

OPERATIONS, IT, AND CONSTRUCTION TIME ORIENTATIONS AND THE CHALLENGES OF IMPLEMENTING IOT

SUBMITTED: April 2023

REVISED: July 2023

PUBLISHED: September 2023

EDITORS: Chansik Park, Nashwan Dawood, Farzad Pour Rahimian, Akeem Pedro

DOI: [10.36680/j.itcon.2023.031](https://doi.org/10.36680/j.itcon.2023.031)

Carrie Sturts Dossick, Ph.D., P.E.
University of Washington, USA
cdossick@uw.edu

Madison Snider, Ph.D.
Siegel Family Endowment, USA

Laura Osburn, Ph.D.
University of Washington, USA

SUMMARY: *The adoption of Internet of Things has grown significantly in recent years both to address sustainability in campus operations and as part of digital twin systems. This study looks at in-depth cases of large university campus owners and the challenges that this IOT introduces for the maintenance and management of these systems and the data they collect. In this ethnography there are three main time orientations related to facilities management (Facilities), Information Technology (IT), and Capital Projects. First, a university campus is like a small city, with buildings, utilities, and transportation systems - taken together we call this campus infrastructure (buildings 50-100, roads and utilities 20-50 years). Second, IT employees think on 2-3-month scale, working through implementing software and hardware upgrades, configurations and patches, at times needing agile operations to deal with emerging cybersecurity threats. Third, in Capital Projects the design phase can last 9 months, and the construction from 1 - 2 years for a typical project, and this is where IOT technologies are often first introduced into campus. While the capital project teams reflect on the user experience, these teams are often removed from the realities of facilities management and do not understand the time scales or the scope of the work that is required to manage a portfolio of Facilities and IT systems. In this paper, we explore how these time orientations lead to tensions in the owners' selection of IOT devices and systems, in the integration of new technologies into existing systems, and in the operations of keeping existing systems up and running for the longer time scales of campus infrastructure life spans. Furthermore, this paper presents a paradox: If they speed up, they lose things, if they slow down, they lose other things, and presents ways that owner organizations manage this paradox through temporal boundary spanners who understand the disciplinary requirements, cultures, and frameworks across the organization and helps to mitigate the tensions across these differences.*

KEYWORDS: *Internet of Things, Information Technology, Facilities Management, Operations, Time Orientations, Organizational Issues*

REFERENCE: *Carrie Sturts Dossick, Madison Snider, Laura Osburn (2023). Operations, IT, and construction time orientations and the challenges of implementing IOT. Journal of Information Technology in Construction (ITcon), Special issue: 'The future of construction in the context of digital transformation (CONVR 2022)', Vol. 28, pg. 585-596, DOI: [10.36680/j.itcon.2023.031](https://doi.org/10.36680/j.itcon.2023.031)*

COPYRIGHT: © 2023 The author(s). This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



1. TIME ORIENTATIONS AND THE INTERNET OF THINGS

Differences between disciplines are often a main theme in design, construction, and operations research when organizational issues are considered. One aspect of disciplinary divisions is the concept of time orientation (Karasti et al., 2010)—the time scales that individuals think about and work within. While the field of project management deals extensively with the management of time as planning and scheduling are core disciplinary concepts, one underexplored aspect of time in project management research is the challenges of managing across different temporal orientations such as when facilities owners manage technology within the context of facilities management where facilities have long time scales, but technology operates on shorter time scales. In our analysis, we identify three main time orientations related to Internet of Things (IoT)—devices and systems connected to either private or public networks—in a facilities management context: campus infrastructure, information technology, and Capital Projects. The introduction of IoT brings professionals with distinctly different time orientations (e.g., facilities, IT, and construction management) together in new ways as IoT devices and systems connect to building and infrastructure operations as well as computer networks and cloud computing. In this paper, we discuss the tensions and impacts that arise and discuss how individuals act as temporal boundary spanners (Stjerne et al., 2019) to negotiate across these differences.

The first category of time orientations relates to the facilities management (Facilities) of campus infrastructure, which includes buildings, utilities, landscaping, walkways, and transportation systems. The facilities managers are responsible for the maintenance and operational conditions of the campus infrastructure. Buildings can have a life span of 50 to 200 years. Roads, walkways, and utilities are maintained over a 20 to 50-year time scale. Similarly, many of the facilities managers spend their entire career at a campus, working up from the trades into management for an average of 30 to 40 years. The timeframes for facilities managers as they manage buildings and infrastructure are relatively long. They work in the same buildings, with the same utilities for a majority of their careers. While small systems like motors or fan belts may change, the majority of the artifacts in the campus infrastructure have relatively long lifespans.

Second, and in contrast, information technology (IT) experiences almost constant change and flux. Computers change annually with most desktop computers being upgraded in 3-5 year spans. IT employees buy new computers constantly when new members join the organization. Software systems have routine updates on the order of months. The technology for networks and services is constantly improving and large institutional owners have to make decisions about upgrades on 3 to 5-year timeframes. When systems are not updated, they begin to feel archaic after 3 to 5 years and some vendors are moving towards automatic hardware and software updates with subscription services. Cloud computing is enabling even faster update cycles for file sharing and data processing. IT employees think on a 2 to 3-month time scale, working through implementing software upgrades and patches, updating network configurations, and dealing with annual software license renewals. Furthermore, this work often requires agile operations to deal with emerging cybersecurity threats. In contrast to infrastructure time, information technology is a rapid-fire dynamic environment characterized by constant change.

