ICT TODAY
THE OFFICIAL TRADE JOURNAL OF BICSI

July/August/September 2024
Volume 45, Number 3

CYBERSECURITY CHALLENGES AND OPPORTUNITIES

IN THE REALM OF EDGE COMPUTING AND IoT

PLUS:

+ The Three "C's" in Agility Applied to Data Center Projects
+ Colocation—Not Just for Data Centers

BICSI®

SAVE THE DATE

BICSI 2025 WINTER

2-6 February in Kissimmee, Florida

CALL FOR PRESENTERS NOW OPEN

Submit by:
23 September 2024

Gaylord Palms Resort & Convention Center

bicsi.org/winter

JULY/AUGUST/SEPTEMBER 2024
Volume 45, Issue 3

contents

SUBMISSION POLICY

ICT TODAY is published quarterly by E&M Consulting, Inc. and is sent in digital format to BICSI members and credential holders.

ICT TODAY welcomes and encourages submissions and suggestions from its readers. Articles of a technical, vendor-neutral nature are gladly accepted for publication with approval from the Editorial Review Board. However, BICSI, Inc., reserves the right to edit and alter such material for space or other considerations and to publish or otherwise use such material.

The articles, opinions, and ideas expressed herein are the sole responsibility of the contributing authors and do not necessarily reflect the opinion of BICSI, its members, or its staff. BICSI is not liable in any way, manner, or form for the articles' opinions and ideas. Readers are urged to exercise professional caution in undertaking any of the recommendations or suggestions made by authors.

No part of this publication may be reproduced in any form or by any means, electronic or mechanical, without permission from BICSI, Inc.

ADVERTISING: Advertising rates and information are provided upon request. Contact E&M Consulting, Inc. for information at +1 800.572.0011 x107 or caleb.t@emconsultinginc.com. Publication of advertising should not be deemed as endorsement by BICSI, Inc. BICSI reserves the right in its sole and absolute discretion to reject any advertisement at any time by any party.

© Copyright BICSI, 2024. All rights reserved. BICSI and all other registered trademarks within are property of BICSI, Inc.

ICT TODAY

THE OFFICIAL TRADE JOURNAL OF BICSI

BICSI BOARD OF DIRECTORS

Board President David M. Richards, RCDD, NTS, OSP, TECH, CT

Board Vice Chair Todd W. Taylor, RCDD, NTS, OSP

Board Secretary Rick Ciordia, PE, RCDD, DCDC, RTPM

Board Treasurer William Foy, RCDD, NTS, OSP, WD, ESS, DCDC

Global Regional Director Fernando Neto, RCDD

U.S. Western Regional Director Luke Clawson, RCDD, RTPM, GROL, MBA

At-Large Director Peter P. Charland III, RCDD, RTPM, DCDC, SMIEEE, CET, NTS, ESS, WD

At-Large Director Ninad Desai, RCDD, NTS, OSP, TECH, CT

At-Large Director William "Joe" Fallon, AVSEC PM, RCDD, ESS, PSP, CISSP

At-Large Director Trevor Kleinert, RCDD, DCDC, NTS, TECH, CT

At-Large Director Jay Thompson, RCDD

Chief Executive Officer John H. Daniels, CNM, FACHE, FHIMSS, CPHIMS

EDITORIAL REVIEW BOARD

Beatriz Bezos, RCDD, DCDC, ESS, NTS, OSP, PE, PMP

Jonathan L. Jew

F. Patrick Mahoney, RCDD, CDT

PUBLISHER

E&M Consulting, Inc., 1107 Hazeltine Boulevard, Suite #350, Chaska, MN 55318

Phone: 800.572.0011 **Web:** www.emconsultinginc.com

EDITOR

Kristin Allman, icttodayeditor@emconsultinginc.com

PUBLICATION STAFF

Clarke Hammersley, Director, Technical Publications

Jeff Giarrizzo, Senior Technical Editor

Allen Dean, Senior Technical Editor

ADVERTISER'S INDEX

ICT TODAY NEEDS WRITERS

ICT Today is BICSI's premier publication for authoritative, vendor-neutral coverage and insight on next generation and emerging technologies, standards, trends, and applications in the global ICT community. Consider sharing your industry knowledge and expertise by becoming a contributing writer to this informative publication.

Contact **icttodayeditor@emconsultinginc.com** if you are interested in submitting an article.

ADVERTISING SALES

800.572.0011 or
caleb.t@emconsultinginc.com

From BICSI's Board President David M. Richards, RCDD, NTS, OSP, TECH, CT

EMERGING ICT TRENDS ARE NOW COMMONPLACE

It is hard to believe that even though I am writing this letter in the springtime, this issue of our trade journal will not be published until sometime in the middle of summer in our northern hemisphere. By now, the BICSI board of directors will have already finished collaborating with BICSI staff on their proposed business plans and budget requests to carry out and execute the board's strategic plan adopted for our next fiscal year. I am proud to state that BICSI has been enjoying a strong start to 2024, and we are poised to take it to the next level as fiscal year 25 officially begins for us on July 1.

Just think: "Convergence" was once considered an emerging trend. I am excited to see that our *ICT Today* trade journal has continued to embrace the evolutions of ICT and has matured well itself, as demonstrated by the variety of fascinating articles we have gathered from some very talented industry professionals. It is also great to see so many traditional cabling contractors continue to expand into the ever-evolving world of systems integration, hence the wide spectrum of technology, from edge computing and shielded cabling deployments to cybersecurity and colocation considerations, covered in this issue. Speaking of convergence, judging by the titles of the articles you are about to dive into, it is clear that BICSI continues to recognize and embrace all facets of the ICT industry.

I recall back in 2019, while I was a product manager, writing an article for another trade publication on what was then considered an emerging trend: edge computing! I am personally looking forward to reading the article penned by one of this issue's contributors titled "Cybersecurity Challenges and Opportunities in the Realm of Edge Computing and IoT." I am curious to see how my now half-decade-old article has stood the test of time... fingers crossed!

Some may ask: Why is there an article referencing cybersecurity in a BICSI trade journal? The answer: As more and more traditional cabling infrastructure contractors expand their businesses into the world of systems integration and adopt some of the abundance of ICT technology offerings in their day-to-day business plans, we should always remember to treat cybersecurity from a technological perspective as a necessary discipline, just as a construction contractor does when it comes to personnel safety. Risk engineering, as it is sometimes referred to by network engineers, is a term that systems integrators need to be well acquainted with. One has to be proactive as opposed to reactive with both disciplines. After all, the protection of intellectual property for our customers, as well as their customers, starts in the design process and continues into perpetuity.

Until the next issue, keep advancing your knowledge and upskilling in the ICT industry. I look forward to seeing you at a BICSI event soon. Go BICSI!

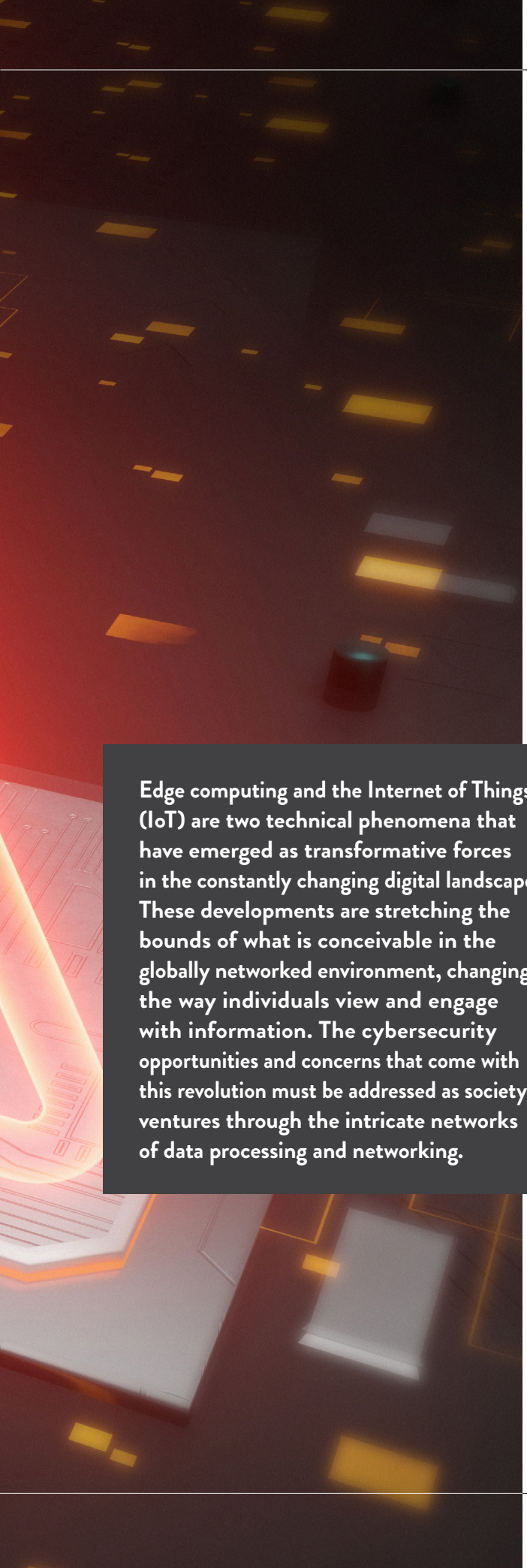
Best regards,

COVER ARTICLE

By Khiro Mishra

CYBERSECURITY CHALLENGES AND OPPORTUNITIES

IN THE REALM OF EDGE COMPUTING AND IoT



Edge computing and the Internet of Things (IoT) are two technical phenomena that have emerged as transformative forces in the constantly changing digital landscape. These developments are stretching the bounds of what is conceivable in the globally networked environment, changing the way individuals view and engage with information. The cybersecurity opportunities and concerns that come with this revolution must be addressed as society ventures through the intricate networks of data processing and networking.

As connected devices proliferate inside IoT ecosystems, new avenues for cyber threats to enter the system are created, underscoring the importance of strong security protocols and proactive risk management techniques.

Edge computing, with its decentralized architecture, offers enhanced speed and efficiency but also raises concerns about data privacy and security, requiring careful implementation and monitoring. Organizations must prioritize cybersecurity and develop a comprehensive strategy that incorporates cutting-edge technologies like Blockchain and artificial intelligence (AI) to fully realize the potential of edge computing and IoT.

As these transformative technologies are embraced, collaboration among industry stakeholders, policymakers, and cybersecurity experts will be crucial to ensuring a secure and resilient digital future.

The impact of IoT and edge computing, its core elements, key cybersecurity priorities, and its challenges and opportunities will be addressed in this detailed article.

THE TRANSFORMATIVE IMPACT OF EDGE COMPUTING AND IoT

Edge computing and the IoT have revolutionized how individuals process and utilize data. With edge computing, processing power is moved closer to where data is generated, reducing latency and enabling faster decision-making. This means that devices can process and act on data in real time without needing to send it back to centralized data centers.

This has a transformative impact across various industries. For example, in healthcare, edge computing allows for real-time monitoring of patient vital signs, enabling immediate intervention in case of emergencies. In manufacturing, IoT devices can communicate with each other to optimize production processes and reduce downtime.

Furthermore, the integration of edge AI allows devices to make intelligent decisions locally without needing to rely on cloud services. This opens up new possibilities for applications, such as autonomous vehicles, smart cities, and predictive maintenance.

Overall, the combination of edge computing and IoT is driving significant advancements in efficiency, speed, and capabilities across industries, paving the way for a more connected and intelligent world.

THE CORE ELEMENTS OF IoT AND EDGE COMPUTING

From the perspective of IoT and edge computing, the core elements of these technologies are intertwined to create a powerful ecosystem of connected devices and data processing capabilities. IoT is comprised of interconnected devices, ranging from smart home gadgets to industrial sensors, that collect and transmit data. This network enables the seamless exchange of information between devices, leading to enhanced automation and efficiency in various applications.

On the other hand, edge computing complements IoT by bringing data processing closer to the source. This means that devices can analyze and act on data locally, reducing latency and enhancing privacy and security. Edge analytics plays a crucial role in this process, enabling devices to process data efficiently and make informed decisions in real time. Furthermore, the integration of 5G connectivity has revolutionized IoT by enabling faster and more reliable communication between devices. This facilitates real-time data transmission and response, opening up new possibilities for applications that require high-speed connectivity.

Overall, the collaboration between edge computing and IoT is symbiotic, with each technology enhancing the capabilities of the other. This partnership has the potential to revolutionize industries by enabling data-driven decision-making and unprecedented connectivity (Figure 1).

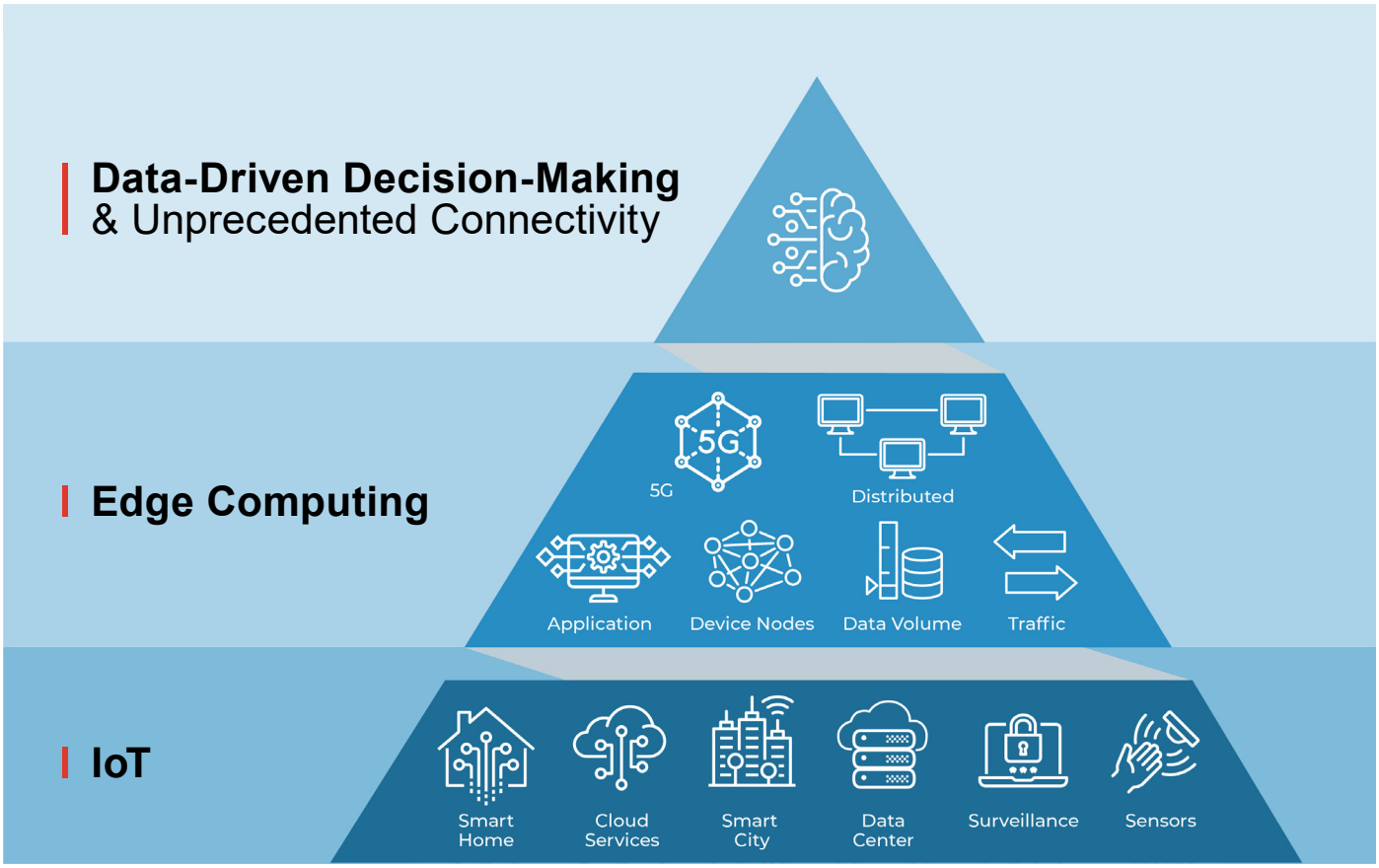


FIGURE 1: Edge computing and the Internet of Things (IoT) are transformative forces in the digital landscape, enabling data-driven decision-making and unprecedented connectivity, reshaping how we interact with information and necessitating attention to cybersecurity as we navigate the complexities of data processing and networking.

