certificates/chain-of-trus
  - Password management "protocol"
- **Access Control:**
  - Access Uptime
  - Failed Access Attempts

    - % of devices with current firmware
    - Scanned for cyber threats
    - Private certificates/chain-of-trust
    - Password management "protocol"
- **Cabling:**
    - Electrical monitoring
    - "Eavesdropping" or other breaches – scan for threats (pen testing, etc)
    - How to assess degradation of cable
    - Cable tampering/connector modifications
- **Environmental:**
    - Battery life monitoring/reporting
    - Security Risk Assessments completed on time (including assessment of countermeasures and response time)
    - Number required will vary based on tier (e.g. lowest tier might just have at system commissioning)
- **Alerts:**
    - How they are responded to
    - What percent are false
    - Is video verification used

VIII. CLOSING THOUGHTS

"Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance." [1]

The Security Working Group understands that these considerations are a step in the direction of providing guidance for Edge Data Center sponsors, designers, and users. In this step, the collected work of several team members has been assembled for an this article which is now offered for review in compliance with TIA practices. The Security Working Group believes that providing insights and considerations that can serve as guidance to an EDC Risk Management will help lead the success of EDC into the future. To learn more about the TIA's Working Group efforts in developing information and standards on Edge Data Centers (EDCs), go to the TIA website: www.tiaonline.org. If you have opinions or expertise to lend to this effort, please reach out to edcinfo@tiaonline.org.

** Disclaimer: The information and views contained in this article are solely those of its authors and do not reflect the consensus opinion of TIA members or of TIA Engineering Committee TR-42. This article is for information purposes only and it is intended to generate opinion and feedback so that the authors and TIA members can learn, refine, and update this article over time. The Telecommunications Industry Association does not endorse or promote any product, service, company or service provider. Photos and products used as examples in this paper are solely for information purposes and do not constitute an endorsement by TIA.*

[1] NIST paper – Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018