FOOD
ENGINEERING
THE MAGAZINE FOR OPERATIONS AND MANUFACTURING MANAGEMENT

FEBRUARY 2025
Vol. 97, No. 2

Using Data to Drive Predictive Maintenance Strategies

How Does Your OT Cybersecurity Stack Up?

How Technology is Transforming Transportation Management

Optimizing Brewery CIP Systems

SPONSORED BY: RYCHIGER

A bnp media PUBLICATION

www.foodengineeringmag.com

AD INDEX

FOOD ENGINEERING

ADVERTISER // Contact Info

Further information on these companies can be found in the 2024 FOOD MASTER CATALOG. This index is published as a convenience. No liability is assumed for errors or omissions.

FA&M

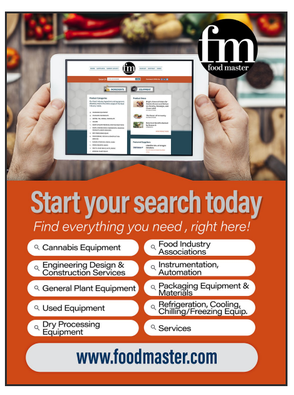
SEE OUR AD

VISIT OUR WEBSITE

Fisher Construction

SEE OUR AD

VISIT OUR WEBSITE



Food Master

SEE OUR AD

VISIT OUR WEBSITE

Food Master

SEE OUR AD

VISIT OUR WEBSITE

Lubriplate Lubricants Company

SEE OUR AD

VISIT OUR WEBSITE

PreciPak

SEE OUR AD

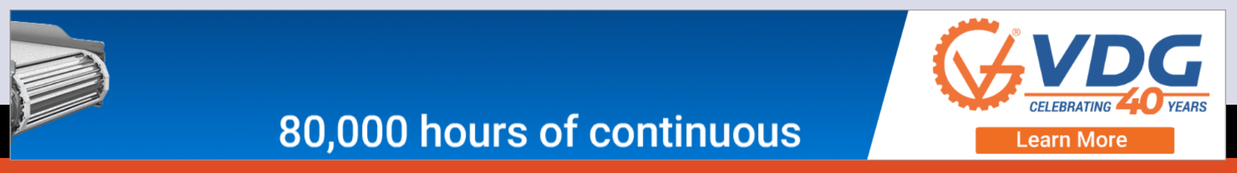
VISIT OUR WEBSITE

Rychiger

SEE OUR AD

VISIT OUR WEBSITE

NEXT ARTICLE



food master

Cannabis Ingredients

Save time finding what you're looking for anytime, anywhere!

- **Searchable by keyword and location**
- **Find detailed product information, videos, and more under any ★ company**
- **Submit a Request for Proposal (RFP) to suppliers of your choice with details on what you need with a click of a button**

FOOD ENGINEERING

FEBRUARY 2025
Vol. 97, No. 2

SCROLL DOWN

COVER STORY

Using Data to Drive Predictive Maintenance Strategies

Food and beverage manufacturers are discovering that machine learning is a vital ingredient in moving to predictive maintenance strategies. Larger food companies have the jump on digital transformations, but smaller companies are starting small and increasing spending to start the journey.

COLUMNS

Optimizing Brewery CIP Systems: Part 1

Though breweries face production and staffing challenges, there are opportunities for them to optimize operations — particularly through clean-in-place (CIP) systems. The first part of a two-part series highlights these challenges and the importance of "cleaning with intent."

How Technology is Transforming Transportation Management in Food Supply Chains

Transportation management systems have become crucial in supply chains to mitigate the impact of unexpected delays, improve communication between stakeholders, and optimize planning for more efficient logistics processes.

FEATURES

How Does Your OT Cybersecurity Stack Up? Tips for a Safer and More Secure Operation

Poor cybersecurity practices can result in disastrous consequences, though many incidents occur through simple mistakes or forgotten equipment settings. We point out some methods to help alleviate the human error that can result in disaster.

FEATURES

Adapting Drying and Curing Technology for Cannabis

Building on principles for drying and curing meat and cheese, Cannatrol has developed technology to control water activity in cannabis, leading to higher yields, improved terpene retention and reduced labor.