The third category of time orientations is Capital Projects. These professionals work in architecture, engineering, and construction management disciplines. They work on the design and then construction of new facilities or the renovation of existing facilities. While early project scoping and budgeting may take many years, once the designers and builders are under contract, the design phase typically lasts 9-12 months, and the construction from 1 - 2 years. These are deadline driven project environments where the designers and builders are working under contracts with milestones often tied to payments. In the context of a campus, they are temporary workers, hired to do a specific and defined project usually confined to a single building or campus area. They are highly trained and bring in the latest technologies and building systems into the projects. While the project teams reflect on the user experience, these teams are often removed from the realities of facilities management and do not understand the time scales or the scope of the work that is required to manage a portfolio of campus infrastructure or campus IT. New projects bring new IT challenges to the facilities management team as they introduce emerging IoT technologies that are designed to improve building performance, but bring with it new IT management needs.

In this paper we explore the dynamics and challenges that emerge when facility owner organizations grapple with these three-time orientations as they implement new IoT technologies. The adoption of IoT requires increased collaboration and integration of owner organization staff, in particular those with disciplinary agendas related to IT network security, facilities management, and capital projects. In this paper we use ethnographic observational methods to define and explore the technology adoption challenges that arise in part due to distinct differences in

time orientation between the three groups. We then turn to how facilities management staff are adapting organizational strategies to address these tensions through the use of temporal boundary spanners (Stjerne et al., 2019), who act as information gatherers and knowledge brokers between the different temporal scales of Facilities, IT, and Capital Projects.

2. REVIEW OF LITERATURE

First, we review the context of hybrid organizations and then introduce the concept of time orientations, followed by the concept of temporal boundary spanners. Different time orientations emerge as important organizational dynamics in hybrid organizations where there are multiple divisions and a variety of disciplines. In the context of higher education campus owners, their organizations contain both sustaining disciplines of Facilities and IT as well as project-based disciplines of Capital Projects. Time orientations both shape and emerge from disciplinary culture, which in turn shapes and is shaped by the artifacts they work with. Time orientations are not only dealing with project management concepts like task duration and the time scale for planning, but they have different interpretations and emphasis on past, present and future tasks and actions. Temporal boundary spanners are actors whose organizational role consists of bridging and mitigating the tensions between disciplinary temporal scales.

2.1 The organizational problem: hybrid organization

In this work, we studied large organizations that consist of multiple divisions that represent a variety of disciplines. While scholars have used the concept of hybrid for identities and rationales, we focus here on the work around hybrid forms (Battilana et al., 2017). Large institutional owners (e.g. higher education, healthcare, government) have both project-based work in the form of new construction or renovation projects alongside operational work in the maintenance and operations of buildings and infrastructure across a campus. Organizational science recognizes the complexity of this type of multi-faceted organizational form with the concept of hybridity where “the combination of identities, forms, logistics or other core elements that would conventionally not go together” creates contradictions as well as interdependencies across teams (Smith & Besharov, 2019, p. 1). This work suggests that leaders and managers need to understand hybridity through how and what ways different parts of the organization and the disciplinary frames interact and how these points of intersection set up constant tensions and contradictions that the teams need to navigate (Benson, 1977, Schade et al., 2011). In this paper, we focus on one aspect of hybridity: different time orientations.

2.2 Time Orientation and how it shapes work

Scholars in science and technology studies and organization studies have found the concept of temporal orientation useful to understand the dynamics between technology development and infrastructure management (Karasti et al., 2010). Temporal orientations relate to a group’s understanding of the meaning and value of time, and their interests, aims, and motivations (Karasti et al., 2010). Temporal orientations are socially subjective understandings of time that create work-culture expectations, often defined by discipline and the scope of work that a group of people are tasked to do (Karasti et al., 2010). However, temporal orientations are also not stable understandings of time, but are emergent orientations that respond to the daily activities and work requirements of an occupational group (Orlikowski & Yates, 2002). This means that a worker can shift from one time orientation to another depending on the task at hand and its accompanying purpose, deadlines, and required activities.

In infrastructure work, there are often tensions between the demands of the present and those of the future (Ribes & Finholt, 2009). Karasti et al. (2010)’s found this tension in the temporal orientations of developers and information managers working on the development of a metadata standard for an ecological research center. These tensions occurred between two particular orientations that are often in tension: “project time” and “infrastructure time” (Karasti et al., 2010). Developers’ “project time” orientation reflected their need to often complete specific metadata projects for a specific research group within the research center. These projects often had a clear beginning and end (Karasti et al., 2010). Information managers, on the other hand, had an “infrastructure time” orientation in that they favored work practices that would achieve the long-term goals of the center beyond a specific project (Karasti et al., 2010). Tensions between the two orientations would arise when developers would view information manager plans and expectations for their work as too open ended and unrealistic to achieve project goals. Information managers would, in turn, view developers as “short-sighted” and isolated from the larger purpose of the research collaboration (Karasti et al., 2010).

These same tensions play out for IT, Facilities, and Capital Projects in the management of campus infrastructure. As IT and facilities management professionals plan the work of managing future facilities and IT infrastructure, they anticipate the tasks, timelines, and resources they will need for that work based on their past temporal rhythms—the recurring patterns of their collective work (Reddy et al., 2006) - and how they should arrange and organize their temporal rhythms to meet specific milestones, deadlines, or appointments (Reddy et al. 2006). Scholars have defined this futuring work as anticipation work, which is the practices that cultivate and channel expectations of future, design pathways into these expectations or imaginations, and maintain visions of future in face of a dynamic world (Steinhardt & Jackson, 2015). What we found in this research is that the introduction of IoT into facilities management challenges the anticipation of work for both the IT professionals and the facilities managers. One of the main conflicts in this change were differences in time orientations between the three disciplinary groups in the hybrid organization of a large campus owner: Facilities, IT, and Capital Projects.

