Question Asked	Answer Given
Cyber Certification good idea..	yes it is, at least awarness training for staff geared towards ICS and OT systems
What tools are available to secure the engineering workstations and other superviory devices on the OT network that are targeted by Hackers to gain access to the IT network?	We are moving towards a zero-trust model for remote access to these systems, at the same time restricting the system workstations access to public facing internet connections. The traditional IT tolls are way too intrusive and can cause more harm than good, so a passive approach is needed in the OT environment.
How do we stop phishing emails from having the ability of gaining access to the network (even a secured network) when credentials are stolen.	Keeping email off of critical systems and out of critical networks by segmentation. We also recommend a strong cybersecurity awareness training program, including simulated phishing campaigns for all employees and rdepartmants. Unfortunately, once a phishing email is acted upon on one of these critical systems, the cat is out of the bag so to speak.
What do see and fell about VM and Virtulization of OT systems - Considering there is no regulations at this time	Histroically OT system have not been virtualized but we have seen an increase over the past few years. They can be deployed within the VM environment so long as the right policies and procedures are in place to ensure security has been taken into account. It si important to understand the OT policies will be different from IT policies.
We are now seeing OT systems move to VMware and A VMware based enviroment - What I have seen - there are NO OT Cyber-security requlations for OT systems in the Cloud or OT systems being in VM enviroments - There is IT regulation, but not OT - there is not 800-XXX for OT systems security as a standard for NIST, PCI. IEEE , or CISA requlations	You're right, there is a lack of regulations for OT systems (internationally and local jusrisdictional regs). (CS)2AI has active participants that are helping to drive the industry.
When your systems are behind a corporate firewall, how vulnerable are they if common access protection is in place? Usually the OT systems are on a separate VLAN invisible by the corporate insiders and users.	There is no common access method, but its the unknown. But typical firewalls don't prevent inbound threats looking for connections. Firewalls sill allow traffice, but just under a set of rules. In most cases the OT systems are isolated on a separate network away from the corporate network, but are common for CCTV, card access and the building automation systems in the building. If the bad actor can compromise any of those critical systems with malware / ransomware. They need not go any further.
There is a great amount of hesitance of IT department persons to acknowledge OT systems in their buildings. Sometimes they are not even aware that OT is running on their backbone. We have found that due to older technology networking equipment being less sophisticated, need a VLAN OT network that does not traffic huge amounts of data so that the older technology can keep up without going off line as described by the last session. Of course the IT department hesitance extends to maintenance of the OT system as well, so sometimes education is warranted to keep everyone in sync and secure.	Thanks for the input!
Do you see Building Cyber Security certification similar to LEED for sustainability but from here: https://buildingcybersecurity.org/	Building Cybersecurity.org is specifially working on a certification for building cybersecurity that is LEED like.
Where are we are what could be improved in terms of cyber threat intelligence in the context of building control systems?	We have developed policies for the OT environment that relies on the NIST framework The Core includes five high level functions: Identify, Protect, Detect, Respond, and Recover.
**Where are we in terms of cyber threat intelligence and what could be improved in the context of building control systems?	There are some great options for threat monitoring entering the OT space for monitoring that are tailored for the delicate needs of those systems.
My team continues to see owners and occupants refuse to recognize cybersecurity as a threat to building control systems with owners that claim they will just trigger their cyber insurance when something happens... does the panel forsee upcoming changes to the market driven by insurance companies requiring proof of mitigations or other methods to limit the payouts?	There is currently in the works groups which include large insurance companies to address this. Right now there is nothing specific but stay tuned by the end of the year you will begin to hear more about this.

In lieu of a 600% increase of hacks from 2017 to 2020 and the implemention of the counter measures that would ensue to prevent them in the future. I am curious as to if any of those counter measures might be or include vendor backup commitments that would be part of the initial bid process prior to the commissioning of the building itself?	yes, potentially these counter measures and data backups could be included as part of an initial bid. It will be important to understand the actual capabilities the vendor is providing to ensure it meeting all cyber requirements.