DEPARTMENTS

Editor's Note

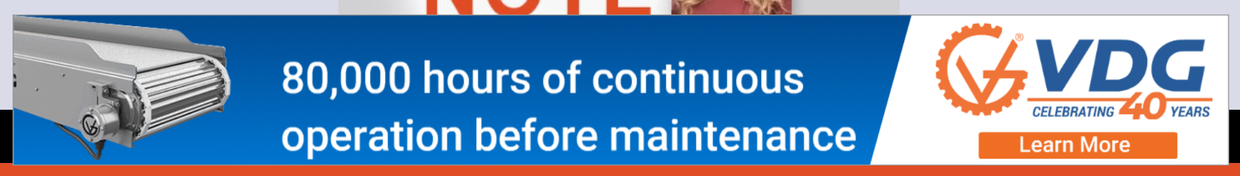
Regulatory Watch

New Plant Products

Ad Index

Masthead

NEXT ARTICLE



From the

What Will Happen with M&A in 2025?

LAST YEAR BROUGHT A HANDFUL OF HIGH-PROFILE ACQUISITIONS TO THE FOOD AND BEVERAGE SPACE, but what will 2025 bring?

We're off to an active start, but before we look at this year's acquisitions, let's recap a few from 2024.

FOOD ENGINEERING reported on at least 20 company and facility acquisitions in the food industry last year.

The largest — and likely the most talked about — is Mars' proposed acquisition of Cheez-It and Pop-Tarts maker Kellanova for $36 billion. Announced in August, the transaction is expected to close in the first half of this year. Once complete, Kellanova will become part of Mars Snacking.

In October, PepsiCo announced it would acquire Garza Food Ventures LLC, doing business as Siete Foods, for $1.2 billion. Siete Foods produces better-for-you tortillas, salsas, seasonings, sauces, cookies, snacks and more. This acquisition closed in January.

PepsiCo followed that announcement with plans to acquire the remaining 50% interest in Sabra Dipping Company, LLC and PepsiCo-Strauss Fresh Dips & Spreads International GmbH (Obela). Set to close by the end of last year, PepsiCo would become the sole owner of these companies, which make Sabra and Obela products.

In November, Lakeview Farms, a portfolio company of CapVest Partners LLP, revealed its plans to acquire the noosa yogurt brand from Campbell Soup Company. Lakeview Farms produces refrigerated desserts, dips, salsa, hummus and specialty products under several brands including Fresh Cravings, La Mexicana, Señor Rico and Salads of the Sea. This acquisition is expected to close in the first quarter of this year.

These acquisitions align with a recent report from CoBank highlighting merger and acquisition activity in the food sector. The firm pointed to two themes driving these moves: companies seeking to streamline their product portfolios and expand their footprint into the snacking and better-for-you categories.

Nonetheless, CoBank pointed to a slowdown in overall activity in 2024, but with higher per-deal capital investment. Citing data from PitchBook, the firm reported that the total quarterly number of food and beverage M&A deals never dropped below 650 between the third quarter of 2021 and second quarter of 2023. The total number of quarterly deals dropped to 485 in the first quarter of 2024 and 416 in the second quarter of 2024.

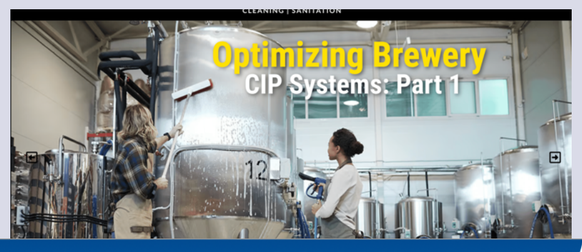
However, the per-deal average of capital investment increased to $53.6 million per quarter in 2024, up from $30.4 million between 2021 and 2023.

"With consumers focused on better-for-you snacking, M&A opportunities in those spaces will likely increase, especially as certain segments appear overcrowded," writes Billy Roberts, senior economist, food and beverage, CoBank. "Specifically, categories such as plant-based meat alternatives have a wealth of smaller brands, and with limited category growth of late, consolidation is likely. Elsewhere, major companies have opportunities to expand with strategic acquisitions of smaller players or for smaller companies to build share through merging."

Within the first two weeks of January — even after the holiday season — Flowers Foods reported it would acquire better-for-you snack and baking mix manufacturer Simple Mills for $795 million. Additionally, Day-Lee Foods acquired B and D Foods, Mountain View Packaging and Tamarack Foods, while Westfalia Fruit acquired Syros, a Belgian manufacturer of avocado products.

