BuildCentrix

CONSTRUCTION IN THE CLOUD

July 2022

SpecialProjects -

BIG REVENUE

© Can Stock Photo / peshkova

www.buildcentrix.com

SpecialProjects - BIG REVENUE

By / Jessica Kirby

© Can Stock Photo / peshkova

Most mechanical or multi-trade contractors have a “small projects” or “special projects” division from which smaller and/or simpler scope, primarily field-managed projects operate. These are the one-offs, the smaller custom jobs, and the ones that require a minimal team to operate.

“A lot of big construction companies have a special projects division, but these departments usually work outside the typical office staff, and they are not typically bid-design-construction type projects,” says James Beveridge, CEO of BuildCentrix (BCX). “The team goes to site, and the projects are usually retrofits, tenant improvements, and are usually in existing buildings or involve custom work.”

Special projects tend to be field and foreperson based. The foreperson does the takeoff, quotes the job, and runs the work. But although they are smaller in scope, special projects are, for a lot of companies, not so small when it comes to revenue. They’re lower cost—thanks to no VDC overhead—they typically have a faster turnaround, and they can contribute a significant amount of annual revenue.

Special projects are lower cost—thanks to no VDC overhead—they typically have a faster turnaround, and they can contribute a significant amount of annual revenue.

"In more and more companies, it is a higher profit margin style of work and a proportionally higher portion of revenue (20-30%) than a traditional bid and design because there is less overhead," Beveridge says. "Special projects are custom and tend to be smaller in scale. The bigger the project, the more breaks you are offering, so custom projects end up larger-ticket items at the end of the day."

For example, a company could be running a $5 million project and make $1 million in profit, while on a $50 million project, that company might make $500,000 in profit.

"These are amazing little divisions, and since they don't have a tremendous amount of office support they don't use a lot of modeling or tech," Beveridge says. "They require the ability to order from afar, build their own models, and get instant intelligence and costing, including labor, materials, and markups."

So, why don't they get a lot of attention?

"This is a common sense issue," Beveridge says. "It is an area of the company that shouldn't be ignored from a technology standpoint, but there was no purpose-built technology this division can use, until BCX Assembly Builder."

BCX Assembly Builder is costing, pricing, ordering, modeling, and fabrication baked into one tool. Special projects also get budgeted fabrication time, including labor information, so the user can generate a model that goes directly to the fabrication system and give financial data.

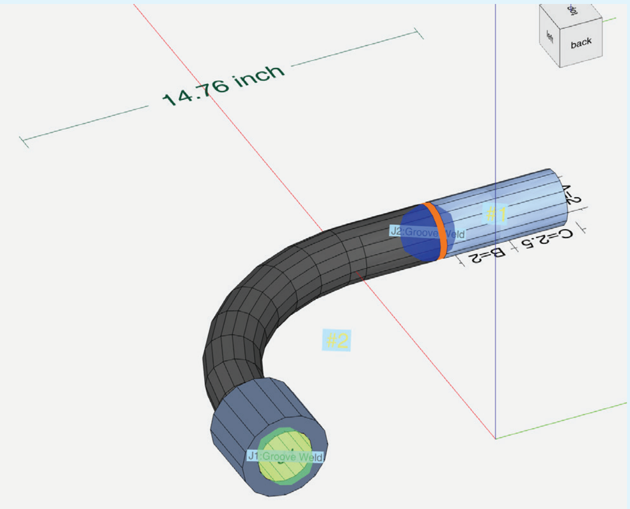
"We offer the only software that companies can use in the special projects division," Beveridge says. "We can build models and generate financials because these are fast-paced, mobile works, and we offer a way to use technology and streamline the process to be more efficient."