2.3 Temporal Boundary Spanners Navigate Cultural Differences

One of the ways of mitigating these tensions are through temporal boundary spanners (Stjerne et al., 2019). Boundary spanners are actors who engage in knowledge exchange between groups (Haas, 2015). In a review of engineering literature, Jesiek et al., (2018) found that boundary spanning research in engineering includes negotiating across disciplinary differences and across project stages. Boundary spanners often have broad expertise, and/or cultural knowledge that helps them to navigate and mitigate tensions and advocate for multiple points of view between different groups, which can improve collaboration (Di Marco, et al., 2010). In this paper, we bring in the more specific concept of temporal boundary spanning from organizational science literature. Temporal boundary spanners are actors who engage in knowledge exchange and group tension mitigation, but their spanning work is focused on identifying and mitigating temporal tensions on teams (Marrone, 2010) or between organizations (Stjerne et al., 2019). This includes tensions related to temporal conflicts between short-term and long-term needs and goals (Stjerne et al., 2019), which has as yet to be explored in the engineering domain.

3. METHOD

This paper reports results from a 3-year study funded by the National Science Foundation in the US. As we sought to answer questions about how and why IT and Facilities teams struggled and succeeded to create shared cybersecurity culture, this study includes a 2-year in-depth ethnography of a higher education campus (120 hours of observations with 178,933 words of notes), 7 ethnographic interviews, 40 national interviews, and 5 case studies of higher education organizations. This paper focuses on findings from the ethnographic observations in 2020 and the ethnographic interviews conducted between 2020-2021. The selection of our ethnography site included finding a large owner organization who was implementing IoT systems across their buildings and how had cybersecurity concerns. We focused on higher education as one of the most targeted type of owners in terms of cybersecurity (Honeywell, 2021). The owner organization we selected for our ethnography had IT teams who were experts in cybersecurity, and a large established facilities management department. Our observations were focused on meetings that included staff from both IT and Facilities, where these staff members worked on IoT implementation and management. Our ethnographic interviews centered on collecting participant's opinions and experiences with IoT integration within the context of a specific building project. Due to COVID lock down procedures, a majority of our observations and interviews were conducted on zoom. One or more of the research team would sit in on the meetings, observe the conversation, and take detailed field notes. In developing this paper, the authors met weekly to iteratively review field notes and the literature, to build organizational theory of the phenomenon.

4. CAMPNET: TIME ORIENTATION CLASHES AND THE PARADOX OF LOST THINGS

CampNet is a pseudonym for a computer network system in our ethnography, short for Campus Network. Campus IT established this network behind a firewall to protect building systems that needed to have internet access. Over time a variety of devices and systems were connected to this network without centralized record keeping or tracking. From January to November of 2020, the research team observed specific meetings between Facilities, IT, and electrical engineering vendors, who work on the CampNet. Amongst the professionals working on CampNet were Michelle, a network engineer and Dave, a cybersecurity specialist, both of whom worked in the campus' central IT organization. From the campus' Facilities organization were Glen, a utilities operator, Vince, an IT specialist who led a Facilities-oriented Business Innovation and Technology (BIT) group, and James,



Facilities BIT information manager and GIS specialist. In addition, there was Nick, a specialist in technology infrastructure for Facilities and a representative from an electrical engineering vendor specializing in control systems that had been hired by Facilities as a consultant.

The particular project of focus in these CampNet meetings was a migration from the “old” CampNet to a “new” one. This transition exemplifies the time orientation clashes between Facilities, IT, and Capital Projects. First, within the meetings, two orientations came into play: IT and Facilities orientations. Orientations were often invoked by professionals from specific organizations on campus (IT orientation held by IT departmental staff and facilities management orientation held by Facilities staff and engineering vendors). However, some staff, such as Vince, who had disciplinary backgrounds and agendas that crossed organizational boundaries, would shift from Facilities to IT orientation depending upon emerging concerns, at times functioning as a boundary spanner. A third orientation then was introduced when Capital Projects adds new devices and systems to the existing network. This project orientation created timing and logistics challenges for how, when, and where the new project systems were connected to new or old networks.

4.1 January, 2020 (before COVID Lockdowns began in the US).

When we started attending CampNet meetings the conversations were focused on server space and an impending change to CampNet though it was not clear what the best change would be. There was discussion about the risk of CampNet remaining an island—that is, isolated from other networks—and the possibility of converting to a cloud-based network. A lot of this conversation was contingent on funding that was decided outside of this group. The discussions about funding were strategic in terms of how to successfully request funding. This demanded “thinking five years ahead” to what technology they will need. The conversation included the option of transitioning to a cloud-based network as a matter of security. As they discussed the risks, the group seems to recognize that there are different concepts and definitions between the disciplines in the group so that translation was necessary. Michelle (IT), who has a technical IT orientation stated that CampNet is an “island, [and] as long as it stays an island will only hurt us.” The comfort with an island network was one that was culturally more familiar to Facilities than to IT. The vendor representative, Nick, who had experience working with many large owners, argued that Facilities usually err on the side of separation of networks not integration. This became a theme as IT and Facilities recognized the need to work more closely and reconcile these cultural differences. What did it mean to be an island and why is that going to hurt us? What are the ramifications of using new cloud technologies? How do we keep the campus operational while also protecting the systems? The two sides weighed in with divergent perspectives that at times were not reconcilable.