For the "bomb in the building" segment - did they calculate the "cost".. ie, did they have to credit tenants for loss or was there an insurance claim for BI?	No, to my knowedge the lease covered emergencies and the time out of the building was short enough that it didn't approach the threshold of any kind of credit.
As a property manager, what cyber security practices are IOT vendors currently doing in their next gen equipment that you already really like? What cyber security would like to see IOT devices do more of?	Manufacturers are working to address risks in their products. However, the company that installs and programming the system rarely does their part.
What support points do you have to make a business case to hire a/an analyst(s) to regularly review logs, and alarms? Seems like this is common areas during an intrusion.	I would say that the IoT world is ready and is probably preparing for the next round of cybersecurity. The BAS/OT world is evolving into the cyber world but probably require some pushing to get them to where they need to get to
There are a lot of certs and vendors starting up and established. What are the most highly regarded industry and standards certifications for BAS vendors to possess and why?	Currently there are none specific to be building control systems. However BuildingCybersecurity.org is working on cybersecurity framework built on 800-53, 62443, and 27001.
Do you guys think the Building Automation OT/IOT industry ready or preparing for the next round of cybersecurity regs and certifications like the new CMMC for DOD providers?	Currently in the works is a framework specifically for building control systems. It is based on 800-53, 62443, 27001. The group is a crossmix of manufacturers, integrators, insurance, and legal. It will take a while to get it integrated into the fabric of building control system industry. The group is called BuildingCybersecurity.org.
What are the suggested methods of air gaping the monitoring network?	A zero-trust approach is the best, at the very lest place these systems behind a firewall, require VPN with multi factored authentication to access remotely. Use unidirectional diodes if possible. Never place directly on the internet.
What are the suggested methods to secure card access systems?	Card Access systems, like any other control systems, require robust network security as well as vendor access policies that begin to mitigate the risks.
U think building staff can be complacent due to incompetency or just lack of knowledge?	it's a knowledge gap in 95% of the cases we have seen. that space is playing catch up after years of bad practices.
Are there no configuration backup for that credential at all?	unfortunately no, as incredible as it sounds
What are the threat hunting tools that are designed specifically for protecting building systems?	The online tools are Censys.io and Shodan.io. There is a BACnet explore available free of charge from SourceForge call YABE (Yet another BACnet explorer)
Why don't building owners hiring firms that can help them with functional specifications, configuration requirements etc for the control system components themselves not just the network stuff?	The short answer is they should. The reality is the end user/building system owner has not fully embraced.
Why don't building owners hiring firms that can help them with functional specifications, configuration requirements etc for the control system components themselves not just the network stuff?	I think is building owners can't fix things they may not be aware of... You don't know what you don't know. As a matter of fact, Intelligent Buildings provides those advisory services to its customers.
Has the real estate industry looked at ISA/IEC 62443 3-3, 4-2, 2-1, 2-3, 2-4, 3-2 etc to create sector specific basic design requirements specificiations for building control systems?	As a matter of fact currently there is a group called BuildingCybersecurity.org is building a framework using 62443, 27001, and 800-53.
In all of these smart building initiatives has the real estate sector considered creating a smart secure maturity model and grading systems that includes functional design security requirements at each maturity level?	it is an emerging need and groups have started that process similar to the development of LEED or WELL
Have building owners looked at secure buildings as an ammenity service?	Interesting take, we haven't seen this before but it is in the interest of the building owner to secure their building themselves.
If the new NIST SP 800-53r5 controls catelog controls had been enacted, would the hack scenarios all have been prevented? Seems like this controls catelog is one of the best condensed listing of controls to at least start with for IIoT and Building control systems cybersecurity hardening, do you agree?	Good question and observation. The problem is the building control system industry has had no guidelines/standards. The industry has begin to embrace cybersecurity before you can give them a ton of guidelines.
Do you think that HR 1668 IoT Cybersecurity Improvement Act of 2020 will help drive the commercial industry to adopt the same standards that are meant to be the Federal standards?	Currently there is a group called BuildingCyberSecurity.org that is building a framework on 800-53, 62443, and 27001. These will be mapped together specifically for building systems.