Based on CoBank's insights, and the flurry of activity we've already seen, 2025 is poised to be an active year for food mergers and acquisitions. Time will tell. **FE**

NEXT ARTICLE



MAKE CONSISTENT COATING YOUR SECRET SAUCE.

Reduce variability and raise the quality of frozen and prepared meals.

- Perfectly “freezes on” sauces and seasonings
- Reproducible, high-quality taste results
- Longer shelf life from faster freezing

Freeze & Coating Tumblers for Frozen and Prepared Foods

PRECIPAK

Precision from Poly-clip System and beyond.

günther®

precipak.com

Optimizing Brewery CIP Systems: Part 1

Though breweries face production and staffing challenges, there are opportunities for them to optimize operations – particularly through clean-in-place (CIP) systems. The first part of a two-part series highlights these challenges and the importance of "cleaning with intent."

Photo courtesy: Getty Images / SeventyFour

ANDREW KLOSINSKI, SENIOR PROCESS ENGINEER, LSI

THE BREWING INDUSTRY IS EXPERIENCING SIGNIFICANT CHANGES FROM ALL DIRECTIONS. Breweries are dealing with a shrinking knowledge base due to retirements and turnover, facing hiring challenges and operating with lean staffing. This limits the time available for brewing personnel to accomplish everything that is asked of them.

As a result, there is less understanding of clean-in-place (CIP) systems and little time to locate documentation on aging assets and outdated facility drawings. Furthermore, there is increased scrutiny of performance metrics and heightened attention on sustainability. Despite these challenges, there are opportunities to optimize, and CIP systems hold the keys to many benefits for breweries.

EFFICIENT BREWING IS A BALANCING ACT

As brewers, we use our creativity and skills to produce the best and most appealing product for our patrons. In short, we brew – or that is what the outside world thinks we do. In reality, much of our time is devoted to the myriad activities that it takes to be successful in this challenging industry: production scheduling, equipment maintenance, and materials procurement, along with personnel-related items such as staffing, safety and training. Some days it is nearly all we can do to get beer out the door to our customers.

And then, after all of that, we turn our remaining attention and resources to cleaning and sanitation.

BREWING SUCCESS BUILT ON CLEANING AND SANITATION

Our consumers may not give it a thought, but as brewers, our success is built on a foundation of our cleaning and sanitation capabilities and practices. With sanitation being such a fundamental aspect of brewing, it deserves and demands to be as important as the recipes and ingredients to which we devote so much energy and passion.

Think for a moment about your brewery. Where do CIP systems fall in the hierarchy of knowledge, understanding and focus? Are they:

- Done well?
- Repeatable?
- Performed at the right frequency?
- Done in a sustainable manner?
- An afterthought or task to merely get through?

MAKE CIP MORE THAN A CHECK-THE-BOX EXERCISE: CLEAN WITH INTENT

Imagine what it looks like to take CIP beyond a "check the box" exercise. Consider the benefits to your products. Consider the improvement to your profitability through reduced water, chemical, sewer or wastewater costs. Think of how this benefits your staff in terms of engagement and empowerment as they build skills, learn about, and take pride in a critical element of brewing.

Elevating your approach and philosophy to consistently executing quality CIP is well within reach and pays dividends. From this point forward, we will "Clean with Intent," and, as with any journey, we will start at the beginning.

Cleaning with intent requires us to have complete knowledge of the system hardware, instrumentation and controls. It is guided, supported and grounded by change management. Each step follows a path of inquire, observe, document, verify and implement, as shown in Figure 1.

Figure 1: Elements of how to clean with intent. Graphic courtesy of LSI.

BUILD CIP KNOWLEDGE WITH THREE QUESTIONS

Learning begins with being inquisitive. We build our knowledge of CIP by asking three questions:

- What is the intent of the CIP system?
- Is the system capable of achieving these demands?
- Is the technology currently in place appropriate for the application?

In many cases, the first question — the intent of the CIP system — may be a simple and straightforward conversation. For most, a CIP system is intended to provide a clean and sanitary environment in which to brew, ferment, transport, filter, store or package product. The exact definitions of "clean" and "sanitary" are likely where most of the discussion will occur. Spend the time needed and gather a team with a wide knowledge base to clearly set these expectations and establish specifications around "clean" and "sanitary." Being able to quantify, measure, compare and trend CIP data is key to success.

