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

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

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

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

ABSTRACT: *The adoption of Internet of Things is growing 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 Campus Infrastructure, Information Technology, and Campus 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. However, 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 and IT systems. In this paper, we explore how these time orientations lead to tensions and clashes in the types of technologies owners select to implement, integrating new technologies into existing systems, and the challenges 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.*

KEYWORDS: *Internet of Things, Operations, Time Orientations, Organizational Issues*

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 – the time scales that individuals think about and work within. While the field of project management deals extensively with the management of time as scheduling is a fundamental practice, one underexplored aspect is the challenges of managing across different temporal orientations such as when facilities owners manage technology within the context of facilities management. In our analysis, we identify three main time orientations related to Internet of Things (IoT) in a facilities management context: Campus Infrastructure, Information Technology, and Capital Projects.

The first category of time orientations we refer to relates to the management of campus infrastructure, which includes buildings, utilities, landscaping, walkways, and transportation infrastructure. The facilities managers are responsible for the maintenance and operational conditions of the campus infrastructure. Buildings can have a life span of 50 to 100 years. Roads, walkways, and utilities are maintained over 20 - 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 - 40 years. The timeframes for facilities managers as they manage infrastructures 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.

By contrast, information technology (IT) experiences almost constant change and flux. Computers change annually with most desktop computers being upgraded in 3- 5 years 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 are constantly improving and large institutional owners have to make decisions about upgrades on 3-5 year timeframes. When systems are not updated, they begin to feel archaic after 3- 5 years timeframes and some vendors are moving towards automatic hardware and software updates. Cloud computing is enabling even faster update cycles for file sharing and data processing. IT employees think on 2-3 month 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 can last 9-12 months, and the construction from 1 - 2 years for a typical project. 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 workers. They work to bring in the latest technologies and building systems into the buildings they design as well as stay current with design trends. 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. New projects bring new IT challenges to the facilities management team as they introduce emerging Internet of Things technologies that are designed to improve building performance.

In this paper we explore the dynamics and challenges that emerge when facility owner organizations grapple with and across 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 or role agendas related to IT network security, facilities management, and capital projects. In turn, these two groups need to coordinate and collaborate with the capital project endeavor. 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.

2. REVIEW OF LITERATURE

First, we review the context of hybrid organizations and then introduce the concept of time orientations. 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 discipline of capital projects. Time orientations both shape and emerge from disciplinary culture, which in turn 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.

2.1 The organizational problem: hybrid organization

In this work, we studied large organizations that consist of multiple divisions, multiple teams, 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). In this research paper, we look at a large organization that has both project-based work in the form of new construction projects alongside operational work in the maintenance 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).

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 are temporal scales that relate to a group's understanding of meaning and value, and their interests, aims, and motivations (Karasti et al., 2010). Temporal orientations are socially objective understandings of time that set up 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 it 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 managers, and capital projects. 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/channel expectations of future, design pathways into these expectations/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 management, IT network and security specialists, and capital projects.

3. Methodology

This paper reports results from a 3-year study funded by the National Science Foundation in the US. This study includes a 2-year in-depth ethnography of a higher education campus (120 hours with 178,933 words of notes), 40 national interviews, and 5 case studies of higher education organizations. This paper focuses on findings from the ethnographic observations in 2020, when we observed meetings that included staff from both IT and facilities, where these staff members working on IoT implementation and management. Due to COVID lock down procedures, a majority of these meetings 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 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 staff, 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, and Vince, an IT specialist who led a Facilities-oriented Business Innovation and Technology (BIT) group. 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 infrastructure management, IT management, and capital projects. Within the meetings, two orientations come into play: an IT orientation, and a facilities management orientation. 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. A third orientation then is introduced when capital projects add new systems to the existing network. This project orientation creates timing and logistics challenges for how, when, and where the new project systems are connected to new or old networks.

4.1 January, 2020 (before COVID Lockdowns begin 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 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 is a matter of security. Michelle (IT), who speaks in highly technical terms stated that CampNet “the island, as long as it stays and island will only hurt us.” The group seems to recognize that there are different language/vocabulary between the members of the group and so some translation is necessary. The comfort with an island network is one that is 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 does 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?

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, has 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 reminds the group that there are in fact two CampNets–the old and new. Glen calls for an investigation into what is on old CampNet so that they know why they can’t move on to new CampNet completely. This is a seemingly simple request that proves hard to accomplish. This is where the first time orientation becomes clear: the long timelines of facilities management means that devices have accrued on the CampNet over time, like crustaceans on an ocean pier, and no one really knows what all is connected, and what the requirements of those connections are.

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 is now lost and has to be documented anew. The discussion around CampNet transition–from old to new–focused on what that might entail and what risks were involved. For some systems the transition was relatively easy and risk free, but there is always a chance that in making a big transition there is a "big bang" as Vince warned and things go really wrong. 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.

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 is 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 can impact what the campus organization is able to do as far as their own network is concerned. In addition to vendors, IT wanted to use state of the art tools like remote dashboards to manage and monitor the systems, requiring that the new CampNet be less of an island. The IT time orientation put pressure on the team to continually change.

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 is concerned) focused on a new central utility building (a recent capital project that will 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) is 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 connected to a network. Lost things makes IT very nervous.

The team tries 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 emerges again as an important consideration when making networking decisions because the assumption is that with the passage of time the networks will become more and more populated with new devices and there is a need to build the network architecture with foresight into how things will develop. However, it is hard for the staff to anticipate what that will look like. To end this meeting the leader, Dave (IT), introduced an initiative to inventory the systems and devices on CampNet in order to increase awareness of the scope of the network, track its growth, and manage ownership. This is 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 interface with the campus networks.