Was the network traffic from the attacker disguised in this case? If so how?	Because building control system networks are rarely monitored there was no indication.

The question should be: Why are OT vendors creating IP based solutions incapable of being fully used within IT systems that they know use tools for scanning and security monitoring? It feels as though OT vendors want to jump on IT systems for convenience without due diligence to ensure they actually work within it.	The industry is slowly making headway in the products they are delivering, especially when their products become vulnerable to a breach or exploit. The biggest players in the OT control system space are finally getting with the program.
Regarding risk for each of the attacks - were insurance claims filed? How can impacts to insurance cyber, property or casualty policies drive investments in better ICS/BMS/OT protections?	Great question. The insurance industry is just now beginning to address the risks and impacts of buidling control systems.
are there any sensor devices on the market to detect employees with covid symptoms?	There are video analytic solutions that can detect raised temp
Are there any data sources or reports that can provide case studies or metrics on data breaches which originated from OT networks and resulted in unauthorized access to the enterprise IT network?Are there any data sources or reports that can provide metrics on data breaches which originated from OT networks and resulted in unauthorized access to the enterprise IT network?	Because building control system hacks don't involve personal information. So therefore there is no regulatory need to report them. The industry is getting better at collecting data.
The 2013 Target data breach is often cited as a watershed moment in how organizations treat third-party vendors, especially HVAC vendors and other building systems. What other breaches should organizations be aware of, and what are the lessons to take away?	The vast majority of cyber incidents in operational systems are, unfortunately, not publicized. Organizations deal with them privately which is why the most relevant examples are only known within the industry. Some examples have been shared here today.
As part of your vendor selection, do you consider how willing the manufactuer is willing to share securty issues / patches with end users vs only integrators?	very, thats something else you will want to put in writing in the software service agreements, i.e. vulnerability notifications
How much do you see multi-tenant owners/operators having to start forcing cyber controls onto TI improvements? Example would be dynamic lighting controls (Lutron!) with default wireless credentials being very commonly installed into a tenant space. Not purchased by the building, not connected to the building, but the building ends up supporting it long term.	not really seeing it yet... but we are forcing the issue via vendor compliance audits
Was that an issue of running accounts on a specific user level instead of ustilizing service accounts?	It was a mix. the individual had high level / admin access across many facilities and systems due to their position. But due to that access and some errors in setup, when those roles were deleted, there were multiple systems dependent on his access. Policy and proceedure over Technical causes.
Was their network segmentation between the IT and OT network? How did they protect the OT network after everythong was put back online?	Yes, there was segmentation, and they changed strict operational policies to protect from the systems.
I recall a discussion mentioning a data diode for these control systems to handle the security	There are instances where one-way communication is used to transfer data. However, use of data diodes is not common.
How much mature is the IoT to have an out of band management?	Overall, I'd say Out of band management is not mature in the OT / IoT space.
How much are the vendors emphasizing on the security as compared to the automation aspects. We have seen that most of the OT vendors primarily focus on the functionality and does not take account of the security aspects.	There has been a significant increase in vendor focus on security in recent years. Vendors are much more aware of the cyber risks posed and are continuously developing their cyber best practices to secure their systems. However, the industry practice for procurement has generally been lowest bid, which is partly responsible for the mess that the industry found itself it. If this still happens, this is where corners will be cut, and not all of the cyber best practices will be followed.
I would be interested in the statistics of any litigations/disputes lead by a system failure	That would be an interesting metric to track
Do we have a fail safe concept in the BMS e.g. incase of a cyber attach which presents a DoS or other related incidents, the BMS goes to a manual mode that still keeps the life moving?	yes this is usually the default. BMS goes into fail safe mode or manual mode where building operators control the system manually.
Has any hacker or group been caught or claimed making these attacks?	No.
Is insider threat the biggest risk that exists for companies?	yes one of the biggest, and most cases it's not even malicious. Phishing and ransomware are usually successful due to user error, not intentional action by insiders.