In the first meeting, the team reflected on the ramifications of the options. First, leaving CampNet as an island, although perhaps not the most secure option, had benefits in that those who need access to all parts of the network (i.e. Facilities) know they will maintain access. The concern with moving to a new network configuration (perhaps the cloud) would be making sure that access is maintained. Mid-way through this discussion Vince reminded the group that there are in fact two CampNets—the old and new. Glen called for an investigation into what was on old CampNet so that they knew why they couldn’t move on to new CampNet completely. This was a seemingly simple request that proved hard to accomplish. This was where Facilities time orientation emerged: the long timelines of facilities management meant that devices and systems had accrued on the CampNet over time, like crustaceans on an ocean pier, and no one really knew what all was connected, and what the requirements of those connections were.

Due to the long timelines of facilities management and that seemingly it was not important in the past to maintain records, some of what was connected to the network was now lost to the group planning the transition and had to be documented anew. The discussion around CampNet transition—from old to new—focused on what the transition entailed and what risks were involved. For some systems the transition was relatively easy and risk free, but there were always a chance that in making a big transition there would be a “big bang” as Vince warned and things could go really wrong when they did not understand all the devices and systems connected to the old CampNet. To address this concern, the team floated the idea to run old and new CampNets in parallel as a means for avoiding losing things in the transition, which had maintenance and management implications. We see here how they struggle with losing things due to the longer time orientations of Facilities.

Thinking about the design of the new CampNet, the group tries to set up network management structures for virtual management. There was a disagreement that arose between Nick (vendor) and Michelle (IT) about the feasibility

of making the new CampNet less of an island. The benefits of doing so included making more virtual controls possible (this desire was expressed even before we knew how important it would be in 2020 and beyond). There was a brief discussion about how vendors would have to be brought into the conversation and be held accountable to make their systems more dynamic, including jokes about how some vendors are way behind on updating their software. This indicates a second time orientation challenge related to IT and the rapid and dynamic environment of software updates and system changes. The vendors' ability to stay up to date with their software impacted what the campus organization was able to do as far as their own network. In addition to vendors, IT wanted to use state of the art tools like remote dashboards to manage and monitor the IoT devices and systems, requiring that the new CampNet be less of an island. The IT time orientation put pressure on the team to continually change, while the Facilities time orientation wanted isolation and more static network environments.

4.2 March 2020: COVID Lockdown

This was the first CampNet meeting since COVID closures. The group pivoted the agenda to discuss COVID related network surge needs and an uptick in malicious activity.

The discussion in this meeting (as far as CampNet migration was concerned) focused on a new central utility building (a recent capital project that would supply energy to a large portion of campus) and the challenges they were having with connecting these new systems to campus networks. The team debated the benefits and risks that had recently emerged with this networking and whether it is riskier to stay an island or to "poke holes" in the network. Vince (Facilities IT) was one of the facilities team members with an IT disciplinary role. He stated:

"We're on the same page. We're not opening it up to the world unless there's somewhere in the world we can really limit the connection to. Or the window being opened is tightly defined to the one system. The issue is, once you poke that whole system ... you have to have a set of security principles ... that has not introduced risk beyond the security profile of what you're trying to control against. Right now, denying all inbounds means no risk. I cannot say to you that we have a server that has security principles on it that you can say is no risk—that's totally protected. Not having a real risk profile for systems that sit inside these types of structures makes it impossible to calculate what runs in there and what is [at] risk if those systems are compromised."

Here, Vince is alluding to the concern about lost things, both in the past and in the future. While Vince's position is housed within the Facilities organization, he has an IT perspective that is concerned with security. Part of the work of security is to understand what is connected to the network and how it is connected to the network. Any connection in the network is a path in, and once in the cyber-attacker can reach everything else on the network. From the IT perspective, they need to know about all of the devices and systems connected to a network.

Lost things made IT very nervous. Consequently, the team tried to future proof the network design, acknowledging that Capital Projects will continue to add new systems to the network as new building projects come online. Time emerged again as an important consideration when making networking decisions because the assumption was that with the passage of time the networks will become more and more populated with new devices and systems and there was a need to build the network architecture with foresight into how things will develop. However, it was hard for the staff to anticipate what that would look like. To end this meeting the leader, Dave (IT), introduced an initiative to inventory the devices and systems on CampNet in order to increase awareness of the scope of the network, track its growth, and manage ownership. This was both an effort to reach back in time to make sense of what has already been put on CampNet, but also to look forward to future needs in assigning ownership for ongoing management of the building systems and how they will interface with the campus networks.

4.3 April 2020

The meeting started with a discussion of ways to track devices and systems on the network as a means for improving security. This was particularly concerning to Dave (IT) as he saw trends for a future with a lot of growth in networked systems. Dave (IT) talked about CampNet issues as "whack a mole" and the departure of a key staff member in Facilities was brought up as a risk area because this person had "owned" a lot of lighting controls in Facilities, but now ownership was up in the air. Michelle (IT) brought up a wiki shared with IT that included drawings of future lighting control plans but this was not yet available to anyone else in the group. Michelle (IT) mentioned that because these systems had to "talk to other things" they had to be put on old CampNet. Dave called for a list of lists to get an idea of what the scale of the dual home devices and systems problem really was. This

sparked a conversation about who “owns” what and to what degree people know what was on CampNet and what was not.