KEY CYBERSECURITY PRIORITIES

In the realm of edge computing and IoT, it is crucial to recognize the cybersecurity implications that accompany their advancements. Here are some key cybersecurity considerations:

Resolving Security Vulnerabilities in IoT and Edge Computing

New attack surfaces are introduced by the scattered nature of edge computing and the interconnection of IoT devices. Robust access restrictions, secure communication protocols, and device-level security are all necessary components of an all-encompassing security strategy for these contexts (Figure 2).

FIGURE 2: In the realm of edge computing and IoT, it is crucial to recognize the cybersecurity implications that accompany their advancements, as the increasing interconnectivity and real-time data processing create new vulnerabilities and potential entry points for cyber threats, necessitating robust security measures to protect sensitive information and ensure system integrity.

Issues with Privacy and Data Security Techniques

IoT devices create vast amounts of data, which raises privacy concerns for individuals and businesses. Organizations might find it difficult to strike a balance between data collection for innovation and protecting personal data. Adequate data protection tactics are necessary to guarantee user confidence and adherence to privacy laws.

Regulatory and Ethical Considerations

As the digital landscape evolves, regulatory frameworks struggle to keep pace. Ethical considerations surrounding data usage, consent, and the responsible deployment of emerging technologies become paramount. Navigating this complex terrain requires a proactive approach to compliance and ethical decision-making.

CYBERSECURITY CHALLENGES IN IoT AND EDGE COMPUTING

The IoT and edge computing have brought up several new risks or challenges that call for specific cybersecurity considerations.

Decentralized Data Processing

The decentralized nature of edge computing's data processing presents one major obstacle. In contrast to conventional centralized systems, which handle data in a regulated setting, edge computing distributes computation among multiple devices. The possibility of sensitive data being exposed in transit and at the endpoints is increased by this decentralization.

Greater Surface Areas for Attacks

The proliferation of IoT devices exponentially expands the attack surface for potential cyber threats. Every linked device, from industrial sensors to smart home appliances, represents a possible point of entry for hackers. Hackers can take advantage of the complicated environment created by the wide variety of devices and their differing security standards.

Integrating Frequently Insecure IoT Devices

When designing IoT devices, robust security safeguards are typically neglected in favor of functionality and cost-effectiveness. These devices' inherent insecurity presents a significant issue as they are integrated into the broader edge computing environment. Security vulnerabilities in IoT devices could serve as points of entry for hackers to gain access to the entire network.

Data Security

In the linked world of edge computing and the IoT, user data privacy becomes critical. There is a higher chance of illegal access and disclosure when data is processed closer to the source. Examples from the real world include data breaches that result in privacy violations by compromising personal information from IoT devices, including home security cameras.

Device Verification

A key issue in the IoT ecosystem is confirming the identity of devices. Improper access control and possible device manipulation can result from weak authentication procedures. Notable examples include incidents in which hackers were able to seize control of vital infrastructure elements, such as smart city systems, due to inadequate authentication procedures.

Network Security

As edge computing is distributed and dynamic, strong network security protocols are needed. Network security vulnerabilities expose weaknesses that hackers can exploit to intercept and alter data during transmission. Attacks on industrial edge networks that cause disruptions to operations and compromise confidential data are examples of real-world occurrences (Figure 3).

FIGURE 3: Given the distributed and dynamic nature of edge computing, robust network security protocols are essential to prevent vulnerabilities that hackers can exploit to intercept and manipulate data during transmission, as evidenced by real-world attacks on industrial edge networks that disrupt operations and compromise confidential information.

> *"Security vulnerabilities in IoT devices could serve as points of entry for hackers to gain access to the entire network."*

Supply Chain Vulnerabilities

The complex supply chains involved in manufacturing IoT devices can introduce vulnerabilities. Malicious hackers or cybercriminals can exploit these vulnerabilities to implant backdoors or compromise devices before they even reach the end-user, posing significant security risks.

Insufficient Security Awareness

Many users and organizations lack awareness of the security risks associated with IoT devices and edge computing. This can lead to poor security practices, such as using default passwords or failing to update devices regularly, making them more susceptible to cyberattacks.

Lack of Patch Management

IoT devices and edge computing systems often lack robust patch management practices. This can result in devices running outdated and vulnerable software, making them easy targets for cyberattacks. For example, the Mirai botnet attack exploited unpatched IoT devices to launch large-scale distributed denial-of-service (DDoS) attacks.

Understanding these challenges is essential for developing comprehensive cybersecurity strategies tailored to the unique demands of edge computing and IoT. Let us have a look at the opportunities for enhanced cybersecurity.

UNLOCKING ENHANCED CYBERSECURITY: EXPLORING OPPORTUNITIES AND INNOVATIONS

While edge computing and the IoT present significant cybersecurity challenges, they also offer unique opportunities to enhance and strengthen cybersecurity measures. It is worth exploring the positive aspects and opportunities for leveraging these technologies for improved cybersecurity (Figure 4).

FIGURE 4: While edge computing and IoT introduce significant cybersecurity challenges, they also present unique opportunities to enhance and fortify cybersecurity measures, highlighting the potential for these technologies to be leveraged for improved security practices and resilience against threats.

AI-Driven Security Protocols

AI is a major force in the cybersecurity revolution. Security protocols powered by AI can evaluate large volumes of data, spot trends, and quickly spot abnormalities. Machine learning (ML) algorithms offer a proactive defense against sophisticated cyberattacks by adapting to changing threats.

Network Monitoring Capabilities

IoT devices equipped with monitoring sensors can actively contribute to network security. These devices can detect unusual patterns, monitor network traffic, and provide real-time information on network health. Integrating these capabilities into a comprehensive cybersecurity strategy adds a layer of defense.

Improved Visibility

IoT devices generate a wealth of data that, when properly analyzed, can provide valuable insights into network activities. By harnessing this data, organizations can gain enhanced visibility into their network, enabling them to identify potential security threats and vulnerabilities.

Real-Time Anomaly Detection

Edge computing enables real-time analysis and processing of data at the source. This capability is invaluable for implementing real-time anomaly detection systems. By identifying unusual patterns or behaviors in data, these systems can quickly flag potential security threats, allowing for swift response and mitigation.

Decentralized Security Models

Leveraging the decentralized nature of edge computing, organizations can adopt innovative security models. Distributing security measures across the network and devices can minimize the impact of a potential breach. This approach enhances resilience by reducing the likelihood of a single point of failure, a common vulnerability in centralized systems.

Improved Authentication and Access Control

Edge computing and IoT devices can enhance authentication and access control mechanisms. For example, biometric authentication can be integrated into IoT devices to ensure that only authorized individuals have access. Additionally, edge computing can enable localized access control decisions, reducing reliance on centralized authentication servers.

Enhanced Incident Response

Edge computing and IoT can improve incident response capabilities by enabling faster detection and containment of security breaches. Real-time data processing and analysis allow for immediate identification of anomalies, enabling quick and targeted responses to potential threats.

Secure Firmware Updates

Edge computing and IoT can improve the security of firmware updates by enabling secure, over-the-air updates. This ensures that devices are always running the latest, most secure software versions, reducing the risk of vulnerabilities being exploited.

THE IMPORTANCE OF PROACTIVE CYBER-SECURITY MEASURES IN HARNESSING THE POTENTIAL OF IoT AND EDGE COMPUTING

The IoT and edge computing cannot be fully implemented without proactive and innovative cybersecurity measures. These technologies bring a lot of convenience and efficiency to our daily lives and businesses as they become more common. However, they also bring new cybersecurity risks.

Adopting proactive measures is crucial to detecting and reducing these dangers before cybercriminals can take advantage of them. Organizations can enhance the security of their data, devices, and networks by foreseeing possible attacks and vulnerabilities.

Furthermore, in the ever-changing world of edge computing and the IoT, innovative cybersecurity tactics are essential for being one step ahead of cyber threats. To identify and address threats in real time, these strategies make use of cutting-edge technologies like AI and ML.

Through the adoption of proactive and inventive cybersecurity solutions, organizations can optimize the advantages of edge computing and IoT while strengthening their security posture. By guaranteeing the reliability, precision, and privacy of their data, they can safely and securely realize the full potential of these game-changing technologies.

CONCLUDING THOUGHTS

In conclusion, the quickly changing technological landscape, especially with the rise of edge computing and IoT, highlights the vital necessity for collaboration between cybersecurity specialists, developers, and policymakers. For these interconnected systems to guarantee data availability, integrity, and confidentiality, strong security frameworks and standards must be established (Figure 5).

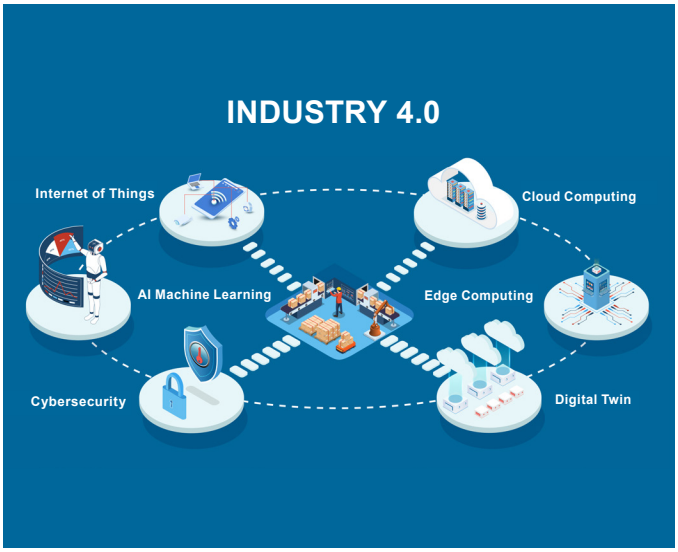


FIGURE 5: Industry 4.0 encompasses IoT, cloud computing, edge computing, digital twin, cybersecurity, and AI machine learning to revolutionize processes through interconnected, intelligent, and secure systems that enable real-time data analysis, simulation, and automation.

Involving developers is essential to the design and implementation of safe systems because they use cybersecurity experts' knowledge to find and fix flaws. Policymakers have a critical role in creating and enforcing regulations that promote cybersecurity best practices and hold businesses accountable for security breaches.

Working together, these stakeholders can effectively tackle the intricate and dynamic nature of cyber threats. This can create a safer digital environment for all, fostering innovation while safeguarding against potential risks. To further enhance cybersecurity, ongoing education and awareness programs are crucial. These courses can assist both individuals and organizations in appreciating the value of cybersecurity procedures and in keeping abreast of emerging risks and countermeasures.

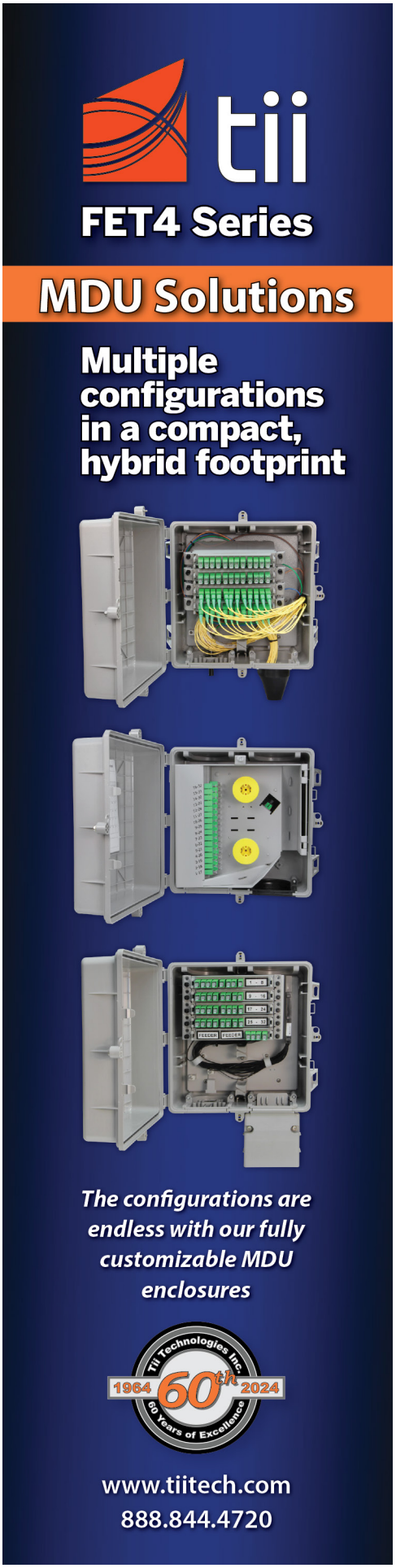
Furthermore, it is crucial to incorporate security by design principles into the development of edge computing platforms and IoT devices. By taking security into account at every stage, vulnerabilities can be found and fixed early on in the design and development process, lowering the likelihood of exploitation.

It is recommended to carry out routine security audits and assessments to detect and address any potential vulnerabilities present in the current systems. By being proactive, it is possible to reduce the possibility of security breaches and lessen their effects when they do happen.

Overall, a comprehensive approach to cybersecurity that includes collaboration, education, and proactive measures is essential to protect edge computing and IoT systems and ensure a secure digital future.

AUTHOR BIOGRAPHY:

Khiro Mishra is a global cybersecurity leader with 25 years of industry experience. As CEO of Cybalt, Khiro is responsible for creating the strategy and driving its execution to establish Cybalt as a global leader in providing next-generation cybersecurity solutions and services. Khiro can be reached at discover@cybalt.com.



THE THREE "C'S" IN AGILITY

Applied to Data Center Projects

By Yuri William Bravo Asencios

1. INTRODUCTION

The technological changes occurring in the IT infrastructure of data centers, driven by the accelerated growth in the demand for data processing within organizations and the need for increasingly faster transmission speeds, necessitate that productive data centers implement changes to accommodate higher capacities and more advanced technologies.

This article focuses on how to respond to this need to make these changes in environments considered mission-critical in an effective way, using an agile approach, considering the context of uncertainty and risk typical of these scenarios.

The article presents the agile approach based on the Scrum framework, characterized by the involvement of the customer in the outcome of the project and the achievement of results in short and incremental deadlines. The Scrum framework is characterized by roles, ceremonies, and artifacts. Three aspects are key to successfully managing an agile project: commitment, communication, and team collaboration.

"When discussing a type of data center, it is important to consider the expected level of availability and reliability."

2. THEORETICAL FRAMEWORK:

2.1. Context

According to the ANSI/BICSI-002-2024 standard,[1] a data center has support spaces such as:

- Computing Room
- Security Room
- Telecommunications Entrance Room
- Command Center
- Helpdesk
- Print
- Loading Dock
- Secured Storage for High Value
- Staging and Assembly
- Vendor Storage
- Print Storage
- Engineering Offices
- UPS, Battery, and DC Systems
- Service Entrance Normal and Emergency Switchboard
- Chillers, Water Treatment, HVAC, and Pumping Systems
- Network Lab and Repair
- Software Library
- Tape Library

Due to its function, each of these areas is important, and carrying out installations or modifications in any of them carries a level of risk that must be considered, considering the topology and reliability level of the data center.