Learn more at *buildcentrix.com* ▪

BITS AND BYTES

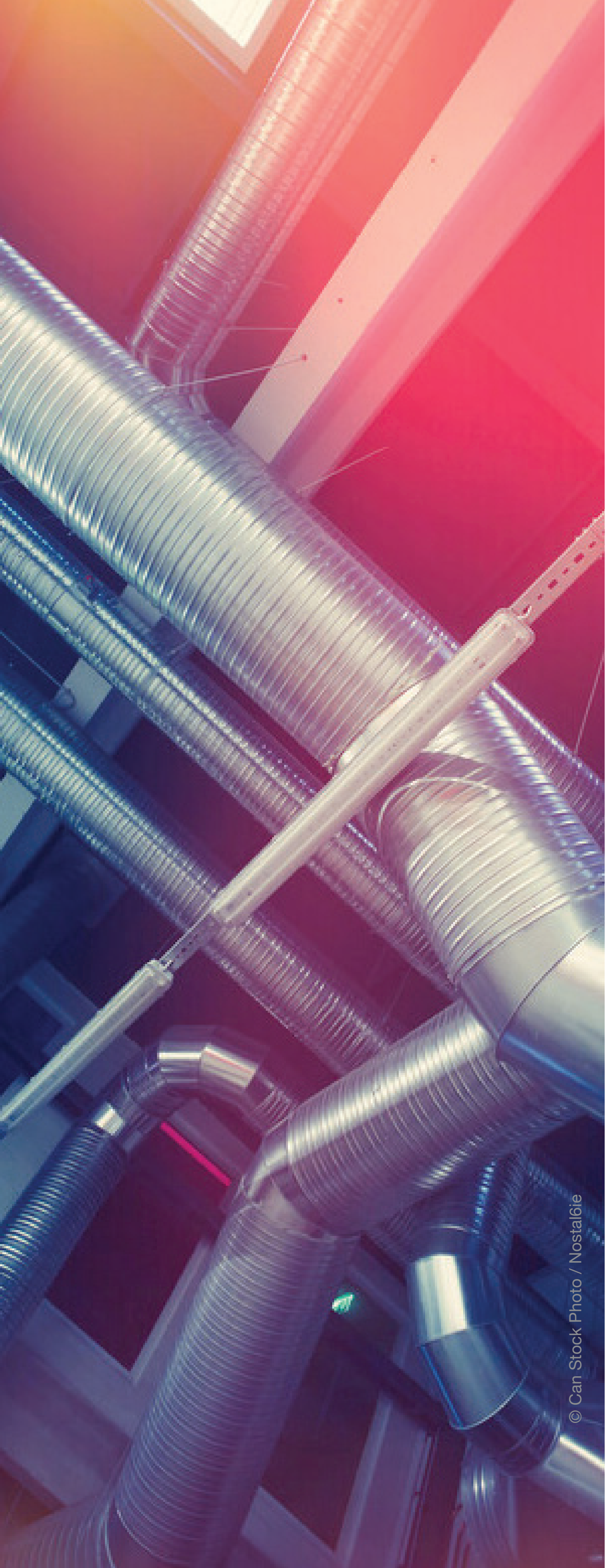
Auto-Calculate Weld Gaps

BCX Assembly Builder auto-calculates the weld gap on any applicable piping fittings. The weld gap is the space between certain material types to allow for a welded connection.



Your Order is in the Oven!

Field procurement should be like ordering pizza from a large chain. You should be able to keep track of your material as it moves through the fab shop. With BCX statusing and ease of use for field personnel, the field can track their material orders through the manufacturing process. The recipient receives a notification automatically (when the pizza is out of the oven) and also receives an automatic notification when shipped.


© Can Stock Photo / Nostalgie

HVAC and SECURITY

By / Jordan Whitehouse

In 2019, ASHRAE released the latest version of its handbook, and two of the more significant revisions were to chapters 41 and 61. Both deal with security—namely, cyber threats and contaminated air being introduced through HVAC and other building automation systems. Chapter 61 reviser Howard McKew says it is worth it for anyone involved with these systems to review the new information.

"Not a daily newscast ends without at least one story about a tragedy inside a building, adjacent to a building, or the potential threat made toward a building or its occupants," he wrote in an *Engineered Systems* article. "Like it or not, this is the environment the world is in, and so the building industry needs to wake up and recognize security must be an integral part of any building program."

These types of security threats are nothing new, of course, but they aren't going away, and some data suggests they could be on the rise. In 2016, Enterprise Strategy Group conducted a study that reported 54% of organizations surveyed had experienced at least one type of cybersecurity incident. No doubt some of those responsible got into the building's network via the HVAC system. Likewise, natural events like toxic fume accidents adjacent to buildings happen annually, as do purposeful acts of chemical terrorism.

Cybersecurity

Chapter 41 of the ASHRAE handbook contains a section on cybersecurity for building automation systems. It has a short introduction to cybersecurity, as well as tips on basic cybersecurity best practices and relevant guides and standards for more advanced users.