4.4 June 2020

While capital projects had added devices and systems to the network in prior meetings, this meeting was the first time we saw a conversation about the timing strategy for this group to be involved in the capital project design and construction processes. Based on the recognition that IoT devices and systems get set up in new building projects in less-than-ideal ways (from this groups’ perspective) there was a shared desire to come up with a better system for submittal reviews and design guides. The idea was floated to create a protocol that would allow someone from CampNet group to catch these issues during design decision-making. It was suggested that this might be a cybersecurity review process or they should consider making this a step in the submittal review process. They defined the problem as not having an “owner” to speak to – no real point of contact for some IoT devices and systems (i.e., lighting controls). But it was an issue beyond lighting controls, as Nick, the vendor, reminded everyone. Timing of how and when CampNet group was to be involved was a key concern.

There was also a discussion about the problem with dual CampNet (new and old) that were both needed in new buildings but do not work well together. Old CampNet connected legacy systems making it impossible to use for new buildings. This was at least partially a problem blamed on the design-build team because they had failed to consider cybersecurity risk early enough to have a meaningful impact on design and make safe connections to old CampNet. Here we saw a clash between the capital project team time orientation focused on a single building and the construction timeline of 2 years and the Facilities timeline of maintaining infrastructure like the CampNet for 50 years.

In addition to connections to CampNet, there were two timing issues for coordinating between the building teams and IT. First, contractors put up devices and systems to measure commissioning data that did not get securely networked and then were often left in the building without anyone in IT/Facilities knowing about them (another way things were lost). This was a cybersecurity issue and had to do with the timescale that design-build teams generally work on as opposed to IT/Facilities teams. Second, clearing IT closets was another issue. IT (and maybe Facilities) needed access to closets and for them to be cleared earlier than was typical construction and commissioning sequencing. This was referred to as “early service” and there was a communication infrastructure team that worked on requests of this nature, but it seemed from the CampNet meeting that in reality this did not happen early enough in the building commissioning for them to gain access to the network connections to be effective.

4.5 July 2020

David (IT), Michelle (IT), and Nick (vendor) organized a breakout meeting to discuss the CampNet transition. By this point it was decided that the transition would not be simultaneous but a staged transition in parts. The benefit of this was to avoid losing things but also being able to identify dual home devices and systems, isolate, and flag them. It was suggested that this could be a building-by-building transition but the final plan was undecided. One timing and labor issue would be the logistical challenge that many of the ~600 devices and systems that will need to be reassigned an IP address (“re-IPed”). It was unclear how many would need to be re-IPed physically with a technician in the field. Many could be done remotely, but not all. It was suggested that there be a mandate to not allow anything new on old CampNet, but there was also a recognition that this would be really difficult to govern. There were systems that need to be on old CampNet for some reason and the timelines for bringing new capital projects online necessitated work arounds that included old CampNet.

4.6 August 2020

The main issue in this meeting was the reconfiguration of CampNet that was being prompted by the Bennington lighting system [pseudonym]. There was concern that reconfiguring the network architecture for a single system was not a great strategy, but others suggested it was an architectural change that they have wanted to do for a while beyond this specific system and it would address some of their migration logistics. As Nick, the vendor, puts it, “way better than the alternative and not necessarily a reaction to [Bennington]. It’s about how to migrate assets off of [CampNet] for several months now and the assumption had been there was no convenient way without having to re-IP everything which would be slow and laborious. Now we possibly have a route out of that box where we can join them together. I think that’s a slam dunk.”



The tensions between time orientations are evident here between those who need the CampNet migration to happen more quickly because they were continually having new systems added through capital projects. However, this was in tension with the need for a controlled phased migration approach that would be more secure and would give them the time to figure out what they have, what might have been missing, and what devices and systems needed to be assigned ownership. This tension was evident in a new capital project coming online at this time where there was a desire to use the new building as an opportunity to migrate all systems to new CampNet, but that migration would slow down the new project which was undesirable to many whose job it was to make the building occupiable. Others argued that this good time pressure as it was the “kick in the butt” needed to sort out the CampNet migration strategy. The question was posed: “Is it even possible to make this migration happen when we don’t know what is on CampNet?” At the end of the discussion, the feasibility of the migration was still in question.

In sum, so far, the team has debated the CampNet migration from “old” to “new” for 8 months. They struggled to find a feasible way to do the migration in part because of the time orientation tensions between the long-timelines of Facilities (managing buildings and devices and systems over years), relatively shorter timelines of new projects (adding new devices and systems to the network), and the extremely short timelines of IT (system changes and cybersecurity threats change monthly if not weekly, accesses needed to manage networks remotely). The CampNet system needed to change immediately from an IT and Capital Project perspective, but the legacy systems of the long-accrued existing infrastructure created challenges in terms of resources to execute a change, quickly if at all.

4.7 September 2020

In a new meeting for CampNet migration, there were still questions about how new buildings could be added to new CampNet since this would result in losing the ability to communicate with some systems from old CampNet - like radios. This was where we saw a paradox of lost things emerge. If the team goes slowly, they lose the opportunity to improve the CampNet functionality because they have connected new building devices and systems to the older network, further entrenching the old CampNet infrastructure. But, if they speed up, they lose some of the functionality of the old CampNet and lose connectivity to older devices, systems, and endpoints that were not documented prior to migration. Either way, they lose things. This paradox was managed as a series of tradeoffs with the team selecting what would be lost or compromised.