4.3 April 2020

The meeting started with a discussion of ways to track devices on the network as a means for improving security. This was particularly concerning to Dave (IT) as he sees trends for a future with a lot of growth in networked systems. Dave (IT) talks about CampNet issues as "whack a mole" and the departure of a key staff member in facilities is brought up as a risk area because this person had "owned" a lot of lighting controls in facilities, but now ownership is up in the air. Michelle (IT) brings up a wiki shared with IT that includes drawings of future lighting control plans but this is 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 problem really is. This sparks a conversation about who "owns" what and to what degree people know what is on CampNet and what is not.

4.4 June 2020

This meeting was the first time we see a conversation about the timing of this groups' involvement in the building process. Based on the recognition that systems get set up in new building projects in less than ideal ways (from this groups' perspective) there is 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 allows someone from CampNet group to catch these issues ahead of time. It is suggested that this might be a cybersecurity review process or making this a step in the submittal process. They define the problem as not having an "owner" to speak to – no real point of contact for some systems (i.e., lighting controls). But it is an issue beyond lighting controls, as Nick, the vendor, reminds everyone, this is just the most obvious one right now. The question of how to demand compliance with their network architecture is the challenge.

There was also a discussion about the problem with dual CampNet (new and old) that are both needed in new buildings but don't work well together. Old CampNet connects legacy systems making it impossible to break-up with in time for new buildings to open. This is at least partially a problem blamed on the design-build team because they have failed to consider cybersecurity risk early enough to have a meaningful impact on design. Here we see 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.

There are two timing issues for coordinating between the building teams and IT. First, Contractors put up devices to measure commissioning data that do not get securely networked and then are often left in the building without anyone in IT/facilities knowing about them. This is a cybersecurity issue and has to do with the timescale that design-build teams generally work on as opposed to IT/facilities teams. It also contributes to the concern about lost things on campus on the networks. Second, cleaning IT closets is another issue. IT (and maybe facilities) need access to closets and for them to be cleaned earlier than is usual. This is referred to as “early service” and there is a communication infrastructure team that works on requests of this nature, but it seems from the CampNet meeting that in reality this does not happen early enough in the building commissioning.

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, 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 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 would 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.

4.6 August 2020

The main issue at hand was the reconfiguration of CampNet that was being prompted by the Bennington system [pseudonym] – there was concern that reconfiguring the network architecture for a single system was not a great strategy, but others suggested it is an architectural change that they have wanted to do for a while beyond this system. They discuss using firewall policies to govern the system on CampNet. 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 are continually having new systems added through capital projects. However, this was in tension with the need for a controlled phased approach that would be more secure and would give them the time to figure out what they have, what might be missing, and what devices need to be assigned ownership. This tension is 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 project which is undesirable to many who’s job it was to make the building occupiable. Others argue that this time pressure as a “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? So 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 over years), relatively shorter timelines of new projects (adding new devices to the network), and the extremely short timelines of IT (system changes and cybersecurity threats change monthly if not weekly). 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 will be new CampNet only since this will result in losing the ability to communicate with some systems from old CampNet - like radios. This is where we see 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 to the older system, further entrenching the old CampNet infrastructure. But, if they speed up, they lose some of the functionality of the old CampNet and devices and endpoints that were not documented prior to migration. Either way, they lose things. This issue is a series of trade offs and selecting what will be lost or compromised.

In this meeting, an interesting discussion happened about the strategy for segmentation. Because of the paradox, it was largely driven by who makes these decisions. Since there were multiple time orientations present in the organization, it would be important that those time orientations are all present. The problem as some in the meeting saw it was that from their disciplinary perspective they saw CampNet as "sacred" and "warrants protection". There was concern that those who are newly gaining access to CampNet will 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 is today. This is part of the accrual of systems and the longer-term scale management of information infrastructure as it supports the longer-term 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. 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 is 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 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.

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 coming online as these tensions continued to be not fully resolved.

5. 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 disciples 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. It is important to understand these organizational ramifications in planning for and organizing the management of facilities and infrastructure.

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 are misaligned and often in tension. When working together, these teams discovered unreconcilable 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, and their priority was to maintain the operations of the buildings. To that end they sought to connect devices and systems 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. However, the IT perspective included more short time scale issues like system updates and cybersecurity. IT ask for more record keeping around what devices and systems were connected, when, and by whom as they interact 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 focuses on a single building and getting that building online for the end users. Taken together, the long timeframe of facilities has resulted in a CampNet environment wherein many devices and systems are connected, some of which are 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 the CampNet needed to be closely managed. The tension between the need to connect and the risk of connections is a main theme throughout. The 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).

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 which were historically connected to the old CampNet because they did not have a record of these devices 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 need 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 and IT and capital projects personnel as they navigated the technical challenges they faced 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 make 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. As the built environment becomes more digitized, and IoT systems become more prevalent, there will be a need for 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.

6. 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, the hybrid nature of the organization meant that different teams work on sustaining operations such as facilities management and IT infrastructure alongside other teams who manage new construction and renovation projects. 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 updates 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 were associated with different disciplines in terms of the ways that these practioners think 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 interdisciplinary teams who have awareness of different time orientations and tools to manage the challenges of limited resources and the paradox of lost things. 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.

7. 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*, *22*(1), 1–21. https://doi.org/10.2307/2391741

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

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

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

Acknowledgements: 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.