For example, consider the scenario of a Class F3 data center undergoing maintenance or improvements on a generator. Given the topology and redundancy of a data center of this reliability level, its operation will not be affected. The risk will be lower because a data center of this level must have another source of energy in addition to the commercial supply. It is true that reliability is affected during the intervention, but considering the topology and the redundancy of the electrical system, it is a risk that can be considered controlled (Figure 1).

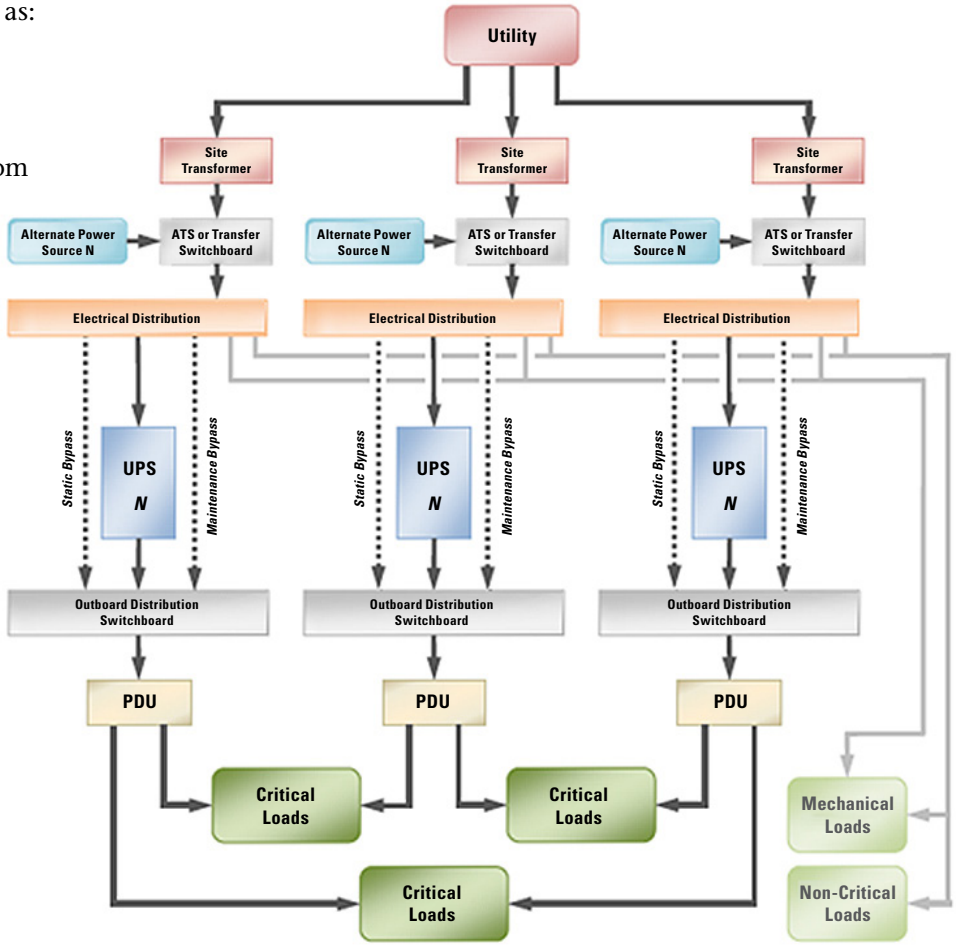


FIGURE 1: Electrical topology of a Class F3 data center (distributed redundancy). Image Credit: ANSI/BICSI 002-2024, p. 111.[1]

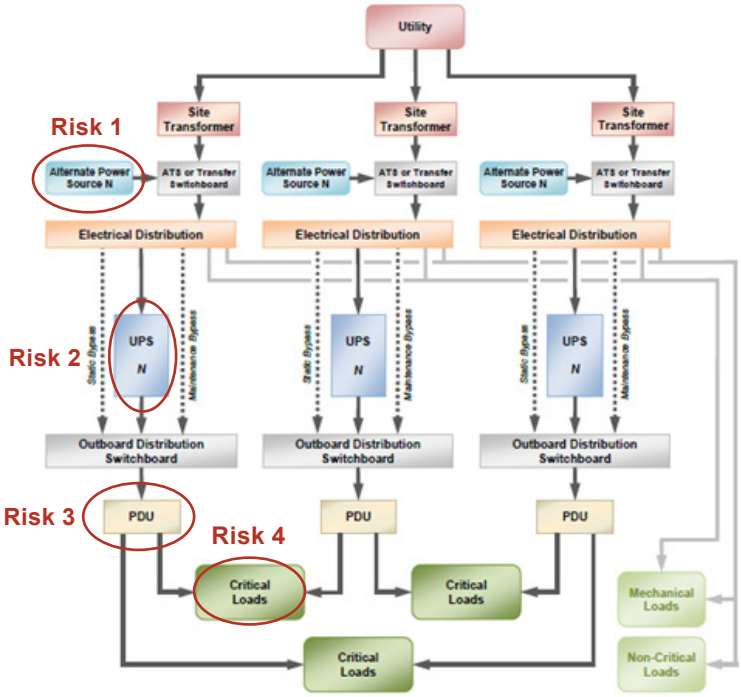


FIGURE 2: Risk levels in the electrical topology of a Class F3 data center (distributed redundancy). Image Credit: ANSI/BICSI 002-2024, p. 111,[1] with the author's annotations in red.

However, if the change is made to a component closer to the critical load (IT equipment), the risk of generating an impact on IT operations is greater, as shown in Figure 2; for example, an intervention in one of the AC power sources will have a risk of 1, an intervention in one of the UPSs will have a risk of 2, an intervention in one of the PDUs will have a risk of 3, and, on the other hand, an intervention in the critical loads (cabinets containing IT equipment) will have a risk of 4.

In this article, the project will be called the "April Project." The context is a Class F3 data center according to ANSI/BICSI 002-2024,[1] and the intervention considered is in the computer room, close to the critical load. That is, the April Project seeks to respond to the need to make a change in the data center area with the greatest risk of impacting the operation of IT services provided by the data center.

2.2. Risk of Interruption of a Data Center

According to the Uptime Institute's Annual Outage Analysis 2024, in a survey of 781 data center operators, 55 percent reported having experienced some level of service interruption, ranging from minor to severe, in the past three years.[2]

In the same report, the Uptime Institute states that, based on its studies, the human factor contributes to between two-thirds and four-fifths of reported data center outages.[2] When 418 data center operators were asked about the most common causes of interruptions related to human error, the top causes were failure to follow procedures (48 percent) and incorrect processes/procedures (45 percent).

Obviously, in the case of the April Project, since it is an intervention in the computer room of a Class F3 data center, it is very important to comply with the processes and procedures established for the work, which must be carried out at all times.

When discussing a type of data center, it is important to consider the expected level of availability and reliability. Reliability is understood as the frequency of failure or crash of a component or system, such as the mean time between failures (MTBF). Similarly, availability is the amount of time that power and cooling are available for IT operations.

The ANSI/BICSI 002-2024 standard[1] proposes a risk assessment scheme to determine the type of data center required for an organization based on the needs of IT operations and the responsibilities acquired with internal or external customers. The data center class is determined by the impact of the data center disruption, as shown in Figure 3.

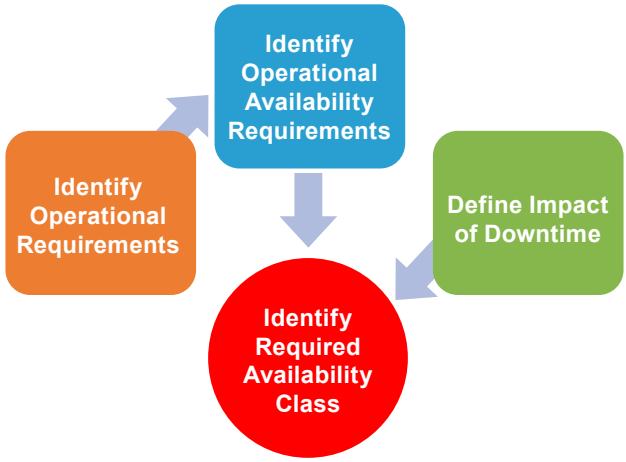


FIGURE 3: Evaluation of factors to determine data center class. Image Credit: Adapted from ANSI/BICSI 002-2024 BICSI 2024, p. 461.[1]

2.3. Risk Mitigation in a Data Center

According to Project Management Institute's (PMI) Standard for Risk Management in Portfolios, Programs, and Projects, risk mitigation actions are taken to reduce the probability of occurrence and/or the impact of a threat. Likewise, it recommends that mitigation actions be taken in the early stages of projects, as they allow for more effective repair of the damage that could have occurred if a risk had materialized. A mitigation action, it points out, might be able to reduce the impact by focusing on the factors that drive the severity.[3]

As in any project, the April Project requires appropriate risk management, which can be performed using the framework recommended in BICSI's Essentials of Data Center Projects, 2nd Edition document (Figure 4).[4]

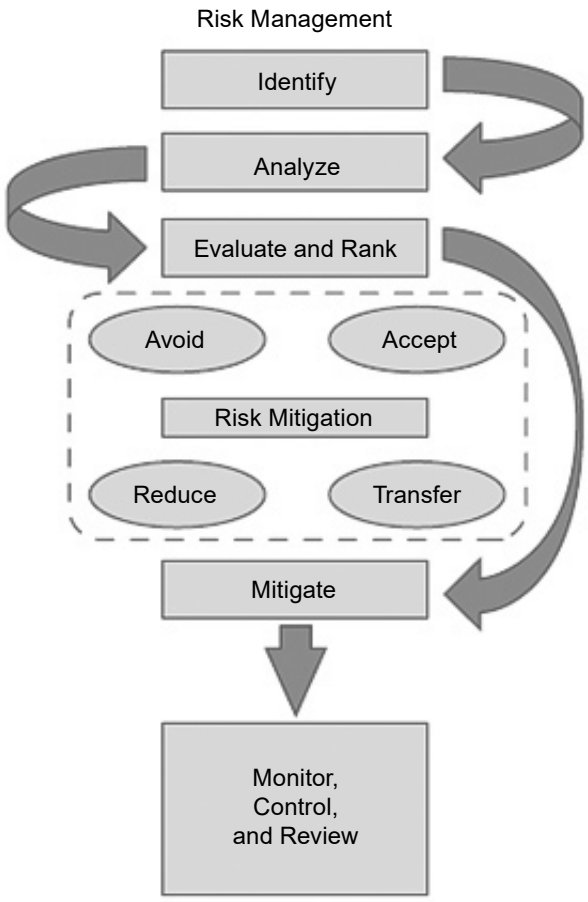


FIGURE 4: Risk management life cycle. Image Credit: Essentials of Data Center Projects, 2nd Edition, BICSI 2024, p. 6–1.[4]

In projects using an agile approach, management must take into account iterations (sprints), which will be discussed later in this article.

2.4. The Agile Approach in a Project

Typically, infrastructure projects have been developed using a traditional or waterfall approach. This article describes the use of agile practices. Figure 5 summarizes the characteristics of each type of approach. The purpose of this article is not to delve into these approaches but rather to describe the use of agile practices and their benefits.

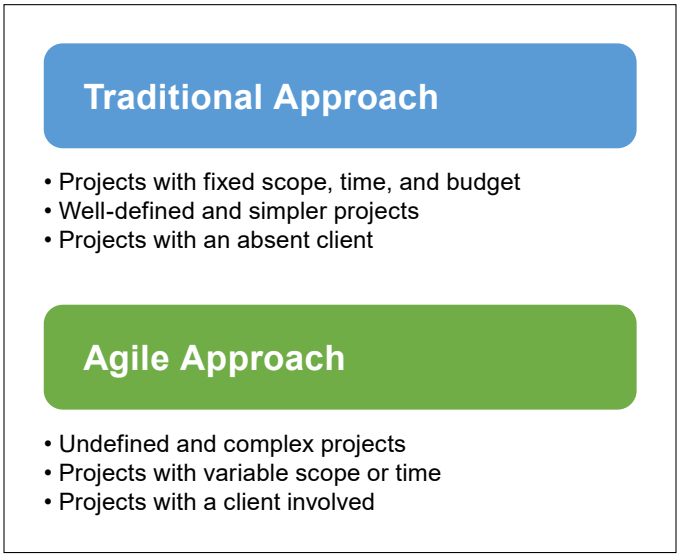


FIGURE 5: Traditional Approach vs. Agile Approach.

It is necessary to clarify that the decision to choose one or another type of approach in a project must be evaluated considering several factors, starting with the organizational culture, the experience of the working team in agile projects, and the characteristics of the project, as well as the development phase. It is recommended to read the article: "Is It Possible to Use Agility in a Data Center Project?" published in *ICT Today* in 2023; in this article, a methodology is proposed that helps to determine which is the most recommended approach.[5]

The traditional or waterfall approach is recommended when the scope is clear, and there is a fixed schedule and budget. This type of project has sequential phases,

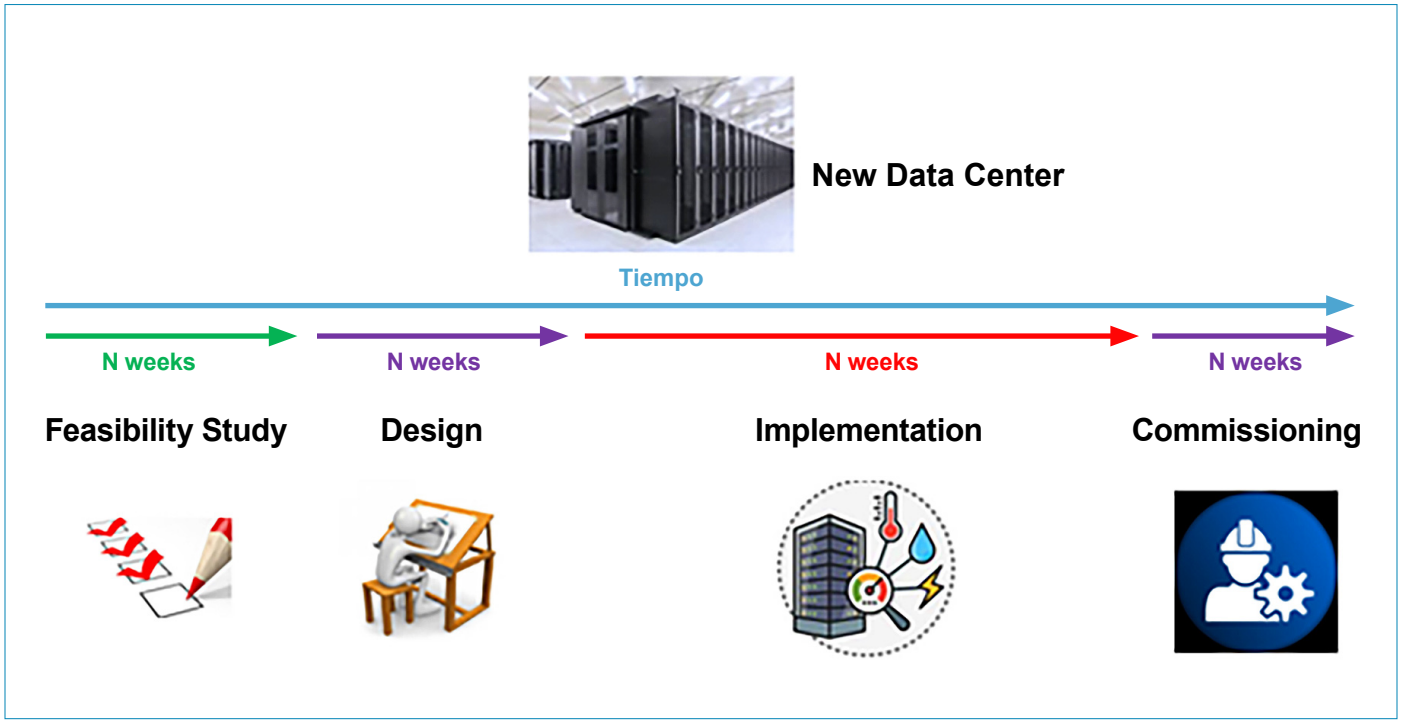


FIGURE 6: Traditional or waterfall approach.

and customer involvement is less. Figure 6 shows a simplified diagram of the implementation phases of a data center under a traditional approach.