Once structure has been created around the intent of the CIP, determining its current state capability may spawn several conversations and will likely result in needing to do some homework. For many of us, we inherited the systems at our facilities. The original design and process flow have likely changed and expanded. Aging assets, varying levels of maintenance and ever-increasing equipment costs may have resulted in the original CIP system looking quite different today than upon its commissioning.

Example questions could include: What is the diameter of the CIP supply pump impeller? Did that CSS pump previously run at a fixed speed? When was the VFD added? Do you know what type of cleaning mechanism is in each vessel? Does each cleaning machine have the same diameter nozzle? And so forth.

ARE OUR PROCESSES KEEPING PACE WITH THE EVOLVING BEER INDUSTRY?

With brewery portfolios expanding into different and novel beverages, give some thought to the implications this has on our CIP systems. For example, is a CIP system once designed solely for beer production capable of addressing and eliminating flavor carryover between batches? Do the current tank cleaning mechanisms have the capability to remove the solids and residue from new yeast strains, non-malt-based wort or ever-changing adjuncts?

CAPTURING CIP PROCESS DETAILS WITH A PROCESS FLOW DIAGRAM

As you can see, there can be numerous unknowns to resolve. This is where a process flow diagram (PFD) provides a starting point to aid the effort and help capture process details as they are learned. Often CIP systems are conducted through loops or circuits rather than in a single pass. With that, start with the cleaning solution tank and work your way through the loop, identifying and recording details on every pump, motor, valve, instrument, heat exchanger, chemical dosing point, cleaning machine and vessel. Some of this work can be done leveraging existing process and instrumentation diagrams (P&IDs), information obtained through a computerized maintenance management system (CMMS) and equipment manuals. This valuable information reflects the current state of the CIP loop and leads us to the next step — verification.

Figure 2: Example CIP Process Flow Diagram (PFD). Image courtesy of LSI.

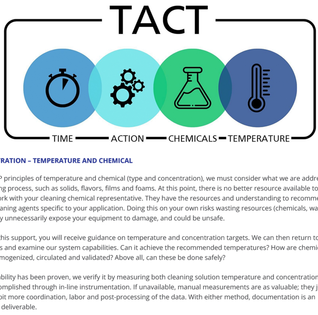
GET OUT IN THE FIELD AND VERIFY

It is at this point we take our understanding of the process and physically verify its details — make, model, size, horsepower, diameter, measurement range, etc. This is a field effort and will necessitate climbing, crawling, dodging and ducking as you follow the process. Along the way, you will capture nameplate and other important details to compare against the original PFD. What you find in the field may not always agree with past documentation. That's okay, and is the point of this effort: we need to understand the constituents of the systems as they exist today. Armed with complete and current-state process information, we can now advance to answering the question — is the CIP system capable of achieving the demands and deliverables being asked of it?

THE FOUR FUNDAMENTALS OF CLEANING

After reviewing the details documented in the PFD, we can now determine the ability to achieve our definition of clean and sanitary against the four fundamental principles of cleaning – Time, Action, Chemical and Temperature.

Figure 3: The Four Cleaning Principles (Sinners Circle). Graphic courtesy of LSI.



CONCENTRATION – TEMPERATURE AND CHEMICAL

For the CIP principles of temperature and chemical (type and concentration), we must consider what we are addressing in the cleaning process, such as solids, flavors, films and foams. At this point, there is no better resource available to you than to work with your cleaning chemical representative. They have the resources and understanding to recommend and source cleaning agents specific to your application. Doing this on your own risks wasting resources (chemicals, water, labor), may unnecessarily expose your equipment to damage, and could be unsafe.

Engaging this support, you will receive guidance on temperature and concentration targets. We can then return to the PFD details and examine our system capabilities. Can it achieve the recommended temperatures? How are chemicals dosed, homogenized, circulated and validated? Above all, can these be done safely?

Once capability has been proven, we verify it by measuring both cleaning solution temperature and concentration. Ideally, this is accomplished through in-line instrumentation. If unavailable, manual measurements are as valuable; they just require a bit more coordination, labor and post-processing of the data. With either method, documentation is an important deliverable.