Excellent video! Just looking at the statistics in the video….given the resistance/inability to change in OT environment OR the change duty cycle measure in years, and given OT enviornments are connected to the internet - how does an OT environment expect to survive without damage/loss due to hacking attacks if they don't change or add cybersecurity platforms?	At a minimum, begin to add security platforms and policies where most vunerable.
When the first engineer had to have the reinstall, where was the questioning attitude to ask why?	There was mouse moment on screen mostly.
Covid19 is impacting companies and the industries, What's policies are implementing for preventing attacks based on fear of people respecting covid-19?	Good question. With the threats to business that the pandemic has posed for the world, strengthening access policies, vistor access and regular tenant access are critical. These should dovetail with strengthening the cybersecurity posture of the company to be sure to address all aspects of the threats in the our 'new world'.

How are you gentlemen addressing IoT being put in the environment without the envolvment of the Information Technology and Security teams. I have worked in these environments and this happens regularly.	Ideally IT should be involved but in the many cases where deployments did not involve IT there are solutions out there to secure these systems like implementing a secure network overlay that implements a zero trust architecture.
How are you gentlemen addressing IoT being put in the environment without the envolvment of the Information Technology and Security teams. I have worked in these environments and this happens regularly.	The large majority of systems are on a network that was put in by a bulding system contractor who don't know much about secure networking. Once a system is in place buildingmanagment is not willing to make major changes. There is product such Tempered Networks that doesn't require major changes.
do you not think there should be honey pots hidden on large networks so something intelligent can highlight abnormal activity?	Absolutely
The firewall is a good start but doesn't it really need an intelligent logging system behind it - otherwise how do you know if something is happening rather than a black box in the corner	You're right, A firewall is never enough. Especially when you need to know what happend, and enabling logging on each system running is critical to controlling configurations AND forensically after an event.
When temperatures out of control cannot we use thermostat based mechanical alarms to respond faster to attacks and disconnecting network access?	There are some monitoring platforms that can automatically detect the treats and remove the device from public access while allowing it to continue to function as normally until the threat can be investigated.
When temperatures out of control cannot we use thermostat based mechanical alarms to respond faster to attacks and disconnecting network access?	-In theory it may be possible. But for most buildings that have a large footprint, multiple points of connection, hundreds of thermostat or temperature sensors, the scale of deploying such a mechanical solution might be too difficult to implement.
What does (CS)2AI think about SBOM (Software Bill of Materials)?	September 15th, there will be a symposium on suppy chain cyber security including SBOM! Tune in!
There has been an increase in the focus on the supply chain risk. What is the future for facility supply chain risks?	As it stands now there is rarely any focus on building system devices supply chain risks. At this stage there is a awareness growing.
How are you currently managing non-personal entity (NPE) devices in building automation?	Sadly once a device has be installed and the network setup there is little to no management of any part of the system. Just as in IT, asset management the start that must happen.
There are a lot of best practices and security controls - lot of documents that are publicy available (sometimes a bit of information overlad). what are the available workforce development tools for building owners?	Sadly the majority of the industry does not follow even basic best practice. That is changing. There organizations that working to educate the industry.
What can building owners do to fix the communication gaps between the management (decision makers) and the technical teams and vice versa? How to relatively quantify (value proposition) return-on-investment (ROI) vs. cyber hygiene?	I know it sounds like a pat answer but because the industry is in its infancy it starts with education.
In case of buildings ICS, where does cybersecuity vs. cyberresiliency comes into scope? whats the difference between them in the context of buidling ICS?	The building control industry is in its infancy so the first steps developing basic best practices and education to understand the importance.
In general, we see some tools that can help with identify, protect, detect functions of NIST CSF but not a whole lot of consistent well-shared information and tools around respond and recover. Any suggestions around tools that can help with respond and recover? current actions typicall involve reaching out to some external entities as part of response and recover. Thinking from a system-level or network-level autonomous response, if you have a list of technologies for folks to look at, that would be great	This is a great point. In many cases, the Respond and Recover steps requires extensive changes like network configuration, setup, policy development, monitoring tools, policy enforcement, organizational changes etc. In the worst case, the system may need replacement and so the steps require a more holistic approach at a system level response.