Regarding the agile approach, this article considers practices of the Scrum framework, which is very widely used in projects that require an iterative and incremental approach and are characterized by complexity and uncertainty, with variable scope and time, and where there is customer involvement. The reader is invited to think about their infrastructure project in the computer room of their data center, for example, in the installation of overhead cabling trays, optical fiber cabling for high-density servers, or electrical circuits for power outlet units in cabinets, etc. In all of these cases, when considering a data center in production, one encounters a complex scenario, given that the services must be interrupted at some point. There will be uncertainty about the intervention date for some equipment, and perhaps, in some cases, it may be overly complicated. To address this, it is required that the owners of the technologies be strongly involved. The approach could involve working by sectors and on them in shorter periods of time, wherein each period, the entire process of feasibility, design, implementation, and testing is carried out to obtain feedback from the customer.

Figure 7 presents a diagram of an iteration of the Scrum framework. It shows elements such as the product backlog, sprint backlog, daily meeting, sprint review, and sprint retrospective, whose applications in the April Project will be seen in more detail in later lines.

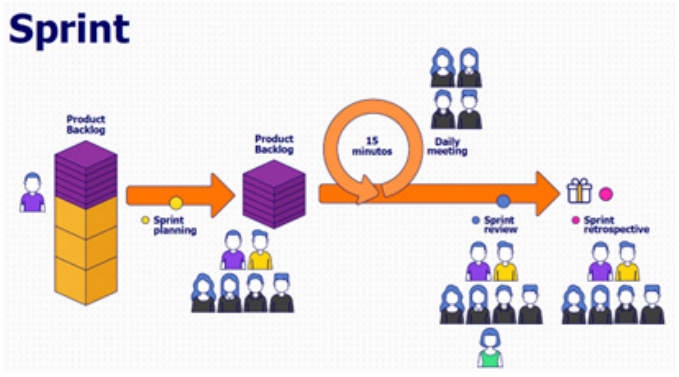


FIGURE 7: Agile Scrum Framework Sprint. Image Credit: Credicorp.

3. APPLICATION OF THE THREE C'S OF AGILITY IN A DATA CENTER PROJECT:

3.1. Application Case

This article examines the "April Project," an IT infrastructure project in the closets of an operational data center.

3.2. The Team

As in any project or initiative, there is a project manager (PM) who is responsible for the administrative management of the project, a user leader (UL) who is the customer for whom the initiative will be carried out, and a technical leader (TL) who is responsible for the technical management of the project. The organization's stakeholders with which there will be some interaction, for example, purchasing management, legal management, logistics, etc., will also need to be considered.

This discussion focuses on the roles of the Scrum framework, specifically the project owner (PO), scrum master (SM), and the development team, as shown in Figure 8.

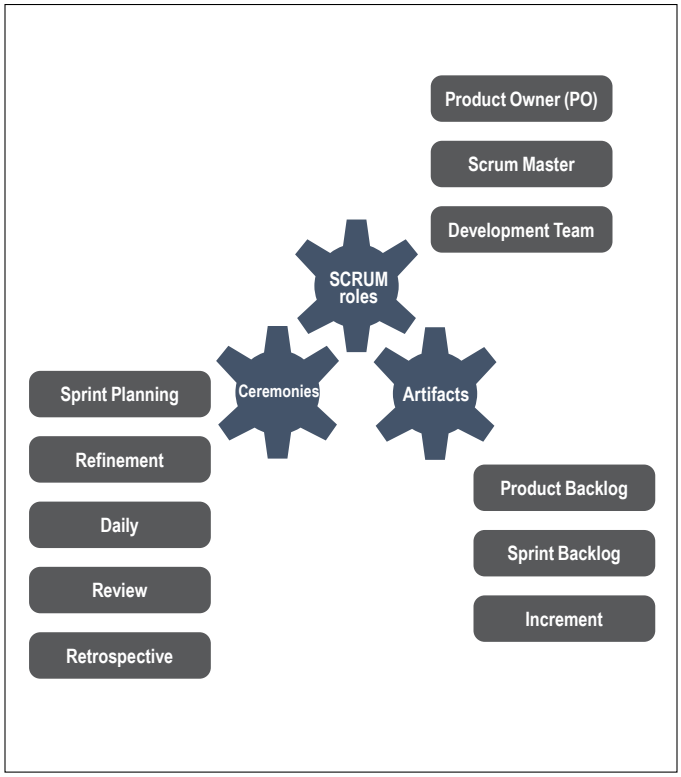


FIGURE 8: Scrum framework roles, ceremonies, and artifacts.

Product Owner: This role is filled by an engineer from the team who manages the data center. She knows the clean room in detail and the equipment installed and has a clear understanding of the services that may be impacted by the project. She approves the product backlog, the sprint backlog, and the sprint review. She is the customer's representative on the project, which, in this case, is the data center manager. The PO is seconded to the team and is almost exclusively dedicated to this initiative. She participates in all ceremonies and represents the client's vision.

Scrum Master: The organization assigns this role to a professional who understands this framework. She ensures that the ceremonies are respected and guides the team in the use of the artifacts. In the April Project, she trains the development team on the methodology, roles, artifacts, and way of working to align the work criteria and ensures that the team is properly focused on the project goals. She is a servant leader and supports team members both in the needs of the project and in understanding if they have organizational or personal issues that may affect their performance on the project. In the daily meetings, she takes note of the obstacles reported by the team members and channels them to the stakeholders with the help of the project manager.

Development Team: In the April Project, these roles are performed by a contractor with experience in clean room installations, who has already performed work with good results, and has experience in performing electromechanical and structured cabling work, so it can be prepared for any risk scenario that may arise. It is necessary for the team to change their working perspective when working with agile practices, as they may have to change their mindset from "waterfall to agile," for which SM training and support are required. In this project, the team is responsible for preparing the clean room plans with the proposal for the installation of the cabinet accessories, carrying out the installation of the accessories, participating in ceremonies, such as the daily meeting, and in the verification of work in the sprint review, among others.

3.3. The Artifacts

The project defines the use of the Scrum framework's artifacts: product backlog, sprint backlog, and increments.

For this project, it was decided to use Microsoft Planner as a collaborative tool, which is part of the Microsoft Office 365 suite. This tool has many advantages, such as integration with Microsoft Teams and, therefore, with groups and internal and external users. It offers integration with Microsoft Outlook for the dissemination of task assignments, task status, and due dates. Microsoft Planner is a tool that allows users to use a Kanban-type board to organize the stories (tasks) of the project.

Product Backlog: Since the scope is to intervene in all the racks, it was decided to group them by sectors (the closest); this criterion may change based on the needs of the project. In this case, it is the most advisable, which is why the stories were oriented toward the objective of implementing a total of eight groups; therefore, the product backlog was approximate, as seen in Figure 9, the development of this artifact. It was held in the Scrum planning ceremony, with the participation of the PO, the SM, and the team; the PM and the TL also participated.

Figure 10 is presented as a reference to illustrate the scope of the project. To illustrate this article, a scope of 80 racks is proposed, where different technological platforms are located, such as mainframe, storage, networking, Windows server, etc. The figure shows 600 mm (≈23.6 in) x 1200 mm (≈47.2 in) cabinets only as an illustration; there are a variety of width and depth dimensions and generic and proprietary racks, such as the mainframe, among others.

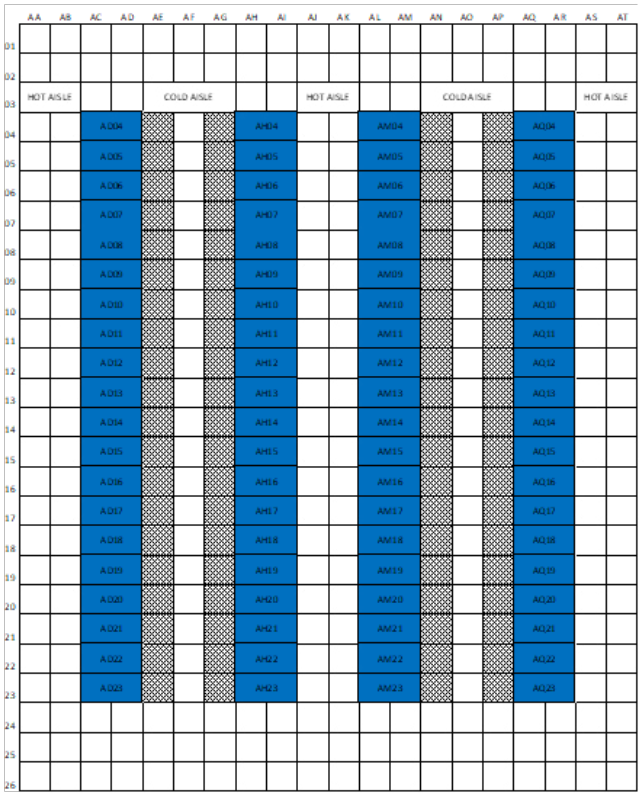


FIGURE 10:
Distribution of the racks in the clean room—April Project.

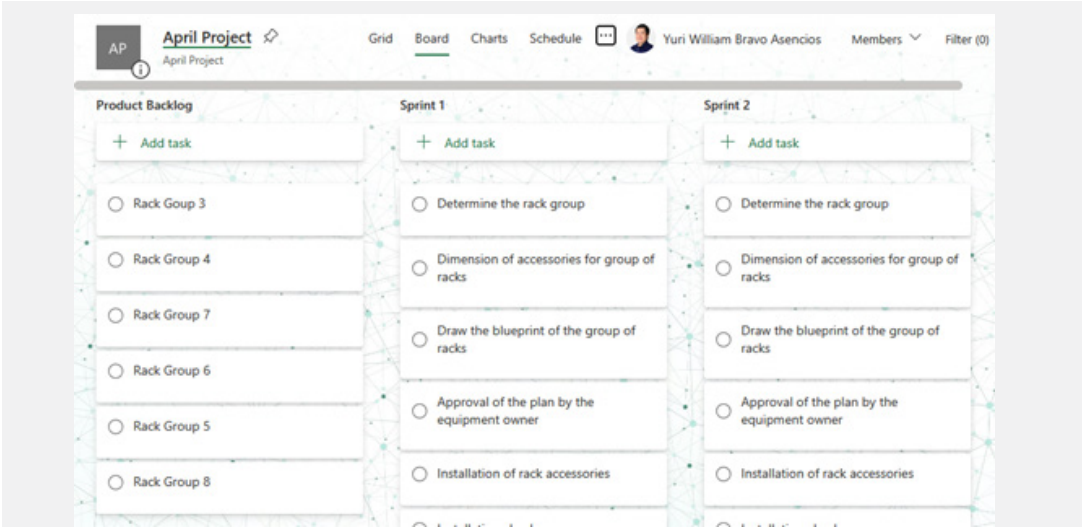


FIGURE 9: Using MS Planner as a Kanban board.

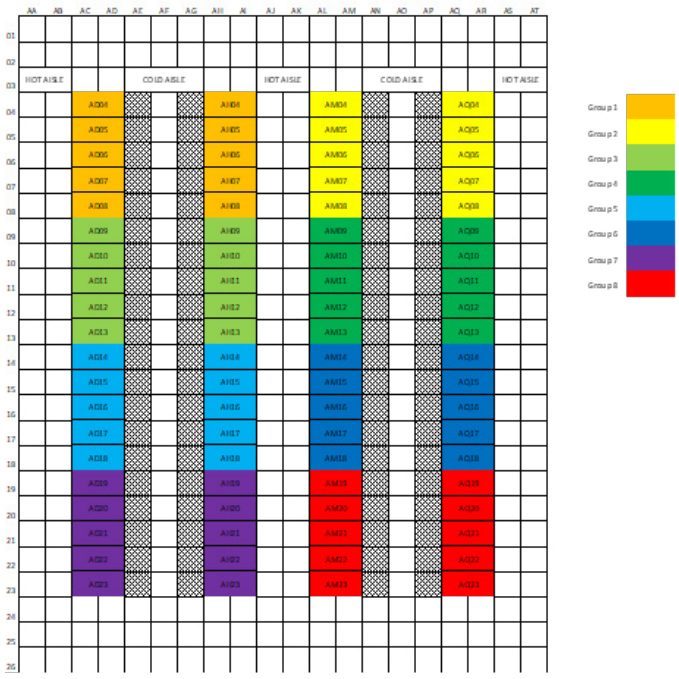


FIGURE 11: Grouping of racks in the white room—April Project.

The racks have been grouped to organize the product backlog, as shown in Figure 11 for reference. This grouping can vary based on the needs of each project, based on topology, services, or other considerations. As can be seen in the figure, each group is addressed in each sprint.

Figure 12 shows a diagram of how user stories are created from epics.[6] In a paper presented at PMI® Global Congress 2011, Michael E. Cottmeyer describes the epics that are associated with a more strategic level of the organization: "The portfolio vision breaks down the organization's strategy into relatively small increments of investment that can be quickly executed, proven, and rolled out to customers on a regular cadence. These investment increments are called epics and live at the top level of the organization's planning process. The portfolio vision enables the organization to understand how these epics will help the organization achieve its broader business goals. It includes information such as expected ROI, key customers, competitive differentiation, market positioning, and competitive alternatives."[6] On user stories: "Once the epics are identified, they are broken down into features that can be delivered by program teams. Program teams take these features through the product delivery lifecycle, breaking them down into user stories that can be delivered by a single team in a single sprint. As teams deliver user stories sprint after sprint, these user stories are rolled up across teams into completed features, which are ultimately rolled up into completed epics that support business goals and can be measured for effectiveness."[6] Although the reference is aimed at large projects associated with portfolios and programs, it allows us to have an idea of how to break down the epics and user stories in the planning ceremonies to determine the stories that should be addressed in each sprint and configure the expected features.

FIGURE 12: Organization of user stories, from epic to sprint. Image Credit: Project Management Institute.[6]

Sprint Backlog: In the sprint planning ceremonies, if the PO prioritizes the user stories or even adds new ones or refines them, that is his prerogative. In the April Project, the stories are associated with the intervention of the racks of each group; for example, in Figure 13, the stories for Sprint 1 associated with group 1 are:

- Dimension of accessories for a group of racks
- Draw the blueprint of the group of racks
- Approval of the plan by the equipment owner
- Installation of rack accessories
- Installation check

Increments: They represent the results of each sprint, which are presented to the PO and UL at the end of the sprint during the sprint review. During this review, the team must present the features achieved in that iteration. For instance, at the end of Sprint 1, the team should show the results of the work in Group 1 (see Figure 13). The PO may approve the results according to the criteria established in the stories. If the results are not approved, they can be moved to Sprint 2. This means that, although each group of racks is planned in each sprint, there could be activities from one sprint transferred to another subsequent sprint. Additionally, some tasks might also be deprioritized.