In this meeting, an interesting discussion happened about the strategy for segmentation. Because of the paradox, who made decisions was very important. Since there were multiple time orientations present in the organization, it would be vital that those time orientations are all present, else those disciplines are not represented and their time orientations are not accounted for. Furthermore, without the other perspectives, there was concern that those who were newly gaining access to CampNet would not understand the importance of protecting the network and would unintentionally put it at risk of operational breakdown or cybersecurity threats. Beyond the operational and security concerns, there was a deeper sense of responsibility to CampNet based on all the work done in the past to get it to where it was. This was part of the accrual of systems and the longer time scale management of information infrastructure as it supports the longer scale of buildings and infrastructure.

The management of CampNet was more aligned with the Facilities time orientation than the IT time orientation in that it needed to be maintained over a long time scale and this is a longer time scale orientation than typical IT approaches. In this way, the network became a material artifact of the disciplinary time orientation differences between CampNet people and others. As Dave (IT leader) explained “I also get concerned in some places-- when we meet here and in the critical infrastructure group, [CampNet] is kind of sacred to us: it warrants protection. When other groups use [CampNet], that same feeling of specialness doesn’t get passed on. And there’s not a reason why it would. So we could have the same network with people using it that have very different perspectives, and that causes me some concern.” The desire to have a strategic approach to segmentation was in part an effort to maintain the “specialness” of CampNet and to maintain control over its future and avoid barnacles getting attached to it without the institutional knowledge of the cybersecurity design intent that this team created.

4.8 October 2020

At this point, the CampNet migration was largely handed over to the Building and Information Technology (BIT) team within Facilities and an MOU was established to outline how they would manage this transition using firewall policies. At the time of this meeting, the MOU was not yet solidified, but was “conceptually” in place according to Vince. The time pressure from capital projects coming online continued to be a theme in this meeting. A newer

specialty lab building on campus was an example of a building that was neither on old or new CampNet— as it was on a network that was “kind of its own thing”. This building was used as an example of what they want to avoid.

Again, a new campus building was a trouble spot in the migration because of the project time. As one CampNet group member noted “stuff keeps coming at us and it gets more and more all the time. So at least we’re bringing in assets in an organized way.” If not coordinated perfectly, which was perhaps not even possible, the installation of new devices and systems of devices created “chaos” when it came to bringing new buildings online via the facilities network. This chaos was accentuated in this particular moment as the facilities network itself was getting an update. The chaos of getting new buildings online, a perpetual challenge, was made even more challenging during a time when the network itself needed to be upgraded.

After 10 months of discussion between IT and Facilities, choices were made, migration was planned, and the team had to navigate timelines of new capital projects’ devices and systems coming online as these tensions continued to be not fully resolved.

5. TEMPORAL BOUNDARY SPANNERS: MITIGATING TENSIONS TO MANAGE THE PARADOX

During the ten months of discussion and decision-making about how to move forward with CampNet migration, the emergence of a temporal boundary spanner proved to be a useful strategy for moving through the complexities illuminated above. James, the information manager and GIS specialist in the Facilities BIT group became a key liaison between the time orientation of Capital Projects and that of Facilities. James was encouraged to join building and design meetings in response to a recognition by IT and Facilities teams that part of the CampNet transition issues were the fact that the network was not static, but in fact in a constant state of change with new devices and systems being added by Capital Projects and AEC team decisions. By virtue of his position within the IT-centric team within the Facilities organization, James was already spanning the IT and infrastructure time orientations. When he started attending capital projects meetings in October 2020, James was able to function as a temporal boundary spanner, bringing IT and infrastructure time orientations and historical knowledge about CampNet design decisions to the capital project meetings, and also bringing the Capital Project time orientation considerations back to IT and Facilities. Reflecting on his own work, James alluded to the need for a temporal boundary spanner and the skills he brought to this role:

“That’s what they’re bringing me in for. When Philip and [other facilities managers] come with a problem where they’re like, “Well, I’m a manager and this is a side thing that I really don’t have time for. But this is the problem that’s happening: we’re losing track of where these things are being distributed.” And, that’s where my skill comes in: to go to these Commissioning meetings, where these assignments of these IP addresses are being given. So now, ... I see myself producing some best practices, develop a workflow, and then a policy so that we can introduce that to a new project.”

Here in this statement, not only does James describes his temporal boundary spanning role, but talks about methods of codifying what IT and Facilities design intentions are in policies that help keep those perspectives present in capital projects settings. James goes to both capital project meetings and CampNet strategy meetings to share information between these groups about new systems coming up in capital projects, like lighting systems. With James in the meetings the CampNet group knows what things will be gained on either the old or new CampNet or else lost and they can make strategic choices. The mitigation of more lost things is linked to the success of this boundary spanning work. As James’ supervisor, Jacob puts it: “James has done a lot of work identifying ‘where other bodies are buried.’” It is in this way that the temporal boundary spanner helps the team manage lost things and explain the policies and rationale for the CampNet design.

6. DISCUSSION

What we found in this study was that the management of shared IT infrastructure and the implementation of IoT in buildings was challenging due to the different time orientations across the hybrid organization of Facilities, IT, and Capital Projects. These time orientations were both defined by the teams as well as the disciplines of the individuals on those teams. For example, while Vince was in the Facilities group, he had an IT background and often came to the meetings with the IT time orientation, and therefore could function as a temporal boundary spanner. It is important to understand these organizational ramifications in planning for and organizing the

management of facilities and infrastructure. Likewise, it is important to understand how temporal boundary spanners can be a key to (partially) resolving the tensions and paradox of lost things.