Michael Galler, a mechanical engineer at the National Institute of Standards and Technology, says that because building automation systems commonly use the same IT networks that are used for business purposes, operator workstations or remote connections into the building automation system can be a place to initiate an attack on anything connected to the network.

"It is less common that the building automation system itself is the focus of the attack, but that can happen," he says. "The concerns in this case would depend on the type of facility involved. A factory, a warehouse, a data center, and an office building would potentially all have different levels of concern and different types of vulnerabilities."

Johnson Controls Senior Product Manager Carol Lomonaco echoes this, and says that her biggest concern is that people don't take the security vulnerabilities at the server level serious enough.

"Some operators—and I'm not saying all—are sitting on the server that's really supposed to be the building operations server or the centre where you can see and troubleshoot everything, and they're out there shopping or getting their personal email and clicking on things they shouldn't be. That can be a big security risk, and it comes back to a lack of respect for that server."

The impact of not taking cybersecurity seriously can be huge, though it does depend on the type of facility and the type of threat.

"Malware might have negligible impact on the HVAC system, but a disastrous impact on the company," says Galler. "A malicious attacker who modifies a temperature setpoint could have a relatively minor impact on an office but a disastrous impact on a temperature-controlled storage facility. While the actual impact may vary greatly, there is always the potential for significant harm."

Air contamination

As for chapter 61 in the ASHRAE handbook, Howard McKew says it's all about the harmful air that could be introduced through HVAC systems and what can be done to stop it. The chapter starts with understanding what HVAC security requirements might be needed, followed by a discussion of risk evaluation, an overview of HVAC systems that can secure environmental health and safety, the modes of operation, commissioning, recommissioning, and maintenance management.

Smoke is the obvious big potential air contaminant, and HVAC engineers are very familiar with how to deal with it, says McKew. But there are lots of other risks that many people likely need more information about. Toxic fume incidents happening near buildings, such as railroad car accidents, is one, as are acts of terrorism wherein airborne chemicals are introduced at outdoor air intakes serving the HVAC systems.

And then there are the risks of harmful incidents happening within a building, such as the delivery of packages into mailrooms containing ricin and anthrax, or the accidental dissemination of harmful chemicals through a building after, for example, an explosion in a laboratory.

"The average HVAC person really doesn't get into all this; it's still a reactive responsibility to address the security issues," says McKew. "Most design engineers don't write their own automatic control sequence of operation. They'll have engineers provide them with a library of control diagrams and sequences of operation, and it makes it easy for them to just pull out the diagram and plop it on the drawing. But if you haven't written it, you may overlook something that is unique to your particular job that is not in the sequence."

What's to be done?

These chapters in the ASHRAE handbook aren't intended to be comprehensive security guides, but are instead meant to raise readers' awareness. And besides, says McKew, the HVAC design engineer doesn't have all of the solutions to these security issues, which is why the chapter also recommends hiring on a security consultant to deal with some or all of these threats.

Carol Lomonaco agrees that security consultants can be a big help, and adds that for cyber threats in particular, it's crucial to keep systems updated.

"You have to keep that building automation server up to date, and we just don't see everybody jumping to do that. Maybe it's for good reason—they don't have the budget—but some just have an old way of thinking, that 'Oh, these systems can last 20 years.' Well, that's your old system. Now you have a new system and you have to think about it differently."

Lomonaco's colleague Jason Christman would also add security monitoring to the list of preventative measures. He's the chief product security officer for global products at Johnson Controls.

"Most of these control system environments don't have a continuous security monitoring infrastructure in place to look for threats," he says. "You want to go in hardening these systems when you first install them, keeping them updated and patched over time, but also you want to be able to detect threats as they're happening so that you can stop them. And that's a big challenge across the industry."

Given all of these security challenges, a big question is how the industry is going to change to properly address them. Awareness is huge, McKew says, but there's actually big potential at the contractor level.

"Design engineers aren't going to take the lead on HVAC and security and cybersecurity, but contractors and the craftsmen who install these systems will," McKew says. "It could be the difference between them getting the job and not getting the job. And they have more to gain from that because the design part of a job is probably 10% of the whole project cost, and the contractor holds 90% of the project cost and the workforce is responsible for a quality job. I think that's why the good contractors and craftspersons are very proactive in raising questions and in positioning themselves to be the leaders in this." ■