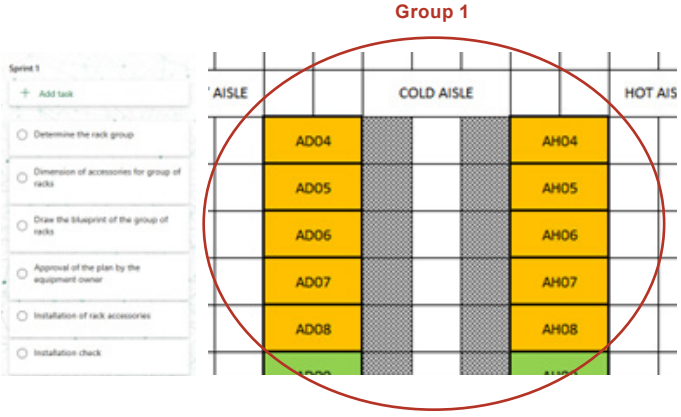


FIGURE 13:
User stories related to Group 1 to be developed in Sprint 1.

3.4. The Ceremonies

Sprint Planning: At the beginning of each sprint, a ceremony is held to plan the user stories to be developed based on the product backlog, and the sprint backlog is built. For example, from the product backlog, the stories that will be developed in Sprint 1 are prioritized, that is, those related to Group 1. In this article, the time box for each ceremony is not referred to since, as mentioned in the beginning, the proposal is to use agile practices with the Scrum framework as a reference. However, it must be adapted to the reality of the infrastructure project, which is different from a software development project. This is why it is necessary to take licenses for each ceremony's duration (time box).

In the April Project, there were some customizations, such as:

- The duration of each sprint was originally set at two weeks. However, because there were more critical teams and intervention approvals required higher levels of approval, they took longer. In addition, there can be, and are, groups of cabinets of greater complexity that require onsite reviews. Some sprints may last two or three weeks.
- In the Scrum framework, daily meetings are held, but in this case, they are scheduled three times a week since this is the only time to evaluate progress and identify obstacles or other issues.
- Due to the risk involved in working in a production environment, activities are scheduled at night, which affects the timing of the various ceremonies. Even the PM's participation was done remotely, for which MS Teams was used.
- The duration of the sprints may be affected by the data center's shutdown periods, periods of the month when some activities cannot be performed.
- It is recommended to conduct a Sprint 0 (Sprint Zero) to carry out a pilot. This pilot will demonstrate the possible scenarios the team may face due to the diversity of rack types and measure the duration of activities in future sprints. This will aid in coordinating with the owners of the equipment and technologies.

Daily Meeting: According to the Scrum framework, it is a daily ceremony in which the whole team participates, usually by looking at the Kanban board (or the MS Planner board), and in which each team member comments on the progress they made the previous day, the activities they will do the current day, and the obstacles they have to move forward. Because this ceremony has to be done quickly (15 minutes), it is also called the daily meeting standup because it is done with everyone standing. As in all agile practices, the team shows a collaborative attitude because if one team member's activities are delayed, they will affect the development of those planned in the sprint.

Sprint Review: The sprint review is the ceremony in which the increment developed in the ending sprint is presented. It is presented by the team and supported in moderation by the SM, and the PO is the one who must give approval. If there is no acceptance, it may result in some activities moving to the next sprint. Otherwise, the results of the sprint will be accepted.

Sprint Retrospective: This ceremony can be reviewed with some analogy to the lessons learned gathering in a traditional project. It focuses on providing a safe space for team members to comment on the work done in the sprint, individual and team accomplishments, mistakes, things that could have been improved, and commitments to improve in subsequent sprints. This ceremony strengthens teamwork and is recommended. Various techniques can be used to conduct a successful retrospective ceremony, such as the timeline retrospective, as described by Anablava Abendroth in the publication "An Easy Guide for Your Next Timeline Retrospective,"[7] where it is explained that the timeline retrospective is made up of three main ingredients (Figure 14):

- Building a shared reality
- Visualizing the emotional journey
- Compilation of future actions and learnings

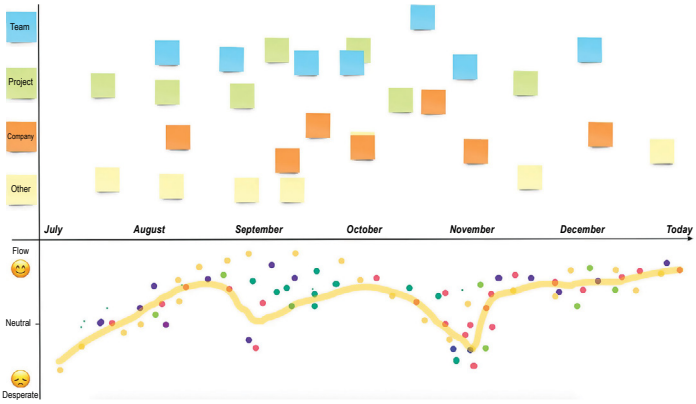


FIGURE 14: Example of use of the timeline retrospective technique. Image Credit: Medium.[7]

3.5. The Three C's Applied to Agility

The Agile Business Consortium, in its publication, "The Nine Principles of Agile Leadership," considers the application of the three C's as key elements for agile leadership: communication, commitment, and collaboration (Figure 15).[8]

The 3 C's	Principle	Guidance
Communication	1	Developing
	2	Reflecting
	3	Learning
Commitment	4	Inspiring
	5	Engaging
	6	Unifying
Collaboration	7	Empowering
	8	Achieving

FIGURE 15: The three C's of agile leadership. Image Credit: Agile Business Consortium.[8]

Taking as reference the principles proposed by the Agile Business Consortium, we propose some recommendations on how to apply the three C's in a case similar to the April Project and obtain successful results:

First C, Communication:

- **Actions speak louder than words:** Leadership in a project must be helpful and lead by example. (The best way to give feedback to the team is on the "battlefield," i.e., in the clean room, not on a cold desk or table far away from the "action.") Likewise, respect for agreements and rules, starting with leaders, is a message that the entire team understands better than empty statements. An individual's behavior is the best communication.

- **Improving the quality of thinking leads to better results:** The best information comes from those who are developing the work, so interacting with the development team in the workplace, where it happens, is important in agile practice problems, and you can get the best ideas for solving them. Then, use ceremonies like daily meetings to listen to the team and their ideas.

- **The team improves through effective feedback:** It is important to give and receive feedback, known as 360-degree feedback. A very useful ceremony for this is the retrospective. Leaders should take advantage of the retrospective, which can be held at the end of each sprint as well as at the end of the project. They should not only give feedback to their team, which is, of course, very important as a leader, but also receive feedback from the team so that they can improve their leadership. By doing so, they may be able to build a high-performing team soon.

Second C, Commitment:

- **People need meaning and purpose for their work to be satisfying.** In agility, team members' commitment is critical, so they must "own" the activities they commit to perform. In planning ceremonies, the same team proposes the tasks to be performed to achieve the goal and the duration of those tasks to complete the characteristics of the deliverable or increment. Likewise, recognition must be given in the retrospective or at the end of the project.

- **Emotion is the basis for enhancing creativity and innovation:** Throughout the project, challenges will arise; it is the leader's task in agility to provide space for each team member to have the opportunity to propose solutions through creativity and innovation. Agility is open to change, and to face it, it is better to involve the team with a horizontal organization, not a vertical one.

- **Leadership lives in all parts of the team:** In previous lines, it was mentioned that agile practices could be used for data center projects, citing the good results observed in practice. It is important to understand that agility, in a broader sense, is not just about practices; it is a mindset. It is about being open and knowing how to manage change, working as a team, and being a leader. It is important to empower the team, making the value of each person and their contribution to the team visible. It is imperative to build high-performance teams and train agile leaders for future projects.

Third C, Cooperation:

- **Leaders Delegate:** Delegation should be seen as a way of taking over the activities or tasks of the team and working with the PO to complete the task in the time allotted. This can be applied in planning ceremonies and retrospectives.

- **The Group Collaborates:** In an IT infrastructure project, and even more so in a data center, it is important to have a team made up of the best; the high risk of working in the clean room, near the servers, and other technology equipment has already been mentioned. Therefore, the equipment must be top-

of-the-line, and there must be strict compliance with data center policies and procedures (SOPs, MOPs, EOPs). This is why it is important to build a team that will work on agility; it must be a team that works together and understands that each colleague's success is the success of the team.

- **Great Ideas Can Come from Any Part of the Team:** You should take advantage of the various celebrations to ask for new ideas for the challenges that may arise, such as an unexpected risk or the need to reduce time, among others. Since the team is made up of professionals or technicians with experience in their field of work, they can contribute innovative ideas to move forward.

4. CONCLUSIONS:

- The case presented corresponds to the execution phase of a project in a Class F3 data center, according to the ANSI/BICSI 002-2024 standard,[1] focused on the clean room, where the feasibility of applying agile practices based on the Scrum framework is being evaluated.

- Reference is made to the Uptime Institute study, "Annual Outage Analysis 2024",[2] which shows the risk of interventions in a data center in production and the importance of adequate human factor management to reduce incidents that may cause interruptions or service outages. Therefore, this article suggests that an iterative approach should be used, with constant feedback from the user who may be affected and at short intervals to avoid possible major impacts.

- To apply agile practices, it is recommended to first perform an analysis to define the most appropriate approach for the project, taking into account the organizational culture, the team's knowledge of agility, the uncertainty that may exist in time and scope, the need for customer involvement, among others. Then, if the decision to apply agility is made, it is recommended to use the Scrum framework, with the formation of a team, the use of artifacts, and the performance of ceremonies.

"It can be concluded that implementing agile practices through the Scrum framework in a data center project is feasible."

- At some stages of the project, it may also be possible to use agile and waterfall practices in parallel; this is known as a hybrid approach.

- In the case of the April project, agile practices were chosen, and excellent results were achieved. Some considerations of the Scrum framework had to be adapted, such as the duration of sprints, the duration of ceremonies, such as the daily meeting, the work schedule at night, and the freezing periods when work could not be done in the clean room, etc. In this way, the goal was achieved in the planned time, without any technological incidents or service interruptions.

- One of the most important considerations when applying agile practices to this type of project is the need for user involvement, since only the user knows the impact of an interruption, the best time to make a change, and the windows of work. Since this can lead to rescheduling, it helps to have a high level of user involvement and frequent communication.

- It can be concluded that implementing agile practices through the Scrum framework in a data center project is feasible. This approach ensures strict compliance with operations and maintenance policies and procedures while taking advantage of an approach that delivers results more quickly and adds greater value to the organization. In addition, the incremental outcomes at the end of each iteration foster team engagement and enhance performance through continuous practice.

AUTHOR BIOGRAPHY:

Yuri Bravo is an electronic engineer with a master's degree in strategic management in information technology and a master's degree in administration and project management. He has more than 25 years of experience in information technology and communications projects, of which he has worked for the last 14 years in the Data Center Administration Unit of Banco de Crédito del Perú, which is the largest financial institution in Peru. He has the DCDC and RTPM certifications from BICSI, ATP, ASA, and ATS from Uptime Institute, PMP from PMI, among others, and he has been a professor for more than 20 years, teaching at the Universidad Peruana de Ciencias Aplicadas (Peruvian University of Applied Sciences) and INICTEL-UNI. He has been a BICSI volunteer for more than 10 years and is currently secretary of BICSI-CALA; he also participates in the Technical Committees for Standardization of Data Centers and Telecommunications. He can be reached at yuri.bravo@it-class.net.

WORKS CITED:

1. ANSI/BICSI 002-2014, Data Center Design and Implementation Best Practices.

2. "Annual Outage Analysis 2024." *Uptime Institute*.

3. "The Standard for Risk Management in Portfolios, Programs, and Projects." *PMI*.

4. Essentials of Data Center Projects. 2nd ed., *BICSI*, 2024.

5. Bravo, Yuri and Sandra Elizabeth Rosales Coronel. "Is it Possible to Use Agility in a Data Center Project?" *ICT Today,* vol. 44, no. 3, 2023, pp. 30–42.

6. Cottmeyer, M. E. (2011). "Large-scale program and portfolio management with Scrum and Kanban." Paper presented at PMI® Global Congress 2011—North America, Dallas, TX. Newtown Square, PA: Project Management Institute.

7. Abendroth, Anablava. "An Easy Guide for Your Next Timeline Retrospective," *Medium,* 15 January 2021, https://anablava.medium.com/a-timeline-retrospective-easy-guide-6385fce0affd.

8. "The Nine Principles of Agile Leadership," *Agile Business Consortium Limited,* 2024, www.agilebusiness.org/resource/the-nine-principles-of-agile-leadership.html.

WORKS CONSULTED:

1. *Agile Practice Guide*, PMI, 2017.

Bicsi

ICT Certification Institute

ADVANCING THE ICT PROFESSION

PLAN YOUR PATH TO THE RCDD®

ICT Cabling Installation

Education
- IN101

Education
- IN225

Education
- IN250
- IN251

Education
- TE350

Publication: *ITSIMM*

Education
- Foundations of Telecommunications Distribution Design (DD115)
- Applied Intelligent Building Design (DD215)

Publication: *TDMM*

- RCDD® Test Prep
- RCDD Online Study Group
- Bonding & Grounding vILT

Additional Recommended Reading:
- ANSI/BICSI 006: *Distributed Antenna System (DAS) Design and Implementation Best Practices*
- ANSI/BICSI 007: *Information Communication Technology Design and Implementation Practices for Intelligent Buildings and Premises*
- ANSI/BICSI 008: *Wireless Local Area Network (WLAN) Systems Design and Implementation Best Practices*
- *Essentials of ICT Bonding and Grounding*

Education
- PM101
- PM102
- RTPM® Study Aid
- EVM vILT
- Communication vILT
- PM103

Publication: *TPMRM*

Design and Project Management

Education
- DC101
- DC102
- DCDC® Test Prep

Publication:
- ANSI/BICSI-002
- *Essentials of Data Center Projects*

Education
- OSP101
- OSP102
- OSPDRM vILT
- Fiber to the X vILT

Publication: *OSPDRM*

www.bicsi.org/certification

STRUCTURED CABLING TWISTED PAIR SHIELDING: WHAT IS BEST?

By Gautier Humbert

On the market today, cables for structured cabling exist in various unshielded and shielded types. Customers often ask which are compliant and which are the best for their network.

Based on the international standards ISO/IEC 11801 series, this article clarifies the theory of noise immunity of the pair, the types of shielding, and the concept of segregation to finally define what is standard compliant and what offers improved performance. It also explains what that performance is and the possible benefits.

HOW TWISTED PAIR WORKS

The communication of a symmetrical signal on a twisted pair was designed to limit the influence of outside noise. In a perfect world, the noise is the same on both wires of the pair. See Figure 1 below:

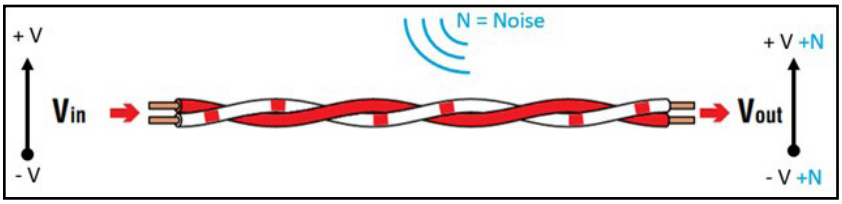


FIGURE 1: Noise affects both wires of a twisted pair equally.

The signal sent is +V – (-V) = 2V.
The signal received, with additional noise, is (+V+ (N)) – ((-V+ (N)) = 2V.
The noise cancels out.

Unfortunately, nothing is perfect, and the symmetry of the noise signal depends on the quality of the pair twist. A cable with a "good" twist and without a shield can be standard compliant for all categories from 5e to 6A. A shield can then be used in the following cases:

- To provide additional protection from electromagnetic interference (EMI).
- To compensate for a lower-quality pair twist.

Based on this theory, it is impossible to assume which type of shield is best. For example, a Category 6A unshielded cable generally has better EMI immunity than a Category 5e shielded cable. It is necessary to look at the standards for actual values and requirements.