First, in this case, we saw a shared IT artifact, the CampNet, as confounding the team members of Facilities, IT and Capital Projects. With finite resources, the management of Facilities, IT, and Capital Projects each had priorities and disciplinary orientations that were misaligned and often in tension. When working together, these teams discovered irreconcilable tensions in the work, where they could not meet all of the requirements of operations (Facilities and IT) and Capital Projects particularly in terms of cybersecurity. Some of these conflicts stemmed from different time orientations as different disciplines work with the same artifact (in this case CampNet) in different ways for different purposes. The Facilities disciplinary orientation was to get things to work as their priority was to maintain the operations of the buildings. To that end they sought to connect devices and systems to the CampNet as soon as possible. Given the longer timespans of buildings and infrastructure and the limitations of facilities management resources, prior to the ethnography, they had not kept detailed records of these connected devices and systems. As the team in this study explored a transition to a new network, this lack of recordkeeping was problematic for keeping facilities operational during the transition. In contrast, the IT perspective focused on short time scale issues like system updates and cybersecurity. IT asked for more record keeping around what devices and systems were connected, when, and by whom as they interacted with those devices and systems much more frequently. While these teams worked through these conflicts the third time orientation joined the discussion in the form of Capital Projects, which focused on a single building and getting that building online for the end users. Capital projects teams were oriented to short time scale based on the construction project schedule with pressure to finish quickly as occupants want to make use of the space as soon as possible. However, this speeding up came at a cost that was less visible to the capital projects teams, which was the coordination of systems and their maintenance over time and was in direct conflict with the longer term efforts for CampNet design, management, and migration. Capital project teams did not have visibility into nor are they incentivized to coordinate with other buildings or cross-campus infrastructure until a temporal boundary spanner was asked to join the meetings and bring these perspectives into the capital project management discussions.

Taken together, the long timeframe of Facilities resulted in a CampNet environment wherein many devices and systems were connected, some of which were unknown to the managers. IT needed to update the CampNet system as computing hardware and software required an update, while cybersecurity concerns suggest that connections to the CampNet needed to be closely managed. The tension between the need to connect and the risk of connections is a main theme throughout. This dynamic is the need to connect from Facilities side (to get things to work) and the concern about connecting from IT side (cybersecurity and network operations risks). This is coupled with the lack of documentation from Facilities side as devices and systems accrued over long time frames with the need to document from the IT side managing all network connections for cybersecurity.

Second, the timelines around implementation of IoT in buildings were also challenged by different time orientations and resulted in a paradox (the team lost things no matter what choices they made). If they were to move quickly forward with the new CampNet, they risked losing devices and systems which were historically connected to the old CampNet because they did not have a record of these devices and systems and may have missed them in the conversion. If they slowed down the migration, then they would lose the ability to capture the new capital projects which needed to connect to the new CampNet (as illustrated by the one high profile project that had done “its own thing”). These concerns emerged as we watched the meetings between Facilities, IT and Capital Projects personnel during which they navigated the technical challenges in the CampNet management and migration. On the one hand they needed to understand what was on the network (longer time orientations from Facilities) and what needed to migrate over (current and future needs of the networks), and on the other they needed to understand the cybersecurity risks that new or uncontrolled connections made in the network. As they navigated the network design choices and the timeframe for the migration, disciplinary priorities and time orientations became important to identify and reconcile. In this case, the CampNet team discovered a paradox – if they speed up they would lose things, if they slowed down they would lose other things. In working through the transition they had to make hard choices that left something out, and as a result they worked hard to mitigate the negative impacts of these choices or worked around the limitations (such as having multiple networks, which was suboptimal), while preparing for a future where more and more IoT devices and systems needed to be connected to the internet.

Third, this paradox suggests that there is a need to design IoT management teams that account for disciplinary differences. An appreciation and awareness of different time orientations is important in the management of IoT systems. For hybrid organizations like a higher education owner, the management of multi-disciplinary teams becomes important as these teams come together to share ownership and management of shared IT systems like a network. An antidote to temporal tensions that can account for disciplinary differences is the boundary spanning work of people like James. This work aimed to recalibrate the pace of project time and technology time with infrastructure time: namely through slowing it down. This was a struggle because of budgetary constraints and institutional expectations, but in light of the potential cost of lost things, a inclusion of an infrastructure temporal orientation was seen by many as necessary. While slowing-down work may not be something that would be well-received by those with a project time orientation, such as a capital projects' commissioning meeting, it was welcome in CampNet and IT groups. This is why James was a good candidate for this position. As William once noted outside of the CampNet meetings, "this is why people like James are so valuable because he has all that expertise in the infrastructure and because he knows who to call on the Central UWIT side."

While this work is specific to a case in Higher Education, the findings can be generalized across the management IoT in building and infrastructure. As the built environment becomes more digitized, and IoT systems become more prevalent, there will be a need for increasing collaboration and integration across Facilities, IT, and Capital Projects. Understanding disciplinary differences in general, and time orientations specifically will be critical to effective management of these devices and systems. Given the nature of the artifacts they are managing – buildings and infrastructure (longer time spans) and information technology (shorter time spans) – interdisciplinary teams will need new ways to manage the tensions and conflicts that emerge in time spans and time orientations in planning and management of these artifacts. In this paper we contribute to the construction management and facilities management literatures by analyzing how the concept of time orientations plays out in the management of IoT systems in campus infrastructure contexts and how the temporal boundary spanner can mitigate and management tensions and paradoxes that these temporal orientations create.