One theme I have been asked by customers in my industry (not building controls) is end of life technologies, patching, updating components. I would like to know what the intelligent building industry is doing to this, what are some best practices out there, are theree any stats on how much of the building components suppliers actually doing end of life support?	The usual process of patching and updating depends on the service or maintenance contract with the vendor. Some vendors are prompt in updates and patches whereas in other scenarios, where remote or auto updates are not possible, contractual conditions such as scheduled visits are when these updates take place. It is imperative for building owners to include contractual language that obligates the vendors to update and patch components while also enforcing this internally.

For a typical AAA-type commerical office building what is the typical range to secure the property? Choose whatever cost metrics that would be relevant such as cost per sqft and make any assumptions necessary--basically I'm curious to know what the typical cost for a basic setup would be and how much it can go to fully cost to secure an office building (knowing this will be a bit of a back of the napkin calculation).	Great question. Because of the variation from building to building and even system to system to even get in the ball park you have to know the most pervasive setups are configured. That being said, if the network is already following IT best practices the cost can be much lower than if the building system integrator setup the network with unmanaged switches.
I saw a lot of stats about cyber attacks on BAS/BMS is there a link to some of this information to help build out use cases	The stats were collected from several different sources. Some from public sources and others from private practice and observation. Please reach out to us separately and we can share more info!
Would you suggest creating a duplicate of all user accounts accessible by admins only before disabling them? To prevent these scenarios	Its better to have a policy in place to manage the users and their level of privledges assigned. if the system or device can utilize credential vaulting, thats also a way to go.
is that nearly 100% statistic concerned with DRP apply to BAS depts or the whole company...?	The traditional DRP planning provided by IP lacks the necessary steps and considerations needed by those systems. Especially a legacy building automation system.
how can DRP of BAS systems be integrated into the IT system with current IT policy and procedures....?	Specific DRP for BAS should be developed due to the nature of BAS. This policy must work in harmony with IT policies but with interoperability of the BAS in mind.
@James: working in a BAS section in the DRP playbook for the company is best ?	Yes we feel its best to create the DRP for the OT systems using the IT policy as a starting point. and crafted to suit OT needs
Found these two resources summarized below: Data Exposed of 35K BAS (Shodan 2019) Tenable Research (Jan 2019) found several zero-day vulnerabilities in the PremiSys access control system used by over 500 companies https://codecondo.com/security-vulnerabilities-facing-smart-buildings/ BCS Deep Study by Gjoko Krstic (Applied Risk) Vulnerabilities (100, 50CVEs): Default and hardcoded credentials, command injection, cross-site scripting (XSS), path traversal, unrestricted file upload, privilege escalation, authorization bypass, clear-text storage of passwords, cross-site request forgery (CSRF), arbitrary code execution, authentication bypass, information disclosure, open redirect, user enumeration, and backdoors Impact: 10 million people by a total compromise of critical residential and public facilities Duration: 1YR Brands: Computrols, Prima Systems, Nortek, and Optergy	Thank you for the information!
And: BAS Risk Report https://forescout.com/company/resources/how-secure-is-your-building-automation-system	Great stuff!
great sources for bldg fails (and safety risks): https://youtube.com/c/TomMunroCHI and SPIKES "Catch a Contractor"	Thanks! We will take a look at this
BAS should consider the automation BYoM (bring your own microncontroller),in using hobby controls such as Pi needs an inclusive? wholeistuc approach to asset visibility. (https://www.tomshardware.com/news/intel-nuc-security-flaws-advisory-vulnerabilities,https://www.cvedetails.com/vendor/19735/Raspberrypi.html, https://www.raspberrypi.org/blog/why-raspberry-pi-isnt-vulnerable-to-spectre-or-meltdown/, https://www.wmlcloud.com/news/the-truth-about-comparing-raspberry-pi-vs-intel-nuc/)	