THE STANDARDS

The international standard for structured cabling is the ISO/IEC 11801 series. It includes performance and design in the 11801-x standards and the planning and installation in the 14763-2. Below is a diagram showing the relationships between the documents in the series (Figure 2).

For instance, when designing offices, one must comply with the general requirements of ISO/IEC 11801-1, followed by the premise-specific design outlined in ISO/IEC 11801-2. One will also need to plan and install according to ISO/IEC 14763-2, which covers the following:

- Specifying the project
- Planning of the project
- Installation practices
- Documentation and administration
- Testing
- Inspection
- Operation
- Maintenance
- Repairs

Each step includes aspects such as:

- The quality plan
- Pathways and spaces
- Installation methods
- Respect to the mechanical properties of the cables, including bend radius, pulling tension, and Power over Ethernet (PoE) heating
- Separation between power and data for EMI purposes

The document also covers the separation between power and data for the safety of the technicians in some specific cases of outside plant cabling.

The project should then also comply with the telecommunications bonding requirements in ISO/IEC 30129, and finally, testing should be done according to IEC 61935-1 and ISO/IEC 14763-3.

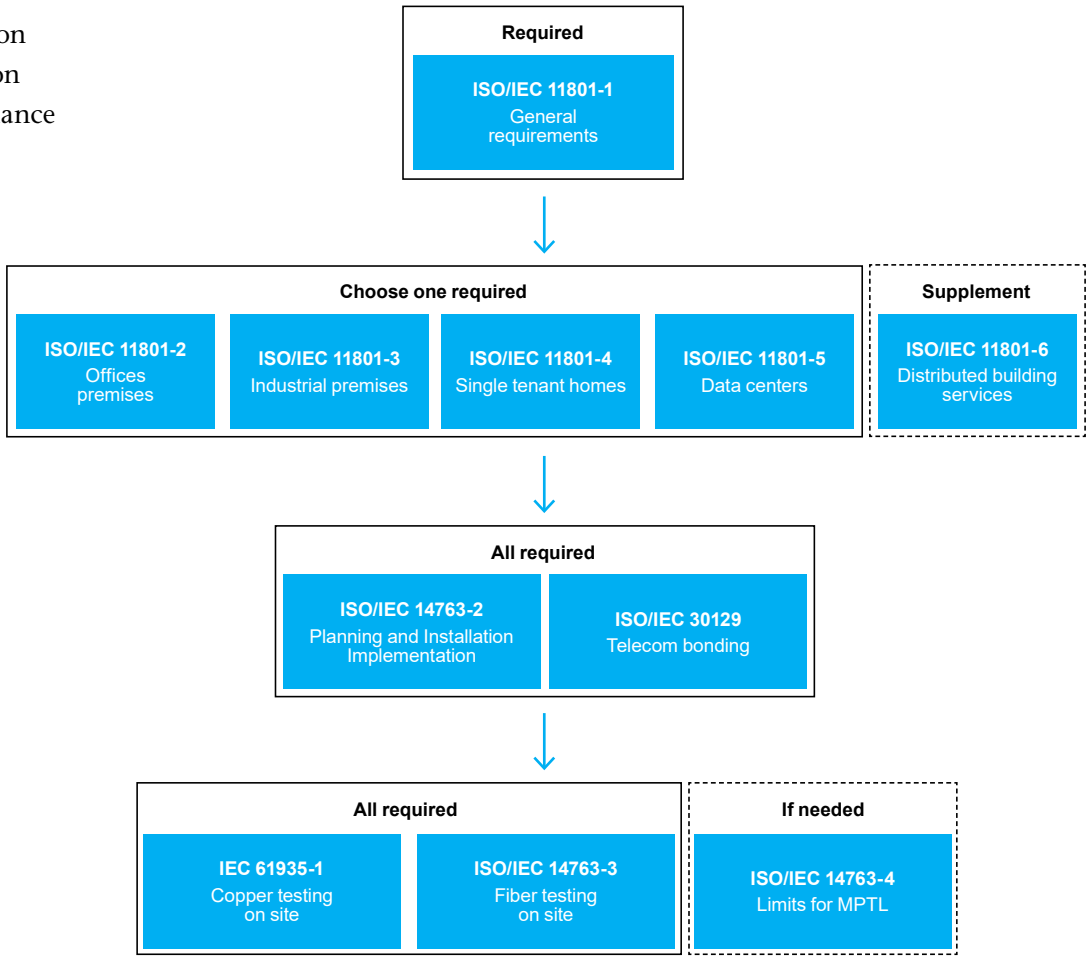


FIGURE 2: ISO/IEC 11801 series: relationships between standards.

TYPES OF SHIELDING

The terminology of shielding can now be clarified. This is defined in the annex D of ISO/IEC 11801-1: 2017. The twisted pair cable can generally have:

- Two locations of shields: around each individual pair and around the combined four pairs
- Two types of shielding material: aluminum or braided wire

A naming is defined to cover all the combinations, as shown in Figure 3 below.

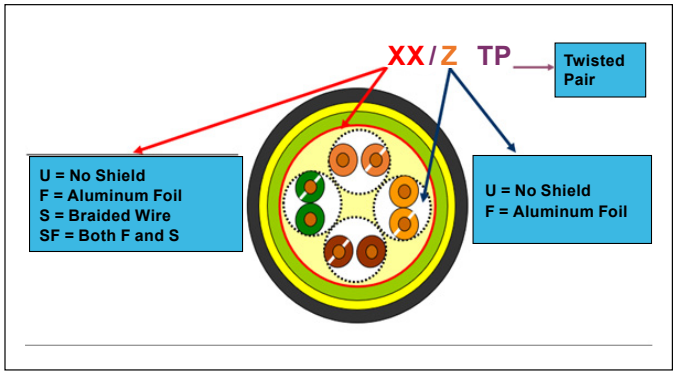


FIGURE 3: Shield Terminology.

For example, a F/UTP cable has only an overall shield but no individual shields around each pair. In contrast, a U/FTP cable has no overall shield and only individual shields around each pair. A U/UTP cable has no shield at all.

Now, the performance of cables in terms of EMI can be examined.

SEGREGATION

The first information is the separation between metallic communications cabling and specific EMI sources found in Table 10 of ISO/IEC 14763-2: 2019, as shown below (Figure 4):

Source of Disturbance	Minimum Separation (mm)
Fluorescent Lamps	130 (≈5.12 in)
Neon Lamps	130 (≈5.12 in)
Mercury Vapor Lamps	130 (≈5.12 in)
High-Intensity Discharge Lamps	130 (≈5.12 in)
Arc Welders	800 (≈31.5 in)
Frequency Induction Heating	1000 (≈39.37 in)

FIGURE 4: Separation requirements between metallic telecommunications cabling and specific EMI sources.

It can be noted that, in this case, the shielding type is irrelevant. The distances are strictly identical for all metallic communications cabling.

To find differences, one must look at the tables concerning the separation of metallic communications cabling and the power supply cables. This is called segregation[1] (Figure 5).

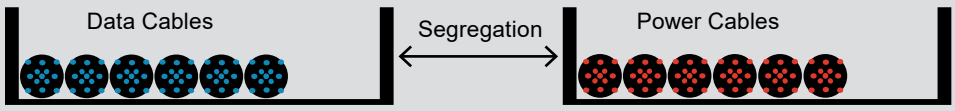


FIGURE 5: Segregation of power and data.

FOOTNOTES:

1. The segregation tables in the ISO/IEC 14763-2 concern installations where one cabling is located in a metal containment, and the other cabling is not. For calculations when both data and power cabling are located in separate metallic containment, see EN TS 60659.

At this point, it is important to be reminded that this segregation concerns only EMI issues and is limited to low-voltage power supplies. The separation of power and data for safety reasons (risk of electrical shock) is a different topic.

SEGREGATION CLASSES

The process of determining the segregation distance is found in Figure 11 of the ISO/IEC 14763-2: 2019 standard and involves the following elements:

- Segregation class of the communications cables
- Type of containment used
- Number of power supply circuits (based on each circuit being 20Amp)

There are four segregation classes, and they apply the following way to twisted pair cables:

- The Class "a" is reserved for cables not compliant with the standards[2], such as Category 3 cables.
- All standard compliant unshielded cables meet minimum Class "b."
- All standard compliant shielded cables meet minimum Class "c."
- The Class "d" is for cables with improved EMI protection. Although not required in the international standard, Category 7 and 7_A cables generally meet this class.

The table below summarizes the segregation class requirements (Figure 6).

As a note, the North American ANSI/TIA 568 series does not recognize various segregation classes. These documents have a black-and-white compliance aspect, so in this regard, having a "better" or "worse" shield has no influence on the installation requirements.

Segregation Class	a	b	c	d
Non-Compliant	Minimum	Possible	Possible	Possible
Unshielded	Not Allowed	Minimum	Possible	Possible
Shielded	Not Allowed	Not Allowed	Minimum	Possible

FIGURE 6: Segregation classes according to the twisted pair cable type.

FOOTNOTES:

2. The term "standards" in this section refers to IEC 61156-5 and IEC 61156-6. These correspond to horizontal cables allowed in ISO/IEC 11801-1.

SEGREGATION DISTANCES

In Table 12 of ISO/IEC 14763-2: 2019, the minimum separation is zero for solid metallic containment. However, this concerns only steel conduits of 1.5 mm (≈.06 in) minimum or equivalent thickness. It is not applicable for solid metallic cable trays of thinner thickness.

So, let us consider examples with Classes "b," "c," and "d," used in typical cable trays of either perforated metallic or open metallic (wire mesh). By applying the power cabling factors of Table 13 of the standard to the minimum separation of Table 12, we obtain the following values (Figure 7):

Segregation Class	b		c		d	
Number of 20A Circuits	Open	Perforated	Open	Perforated	Open	Perforated
1 to 3	15 mm (≈.59 in)	10 mm (≈.39 in)	8 mm (≈.31 in)	5 mm (≈.2 in)	2 mm (≈.08 in)	1 mm (≈.04 in)
4 to 6	30 mm (≈1.18 in)	20 mm (≈.79 in)	15 mm (≈.59 in)	10 mm (≈.39 in)	3 mm (≈.12 in)	2 mm (≈.08 in)
7 to 9	45 mm (≈1.77 in)	30 mm (≈1.18 in)	23 mm (≈.91 in)	15 mm (≈.59 in)	5 mm (≈.2 in)	3 mm (≈.12 in)
10 to 12	60 mm (≈2.36 in)	40 mm (≈1.57 in)	30 mm (1.18 in)	20 mm (≈.79 in)	6 mm (≈.24 in)	4 mm (≈.16 in)
13 to 15	75 mm (≈2.95 in)	50 mm (≈1.97 in)	38 mm (≈1.5 in)	25 mm (≈.98 in)	8 mm (≈.31 in)	5 mm (≈.2 in)
16 to 30	150 mm (≈5.91 in)	100 mm (≈3.94 in)	76 mm (≈2.99 in)	50 mm (≈1.97 in)	16 mm (≈.63 in)	10 mm (≈.39 in)
31 to 45	225 mm (≈8.86 in)	150 mm (≈5.91 in)	114 mm (≈4.49 in)	75 mm (≈2.95 in)	24 mm (≈.94 in)	15 mm (≈.59 in)
46 to 60	300 mm (≈11.81 in)	200 mm (≈7.87 in)	152 mm (≈5.98 in)	100 mm (≈3.94 in)	32 mm (≈1.26 in)	20 mm (≈.79 in)
61 to 75	375 mm (≈14.76 in)	250 mm (≈9.84 in)	190 mm (≈7.48 in)	125 mm (≈4.92 in)	40 mm (≈1.57 in)	25 mm (≈.98 in)
> 75	450 mm (≈17.72 in)	300 mm (≈11.81 in)	228 mm (≈8.98 in)	150 mm (≈5.91 in)	48 mm (≈1.89 in)	30 mm (≈1.18 in)

FIGURE 7: Minimum segregation separation according to the segregation class of the twisted pair cables.

In a case with 13 to 15 power supply circuits in perforated cable trays, unshielded cables require 50 mm (≈1.97 in) segregation, and shielded cables require 25 mm (≈.98 in), while improved shielded "d" cables require only 5 mm (≈.2 in). If both types of cabling are each in metal containment, these distances are further reduced. While it is true that a shielded cable of segregation Class "d" does offer a significant improvement over the

minimum requirement when only looking at numbers, it is important to recognize that these values are in millimeters and, therefore, roughly the thickness of the sides of the cable trays (Figure 8).

Power and data cable trays are typically separated by at least 200 mm (≈7.87 in), but the designer needs to ensure that this is the case. It should also be considered that cable management systems are generally designed independent of types of cables rather than for cables of specific segregation classes, which would limit their flexibility in the future.

EXCEPTIONS

It should be noted that there are some exceptions[3] to these calculations. For example, zero separation is allowed for all standard-compliant twisted pair cables when the power supply conductors comprising a circuit are either:

- Within an overall sheath and provide a total current no greater than 100 A, or
- Twisted, taped, or bundled together, providing a total power no greater than 32 A.

The intent of this exception is to allow power and data to share containment to the outlet. Once again, this is irrelevant to segregation class.

ENVIRONMENTAL IMPACT

The search for higher EMI immunity generally involves using thicker shields with additional braided wire, and the environmental impact should not be forgotten.

The chart below shows the comparison, using the F/UTP as the base of 100 percent[4] (Figure 9).

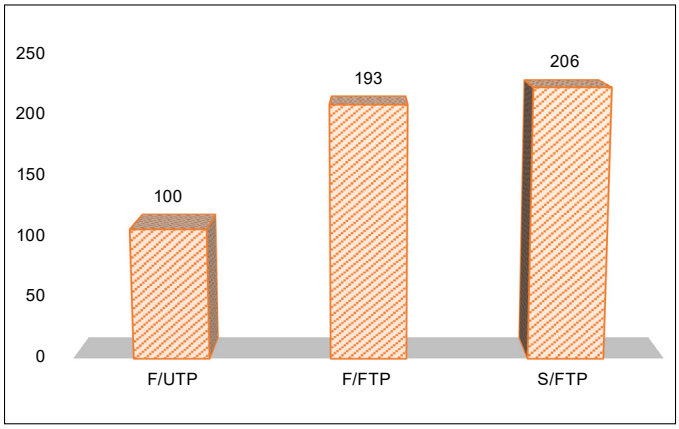


FIGURE 9: Comparison of the weight of the metal composing the shield of various cables.

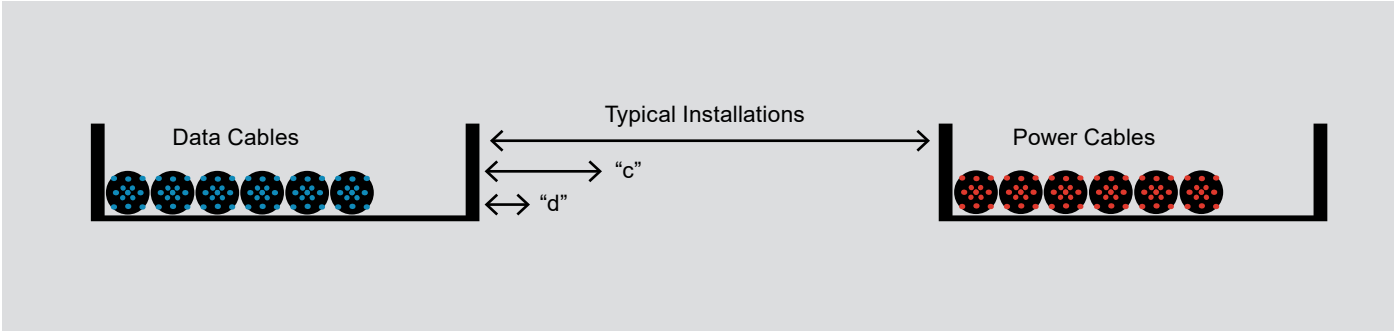


FIGURE 8: Comparison of typical segregation and allowed segregation "c" and "d."