7. CONCLUSION

This paper reports on ethnographic research to study the complex work of implementing and managing IoT technologies in higher education campus settings. This ethnography is illustrative of why disciplinary difference matters in infrastructure management. In this ethnography we found tensions related to time orientations of different teams and different disciplines in the hybrid organization of a higher education campus owner organization. In this case, different teams worked on sustaining operations such as facilities management and IT infrastructure alongside other teams focus on project management of new construction and renovations. The results of this study suggest that different time orientations such as the relatively long-time scales associated with the management of buildings and infrastructure and relatively short time scales of IT hardware and software creates tensions in the management of shared IT infrastructures such as networks, in this case CampNet, a shared network resource that supports connecting IoT devices and systems to the internet. Different time orientations impacted the ways that these practitioners thought about artifacts, tasks, and planning. The findings are three-fold. First, the different disciplines of Facilities, IT, and Capital Projects have different time orientations that create tensions in the management of shared IT infrastructure such as a network. Second, these different time orientations created what we call the paradox of lost things. If they sped up the work they lost things, but if they slowed down, they lost other things. The choices for network management were not clear and the team had to navigate the constraints and work around the limitations. Finally, we conclude that management of IoT in the build environment will require temporal boundary spanners and interdisciplinary teams who have awareness of different time orientations and tools to manage the challenges of limited resources and the paradox of lost things. In particular, temporal boundary spanners can take on roles of gathering and sharing technical needs and values between different disciplines with different time scales. Future IoT management will require diverse teams with managers who have the ability to work through the complexity that arises over time with different time scales and time orientations that impact shared IT resources.

ACKNOWLEDGEMENTS

This is an extended and updated version of one of the best papers presented initially at CONVR 2022 organized and led by Prof. Chansik Park of Chung Ang University in Seoul, Korea.



This material is based upon work supported by the National Science Foundation (NSF #1932769, "SaTC: CORE: Medium: Knowledge Work and Coordination to Improve O&M and IT Collaboration to Keep Our Buildings Smart AND Secure.")

The authors wish to thank our research team colleagues Jessica Beyer and Chuck Benson for their partnership in this project and all of the team members we work with.

REFERENCES

- Battilana, J., Besharov, M., & Mitzinneck, B. (2017). On hybrids and hybrid organizing: A review and roadmap for future research. *The SAGE Handbook of Organizational Institutionalism*, 2, 133–169.
- Benson, J. K. (1977). Organizations: A Dialectical View. *Administrative Science Quarterly*, Vol. 22, No. 1, 1–21. <https://doi.org/10.2307/2391741>
- Di Marco, M. K., Taylor, J. E., & Alin, P. (2010). Emergence and Role of Cultural Boundary Spanners in Global Engineering Project Networks. *Journal of Management in Engineering*, Vol. 26, No. 3, 123–132. [https://doi.org/10.1061/\(ASCE\)ME.1943-5479.0000019](https://doi.org/10.1061/(ASCE)ME.1943-5479.0000019)
- Haas, A. (2015). Crowding at the frontier: Boundary spanners, gatekeepers and knowledge brokers. *Journal of Knowledge Management*, Vol. 19, No. 5, 1029–1047. <https://doi.org/10.1108/JKM-01-2015-0036>
- Honeywell, (2021) "Protecting Operational Technology in Facilities from Cyber Threats: Constraints and Realities," Georgia: Honeywell International, <https://buildings.honeywell.com/us/en/lp/protecting-operational-technology-in-facilities-from-cyber-threats>.
- Jesiek, B. K., Mazzurco, A., Buswell, N. T., and Thompson, J. D. (2018) Boundary Spanning and Engineering: A Qualitative Systematic Review. *Journal of Engineering Education* Vol. 107, No. 3: 380–413. <https://doi.org/10.1002/jee.20219>.
- Karasti, H., Baker, K. S., & Millerand, F. (2010). Infrastructure Time: Long-term Matters in Collaborative Development. *Computer Supported Cooperative Work (CSCW)*, 19(3–4), 377–415. <https://doi.org/10.1007/s10606-010-9113-z>
- Marrone, J. A. (2010). Team Boundary Spanning: A Multilevel Review of Past Research and Proposals for the Future. *Journal of Management*, 36(4), 911–940. <https://doi.org/10.1177/0149206309353945>
- Orlikowski, W. J., & Yates, J. (2002). It's About Time: Temporal Structuring in Organizations. *Organization Science*, 13(6), 684–700. <https://doi.org/10.1287/orsc.13.6.684.501>
- Reddy, M. C., Dourish, P., & Pratt, W. (2006). Temporality in Medical Work: Time also Matters. *Computer Supported Cooperative Work (CSCW)*, 15(1), 29–53. <https://doi.org/10.1007/s10606-005-9010-z>
- Ribes, D., & Finholt, T. A. (2009). The Long Now of Technology Infrastructure: Articulating Tensions in Development. *Journal of the Association for Information Systems*, 10(5), 375–398. bth.
- Schade, J., Olofsson, T., & Schreyer, M. (2011). Decision-making in a model-based design process. *Construction Management and Economics*, 29(4), 371–382. <https://doi.org/10.1080/01446193.2011.552510>
- Smith, W. K., & Besharov, M. L. (2019). Bowing before Dual Gods: How Structured Flexibility Sustains Organizational Hybridity. *Administrative Science Quarterly*, 64(1), 1–44. <https://doi.org/10.1177/0001839217750826>
- Stjerne, I. S., Söderlund, J., & Minbaeva, D. (2019). Crossing Times: Temporal Boundary-Spanning Practices in Interorganizational Projects. *International Journal of Project Management* 37(2), 347–65. <https://doi.org/10.1016/j.ijproman.2018.09.004>.
- Steinhardt, S. B., & Jackson, S. J. (2015). Anticipation Work: Cultivating Vision in Collective Practice. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 443–453. <https://doi.org/10.1145/2675133.2675298>