FOOTNOTES:

3. Additional conditions apply, such as regulations and environmental space respecting classification E1 of ISO/IEC 11801-1.
4. Based on actual measurements of cable shield samples. F/UTP was 100 percent. F/FTP was 193 percent. S/FTP was 206 percent. Drain wires were included in the measurements.

Compared to the F/UTP, the F/FTP requires 90 percent more metal in the shield, and the S/FTP requires double.

Using more metal increases the immediate use of resources, but also the carbon impact of shipping heavier cables, and finally, the oversized cable management.

CONCLUSION

The type of shield is not relevant to specifying higher EMI protection. In fact, depending on the quality of the pair twists, a cable without a shield could be better than a shielded one.

The parameter used to evaluate the EMI immunity of a cable is the segregation class, and shielded cables of Class "d" have better immunity than cables of Class "c." However, in typical projects, the improvement provided does not translate into benefits.

On the other hand, cables with thicker shielding use more raw material and, therefore, have a greater negative impact on the environment.

Customers should balance wisely the relatively small benefits of cables with improved segregation with the negative impact on the environment and reserve those cables for specific uses.

AUTHOR BIOGRAPHY:

Gautier Humbert, RCDD, has been in the industry for more than 20 years, with experience throughout the world. He is currently the standards coordinator for digital infrastructures and participates in multiple international and European committees. In particular, he is on the ISO/IEC JTC 1 SC25 WG3 group responsible for the 11801 series and is the current chair of the CENELEC TC215 WG2 group responsible for the European installation standards. He received the BICSI European Member of the Year Award in 2012 and the BICSI Global Member of the Year Award in 2020. He has also been the BICSI EMEA region director from 2021 to 2023.


Registered Communications
Bicsi
CERTIFIED
RCDD
Distribution Designer
The redesigned
RCDD® Program
is here!
NEW
Course
Manual
Exam
Bicsi

COLOCATION—NOT JUST FOR DATA CENTERS

By Justin W. Hobbs, RCDD, TECH, C.M., ACE

INTRODUCTION

Colocation is a normative technology industry term typically used to describe a type of data center environment. The Merriam-Webster dictionary defines colocation as "to locate [two or more things] together or be located together" and "to place [two or more units] close together so as to share common facilities."[1] This type of functionality has been widely accepted to allow common physical infrastructure (i.e., space, electricity, cooling) to be shared among multiple tenants or users in a singular area with the intent of providing a service to the tenant (and their downstream customers) and a revenue stream (to the owner and operator) to maximize space and service offerings and lower the overall total cost of ownership of a facility.

In another article, the concept of the "Imperative Trinity," or the most important considerations for the design of telecommunications infrastructure, was explained. Space to house equipment, electrical infrastructure, and communications pathways all play an important role in colocation if that is the desired and accepted business case of the owner. Likewise, these same core considerations are equally important when the desire is for a collocated environment as they extend to all tenants and occupants of the infrastructure: current, proposed, or otherwise.

Now, to expand on that previous work, scenarios will be offered and explained on how they work together to satisfy the Imperative Trinity and offer efficiencies within the colocation concept.

COLOCATION IS NOT A NEW CONCEPT BUT RATHER A CHANGING ONE

The concept of colocation is certainly not new. Colocation has been around for some time—just used in different forms and fashions. Consider a hotel or an apartment

building, a common building sharing common infrastructure for the sole purpose of housing people. Lots of people, for that matter. Consider a shopping mall, a common structural complex sharing common infrastructure for the sole purpose of providing marketing, retail, and other commodities to the public. Consider a medium to large airport, a common building or collection of buildings sharing common infrastructure for the sole purpose of getting a person on an airplane to their destination and subsequently back to their point of origin.

Consider a city. How does it serve the multitude of people who live there? How does its governance dictate how space and infrastructure are used? How does it provide for electrical services? Water services? Sanitation services? Transportation services and other services? The simple and vague answer is that it tries to maximize what infrastructure is available to it under the auspices that the *many* can be serviced by the *few and available*. Again, it is the concept of maximizing one's resources. In a city's case, however, the need to grow and expand is ever-present, so careful and prudent planning is key.

Translating this concept to the technology world is not that different or difficult. In fact, machine virtualization is a form of colocation and can trace its roots to IBM circa the 1960s[2] (Figure 1).

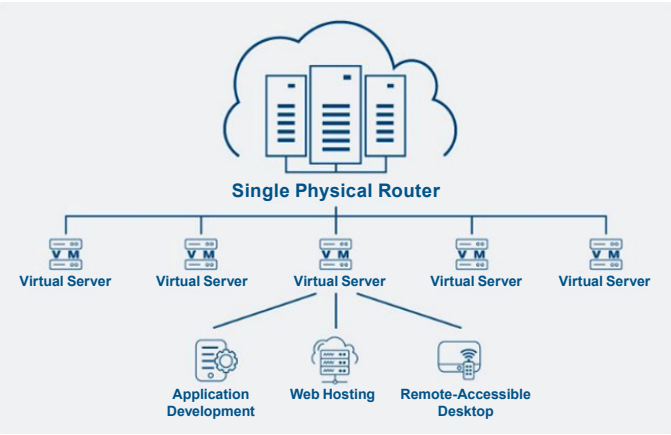


FIGURE 1: Logical VM hardware. Image Credit: FS.com

Passive optical networking is a form of end-user/end-device colocation that shares common core equipment and physical media. We see this technology becoming more and more prevalent as more single-family dwellings and multi-family dwellings are being built because of urban sprawl. Even network engineers are familiar with various forms of colocation with the IEEE 802.1Q Standard (and its addenda) of Virtual Local Area Networking or variants thereof in the routing world, a.k.a. virtual routing and forwarding, or VRF (Figure 2). Many similarities can be found within the wide world, but for the purposes of this article, the focus will remain on physical infrastructure and types of industries where physical infrastructure can benefit from colocation.

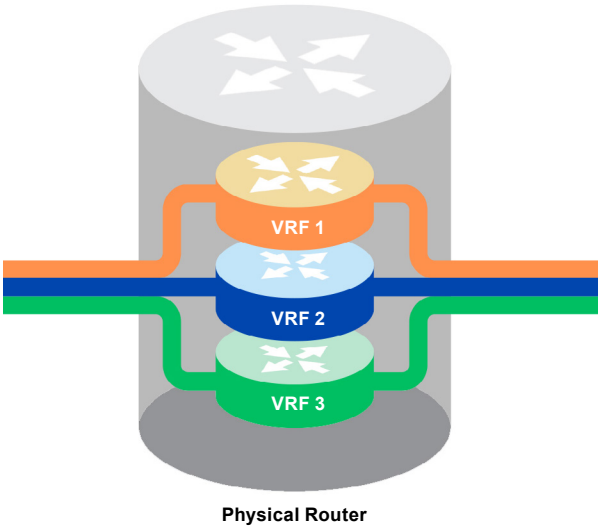


FIGURE 2: VRF. Image Credit: Baeldung.com

As previously mentioned, the concept of colocation is not new. The manner in which it is implemented and deployed continues to influence the world depending on what its purpose is and how it is used. The overarching goal of colocation is to maximize the utilization of available resources to maximize operating efficiencies, occupants, revenues, and many other factors depending on its application. This, in turn, minimizes long-term costs and frustrations with upfits, thus serving the owner and client base better. In short, it is just good business to do it.

THE OUTSIDE PLANT

The outside plant is a common way to collocate spaces and pathways for communications. That represents two of the three entities of the Trinity already established. The basis for colocation in the outside plant is well documented. Telecom service providers have been installing more and more pathways and infrastructure along highways, in neighborhoods, and even at the bottom of oceans for many decades. Oftentimes, one internet service provider (ISP), will lease a certain amount of pathway from an existing provider when the cost-to-benefit ratio is more favorable as opposed to the cost and time associated with constructing a separate pathway. Sometimes, they lease optical fiber outright in a broadband wholesale structure. This, in turn, *purportedly* leads to a lower cost for the end user. The problem is that most ISPs do not work well with one another and compete vehemently against each other whenever the opportunity arises ... as they are wanton to do. When it comes to telecommunications infrastructure at Layer 1, the "turf war" can get quite fierce in the unseen battleground beneath the grass (Figure 3). Likewise, questions can be posed: Have you ever driven down your usual roadway and glanced up at the wooden poles that line the sides? Have you considered the multitudes of strands elegantly touching each one as they stream their way to an obscure destination? Some are quite barren. Others, more heavily laden. This, too, is a battleground for space as pole attachments are also a way to "lease" space for colocation.

FIGURE 3: Congested OSP. Image Credit: JWG.org

With the continued adoption of fabric mesh inner ducts and the increasing popularity of micro duct solutions, the ability to maximize the use of underground pathways is on the rise while lessening the risk of inadvertent damage to others' infrastructure. The cost to install underground infrastructure can vary, which is why the colocation model works well in this situation. It should be common knowledge to many in the industry that the cost to open the ground to install new pathways only becomes more expensive as time goes on, so allowing for additional capacity and even the opportunity for leasing revenue is just good business.

As such, the ability to improve on traditional methods is ripe for harvest. Now, with Class 4 Power Limited and Fault-Managed Power (as defined and described in the 2023 version of the NEC, Article 722 and 726), it too can be installed within the same pathways and spaces as other Class 2, Class 3, and communications circuits (see NEC Article 726). Here is the third entity of the Trinity. And remember, maximum flexibility comes from the satisfaction of all three entities.

Imagine an environment where remote cameras are necessary. What about access control technologies? Traffic monitoring? Environmental sensors where low band 5G might not reach effectively? (However unlikely, but plausible.) Perhaps passive optical networking (PON) and passive optical LAN (POL) technologies would benefit in non-traditional ways from the use of Class 4 power along with optical fiber technology. In some cases, they already have. Think of how the technology environment could benefit from the bandwidth and reach of optical fiber married with the reach and capabilities of digital Class 4 power. One specific scenario, albeit a bit narrow in scope, involved the city of Charlotte, North Carolina, which legally owns and (arguably) operates the Charlotte-Douglas International Airport (CLT). In this scenario, a continuous struggle was encountered with the remote airfield access gates, particularly in terms of serving them efficiently with both power and communications. Since the technology group there was under the jurisdiction of the "city," conflicts on ideology and methodology often arose. Specifically, the use of wireless point-to-point or point-to-multipoint systems was mostly

prohibited. Some temporary installations were allowed with the intent to budget and construct physical infrastructure in the future. In short, those with no hint or clue as to how an airport worked were given governance on what was permissible. If someone finds themselves in a similar situation, a possible solution could be to colocate their existing or future infrastructure with an NEC Class 4 power solution and optical fiber to see if there is an improvement. Many manufacturers offer solutions for both cabling and equipment to satisfy this need (Figure 4).

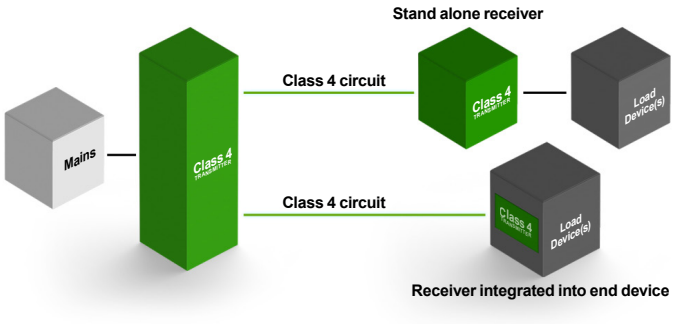


FIGURE 4: Class 4 system diagram. Image Credit: Voltserver.com

Speaking of wireless technologies. Yes, absolutely. The ability to remotely power a wireless repeater or access point without having to engage the electrical service provider and go through the rigors of installing a separate meter and panel for a single circuit or two is cause for consideration. During travels down the nation's interstate systems, one constantly sees the shiny, stainless steel network control cabinets situated on the side of the road, accompanied by various wireless nodes powered by that unmistakable electrical meter at its base. This observation underscores the potential to reduce the quantity of meters and generators while increasing the use of the infrastructure already in place. Such an approach would aim to serve the current installations more effectively and efficiently while also accommodating future installations. Wireless technologies have certainly matured in a wonderful way and deserve a chance to play an integral part in the whole of the technology ecosystem for all environments.

Given the importance of outdoor pathways and spaces to reliably connect sites, sensors, buildings, and essentially the world, it should be highly considered during the design process to overbuild one's capacity where possible, even if only a little bit. Adding even a half-inch to the trade size of a conduit can have lasting positive effects. Remember, it is always more expensive to open the ground later than now. If one must do it, then consider the ability to collocate infrastructure available now and whatever the illustrious industry devises in the next several decades. Otherwise, one will be like a certain service provider recently observed installing additional optical fiber cabling in an occupied right of way. They already had some pathway there, but seemingly not enough. A veritable mass of workers was busy potholing every 25 feet with shovels for approximately 2 miles. Some were busy with pneumatic jacks pushing their way between each said pothole—more than 40 workers at one time. The build took three weeks. All for one cable that could have easily been installed in an existing duct. One can do the theoretical math on that one.

THE CAMPUS ENVIRONMENT—AIRPORTS

As a matter of professional opinion, the campus environment has the greatest advantage of leveraging a collocated physical infrastructure. Insomuch where multiple outside vendors are present, such as an airport, a large shopping mall, a racetrack, a hospital, or any other large venue with similarities. Not so much when few or any outside vendors are present, which may include a college campus, data center campus (depending on the number of customers), or other similarly configured campus. This is the type of environment that stands to either gain or lose significantly in the planning and design of physical infrastructure systems for colocation.

The best way to convey this concept is the well-established cost versus price conversation. And yes, the two terms are NOT equal (Figure 5). "Price" is the monetary amount one would pay for a particular item, overall bid, and/or service. Many times, the price is scrutinized heavily to meet a budgetary number or goal. Many times, however, the price is what dictates what stays within the scope and what is removed.

Many times, physical infrastructure for technology is overlooked or underrepresented. Sometimes, it is outright ignored simply because, in the overall price for whatever, technology typically accounts for a small percentage of the overall construction budget. "Cost" is the amount of effort, money, and other resources the end user or owner must invest over time to keep what has been given in operation. This is commonly known as the "total cost of ownership." Seeing as some physical infrastructure is supposed to last the lifespan of the building, that cost can be great and challenging to quantify upfront, but the cost of not having it can be painfully obvious.

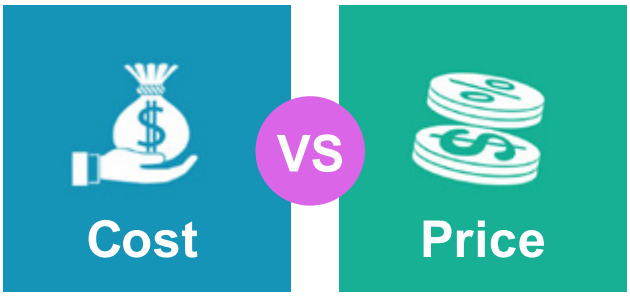


FIGURE 5: Cost versus price. Image Credit: educba.com

It is worthwhile to be forward thinking. Do not kick the can down the road for someone else to deal with it. The argument of "technology is getting smaller and smaller" is countered by this premise. Yes, but there is more and more of it. And with the current times and projections, there will continue to be more of it. The other argument of "Why do you need this much space?" is also countered by the premise that space equals flexibility. Without space, those in technology have no room to bring the wonderful things to life that make buildings and campuses more functional, useful, efficient, and appealing to the masses.

For the sake of this discussion, an airport setting will be addressed.

Airports are wild and weird creatures. There is a saying specific to the industry that "when you've seen one airport ... you've seen one airport." This means colloquially that each airport can be drastically different from another in the way they govern their physical network infrastructure ... or any system for that matter. Some of the larger airports are like cities unto themselves. Airports carry the possibility to be some of the best innovation breeding grounds for technology simply because of the enormous variety of challenges, systems, governance, philosophies, means, and methods present to achieve a simple goal: get a person into the facility and onto an airplane, receive a person and help them get to their destination, or simply transfer a person from one airplane to another.

Space is a premium. It always is no matter if it is new construction or retrofit. Particularly so in an aging airport. Quick note: airports are constantly behind the curve when it comes to construction. Unfortunately, little can be done to improve that aspect.

In an airport, there are many levels of operation. Some have more than others, but generically speaking, there are some that transcend across the globe. The ticketing/boarding level, or the level where origination passengers come into the terminal to check-in and go through security processing; the ramp level, or the level where all the baggage tugs move, the lavatory trucks move, the aircraft themselves move, and all of the operational systems necessary to safely operate aircraft are present, just to name a few. To the passenger, the ticketing/boarding level is the most important. Obviously, because this is typically all they experience. This is where restaurants, shops, and other amenities are found that enhance and contribute to the overall passenger experience. The more space on this level that can be assigned to "revenue generation," as it is called, the better, according to those in management at least. Again, technology spaces are generally not considered revenue-generating, to the detriment of those who believe this misconception. It would be challenging for any commercial service airport with a yearly passenger count above 100,000 to operate in any respectable capacity without technology ... if at all possible.

So, what can be done? Many airports do not have adequate space for their burgeoning technology needs simply because many airports were designed and built prior to the proliferation of technology as it is known today. What was once thought of as sufficient has recently been deemed inadequate. For starters, common-use

terminal equipment (CUTE), common-use passenger processing systems (CUPPS), and common-use self-service (CUSS) have gained popularity (shared use is a separate and logically disparate system) (Figure 6). These systems allow a single set of hardware to serve multiple airlines, allowing maximum flexibility in available aircraft gates, boarding areas, and even ticket counter locations. The burden lies on the airport owner's infrastructure to support the system, which involves a complex back-end virtualization platform to house each airline's own specific system. Not all airlines use the same software systems. It also encompasses additional firewall hardware to create secure connections to each airline's native networks, which, in turn, may lead to additional service provider equipment. In short, physical infrastructure plays a key role here.

FIGURE 6: Shared use interface.
Image Credit: airIT (An AMADEUS company)

This may sound all well and good; however, each airport is different in how it handles its lease agreements with the airlines. Not all gates may be available to use this type of system due to preferential use agreements, particularly in large to major hub airports or "fortress hubs" as they are known. So, what happens when an airline decides to shove its political weight around and balk at this concept? What if it decides to keep its native network systems regardless of what the airport operator (owner) decides to do? This is where innovation comes into play. Enter the well-known segmented cabinet.

Here is the thought exercise. What happens to a city when the uptown (or downtown) section becomes congested? What happens when a concept cannot build outwards (thinking horizontally)? What does it do? When it cannot build outwards, it builds upwards like skyscrapers. The same concept can correlate to this environment. When one cannot expand outwards, one builds upwards.

Ask, does every tenant need a full 7-foot rack for their technology needs? Or do they usually use only about eight to 10 rack units (RU) per deployment? If the answer is "no, they do not need the full height," then the environment is ripe for colocation. There are myriad manufacturers that have multi-compartmented cabinets to choose from. One may say, "I don't like cabinets and they are difficult to work in." There is no disagreement there; however, certain sacrifices have to be made when space is a premium. The encouragement here is to choose the lesser of the evils.

Multi-compartmented cabinets are not new yet are akin to skyscrapers in the fact that they can house multiple tenants or systems independently within the same footprint. Imagine housing three or four separate tenants or systems in the same 7.5-square-foot space (depending on need) as opposed to providing that amount of space (and associated NEC/ANSI/EIA/TIA clear space) for each individual tenant/space. Couple this with the wonderous variety of handle security options available in addition to overall room security, include in-cabinet electrical options, and you have a viable solution to pitch to your organization. Think of it as a gym locker system (Figure 7). Each tenant (airline or otherwise) gets their own space within the overall telecommunications room. They can do with it as they please. Tenants can be given access to the overall room and to their specific cabinet compartment so that their in-house technology personnel can access and support their own equipment. The airport operator provides the basic amenities, such as the cabinet space itself, the electrical supply, and even access to the optical fiber backbone if need be. One could even build a lease agreement or rental agreement around this if one chooses to. The possibilities are quite numerous. Imagine a space where multiple independent users can

house their equipment separately from one another yet maintain secure and independent access to the same within an overall space footprint. Does this sound like a colocation data center? Yes, it does. This begs the question ... which industry began this practice first? Multi-compartmented cabinets existed before the modern data center did as well as the concept of colocation. This leaves one to their own research in resolving that question.

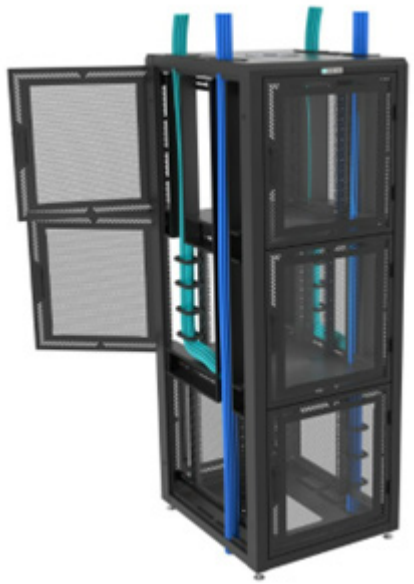


FIGURE 7: Co-located cabinet. Image Credit: GreatCabinets.com

Speaking of optical fiber backbone, this too can be used to collocate multiple independent tenants and systems within the overall campus. The airport operator essentially becomes the "last mile" provider in this instance. The advantages of this include additional leasing options (and associated revenue) as well as maintaining control of crucial pathways and spaces. One does not want to allow the masses to do as they please with the building and its precious infrastructure resources. Maintaining control of the physical infrastructure is paramount to providing an equal and fair experience for all who choose to do business at an airport. What is provided for one tenant must be provided for all tenants. This is crucial as an airport operator. Maintaining control ensures that capacity can be managed efficiently, quality of installation can be maintained, standards can be followed, and construction related outages can be better planned and communicated. In short, it is just good business, and business partners will appreciate it. The downside, however, is that one must be ready to answer calls when a problem arises ... because they certainly will. This equates to having staff on-call, ready, and available at all times, be it in-house or contracted through a local company.

There are other options should an airport (or other facility) not possess adequate space, even for this type of colocation. What if the only telecommunications room within serviceable distance does not have adequate space? This is where a distributed infrastructure would benefit, combined with a collocated optical fiber backbone. The industry knows this as zone enclosures (See Figure 8). CLT developed, with the author, a system of zone enclosures to relieve congestion problems due to a lack of adequate and available space on the boarding level. These enclosures were used to serve one to two boarding gates and associated jet boarding bridges for airport-specific systems, such as access control, building automation, Wi-Fi, flight information displays, video surveillance, and even the CUTE system, to name a few.

FIGURE 8: Plenum zone enclosure. Image Credit: Panduit.com


Bicsi
Essentials of
Data Center Projects
2nd Edition
Bicsi
STANDARDS
ANSI/BICSI 002-2024
Bicsi
an American National Standard
ANSI/BICSI
002-2024
Data Center
Design and Implementation
Best Practices
Bicsi
Design Data Centers
with BICSI
Bicsi

If there is available space and only airport-specific systems are served, then a combination of Class 4 power and optical fiber would be beneficial. If not just within this space, then a combination of others possibly. If, however, multiple tenants need to be served, then a model from, say, a shopping mall can be used here. The airport terminal is very similar to a shopping mall. Anyone who has ever flown and passed through an airport terminal would agree. Usually, but not always, the airport operator has agreements with one or more vendors to govern the food, beverage, and retail spaces found within the terminal.

CLT developed, with the author, what was called a Basic Cabling Package that was used in all renovations and new construction for these types of spaces. It consisted of two Category 6 UTP cables, one Series 6 Quad shielded coaxial cable, and a 6-strand micro armored single mode optical fiber cable. In addition, each suite was required to have dedicated space for a small, wall-mounted rack. The idea was to allow the tenant to house their core equipment within one (or both) of the common-use main equipment rooms on campus and distribute their network via the collocated optical fiber backbone infrastructure, the coaxial network, and even the legacy copper backbone that had been developed over time. The service providers were also housed within the common-use main equipment room, which gave all tenants equal and competitive access to multiple ISP vendors. With a wall-mounted rack in the "back of house" space and the basic cabling package, the vendor had maximum flexibility, which they enjoyed. The airport also benefited from this flexibility. When a space was renovated, changed ownership, or was made into a new concept entirely, the communications infrastructure was already in place. This saved both time and money for all parties involved. A win-win scenario.

Airlines can benefit as well. During design exercises, the overall size and distribution of telecommunications rooms and spaces can be better defined if, and only if, the number of tenants can be adequately projected. This may seem like a farfetched concept, but it does work if given the chance. Physical network infrastructure is usually considered a nuisance during development. If designers of said infrastructure can show that they are trying to be considerate, then it goes much better with the rest of the team. It is here where the quantity of cabinets with their various compartments can be discussed, and overall space can be requested with justification. Oftentimes, that space has to be fought over, and it usually ends up with the owner, architect, construction project manager, and ICT designer embroiled in a verbal argument. One should stand their ground and advocate for their customer; business relationships will flourish when this occurs. The look on a customer's face is priceless when presented with a well-thought-out and adequately constructed space for their vital business systems.

CONCLUSION

In conclusion, colocation is essentially a mindset. It has existed for a long time and will continue to exist long into the future. The options are many, and the possibilities are virtually endless. The idea of colocation is, at its core, to maximize the use of what is available for the maximum benefit of all parties involved. This works for the present. The idea of colocation is also one that can be used effectively for what may or may not come in the future. Adding a little more space, pathway, or capacity in any facet will assuredly pay off. Certainly, do not ever say, "We will never use this amount." For to do so may be to one's own detriment. In the movie *Under Siege 2: Dark Territory* (circa 1995), there is a scene where one of the antagonists, Travis Dane, is hacking a Palm Pilot (remember those?) belonging to the protagonist, Casey Ryback. In this scene, he confidently states that "a gigabyte of RAM should do it." At that time, a gigabyte of RAM was an amazing amount and was certainly considered overkill. But what about now? What the public thinks is overkill now may not be so in the future. Technology professionals are continually faced with more systems, more automation, and, ultimately, more demands on infrastructure. Placing oneself in the colocation mindset and looking at one's technology ecosystem through a different lens may prove beneficial both now and in the future.

AUTHOR BIOGRAPHY:

Justin W. Hobbs, RCDD, TECH is a husband, father, writer, author, and physical network architect. With almost three decades of real-world experience spanning both logical and physical networking, construction, contracting, and system ownership, he has worked in many sectors, including government, military, education, data centers, aviation, and healthcare. Having filled roles ranging from field technician, project manager, consultant, system owner, and subject matter expert, Justin has drawn knowledge from real-world experience, published standards, and other sources to further the awareness and acknowledgment of ICT systems, Layer 1, and ICT holistically. Justin holds a Bachelor of Science from the University of North Carolina at Greensboro, summa cum laude, along with several distinct industry certifications from BICSI and AAAE. In January of 2024, he published his first novel. He lives in Denver, North Carolina, with his wife and two daughters and can be reached at jhobbs4007@gmail.com.

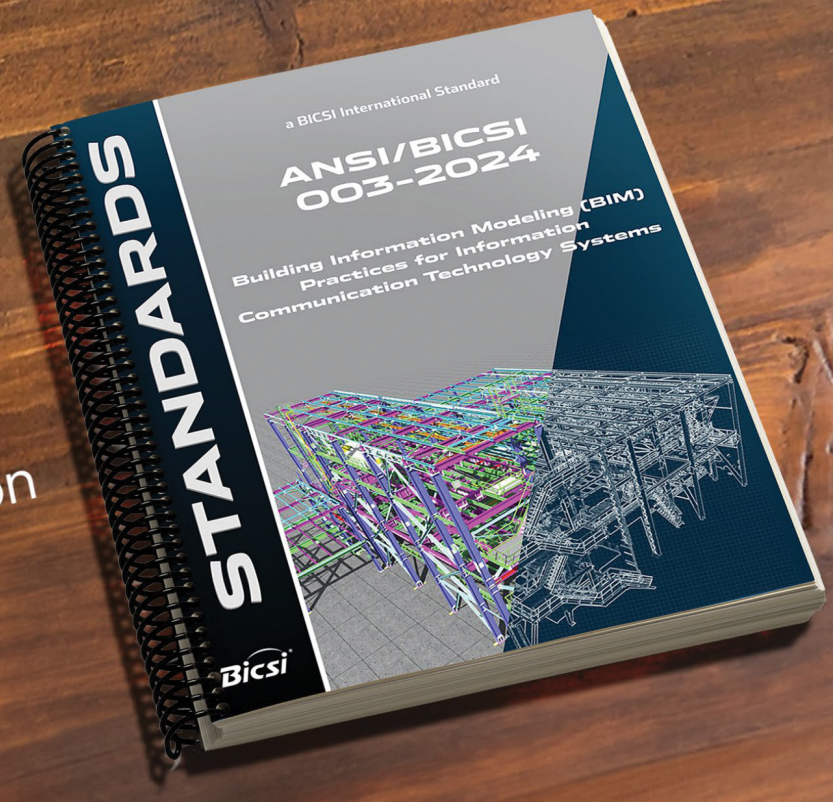
REFERENCES:

1. Merriam-Webster. (n.d.). *COLOCATE definition & meaning*. Merriam-Webster. www.merriam-webster.com/dictionary/colocate#:~:text=%3A%20to%20locate%20(two%20or%20more,Dutton's%20Navigation%20%26%20Piloting%20 14th%20Edition

2. Wikipedia contributors. (2024, May 6). Virtual machine. In *Wikipedia,* The Free Encyclopedia. Retrieved 14:17, May 12, 2024, https://en.wikipedia.org/w/index.php?title =Virtual_machine&oldid=1222494162

ANSI/BICSI 003-2024

Building Information Modeling (BIM) Practices for Information Communication Technology Systems



MISSED THE LAST EDITION?

NO WORRIES,
SCAN OR CLICK
THE QR CODE
TO CATCH UP!

Bicsi®

COMING 2024!

A WHOLE NEW ERA OF PICKUP TRUCK SOLUTIONS.

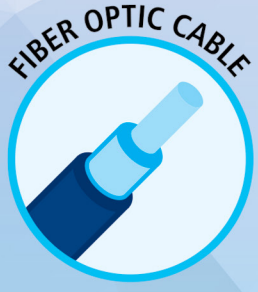
Learn more at NewEra.AdrianSteel.com

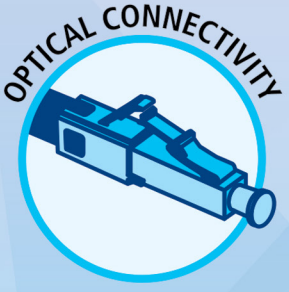
SCAN ME

ADRIAN STEEL®
Cargo Management Solutions for Commercial Vehicles

AFL

Connecting the world, one fiber at a time.





Visit AFL at Booth #2313
during BICSI Fall 2024

LEARN.AFLGLOBAL.COM