From these efforts, we have now achieved optimal temperatures and concentrations. Yet, a substandard CIP may still result. We must address all principles of cleaning equally. To that end, we turn our attention to cleaning action – the mechanics that deliver a great CIP.

See next month's edition for the second of two parts highlighting solutions for CIP in breweries.

NEXT ARTICLE

ELEVATE YOUR PLANT MAINTENANCE PROGRAM...

WITH LUBRIPLATE® 100% SYNTHETIC NSF H1 REGISTERED FOOD GRADE LUBRICANTS.

Engineered from the ground up to provide unsurpassed performance in food processing facilities. These high performance, 100% synthetic lubricants provide extended lube intervals, multiple application capability, lubricant inventory consolidation and improved performance. All while maintaining strict H1 safety requirements.

Lubriplate's NSF H1 Registered Products Include:

- HIGH-PERFORMANCE SYNTHETIC GEAR OILS
- SYNTHETIC AIR COMPRESSOR FLUIDS
- SYNTHETIC HYDRAULIC FLUIDS
- HIGH-PERFORMANCE SYNTHETIC GREASES
- HIGH-TEMPERATURE OVEN CHAIN LUBRICANTS
- NSF H1 REGISTERED SPRAY LUBRICANTS

NSF Nonfood Compounds H1 Registered ISO 21469 Certified

PAREVE HALAL

See the NSF White Book™ for a complete list of registered / ISO 21469 certified products.

"It's the Film." PREVENTS WEAR and CORROSION LUBRIPLATE SUPER-LUBRICATION

Lubriplate® H1 LUBRICANTS

Newark, NJ 07105 / Toledo, OH 43605 / 800-733-4755
To learn more visit us at: www.lubriplate.com

INCLUDED AT NO ADDITIONAL CHARGE

Lubriplate's ESP

Complimentary Extra Services Package

COLOR CODED LUBE CHARTS & MACHINERY TAGS
PLANT SURVEYS / TECH SUPPORT / TRAINING
LUBRICATION SOFTWARE / FOLLOW-UP OIL ANALYSIS

How Technology Is Transforming Transportation Management in Food Supply Chains

Transportation management systems have become crucial in supply chains to mitigate the impact of unexpected delays, improve communication between stakeholders and optimize planning for more efficient logistics processes.

Image courtesy of Getty Image / RichLegg

BY NICK FRYER, VICE PRESIDENT OF MARKETING, SHEER LOGISTICS

THE FOOD SUPPLY CHAIN PLAYS A CRUCIAL ROLE IN DELIVERING FOOD FROM FARMS TO TABLES AROUND THE WORLD. This system involves multiple steps, including production, processing, distribution and consumption.

With the modern global food industry growing at an annual rate of 6.7%, developing more efficient and smoother supply chains is an imperative.

Transportation management is instrumental in securing, planning and executing the movement of food products along the supply chain. The process involves determining the most efficient routes for shipments, carrier management and shipment tracking to ensure on-time delivery.

Nick Fryer is vice president of marketing for Sheer Logistics. Fryer has has over a decade of experience in the logistics industry, spanning marketing, public relations, sales enablement, M&A and more at 3PLs and 4PLs, including AFN Logistics, GlobalTranz and Sheer Logistics.

KEY COMPONENTS OF TRANSPORTATION MANAGEMENT IN FOOD SUPPLY CHAINS

Poor transportation management leads to the disruption of supply chains and delays in the delivery of supplies. To effectively manage and prevent future supply chain crises, it is crucial to understand the key components of transportation management within the food supply chain, thereby reducing the risk of unexpected disruptions. These components include:

Planning

Planning is the foundation of efficient food logistics. It involves forecasting demand, allocating resources effectively and scheduling shipments. Accurate planning helps prevent delays and ensures perishable goods maintain their quality. Logistics teams must account for seasonality and transportation lead times while creating supply schedules that reduce waste and meet customer demand.

Route Optimization

Route optimization involves the determination of the paths that shipments take to reach their destination. Efficient routing minimizes transit times while reducing fuel consumption and costs. For food logistics, optimized routes ensure perishable items maintain freshness by avoiding unnecessary delays. Advanced tools, such as GPS-enabled systems, allow real-time adjustments to routes, further enhancing the efficiency of deliveries.

Tracking

Tracking promotes visibility across the entire food supply chain. It allows all parties to monitor shipments' status and location in real-time. This transparency helps address potential delays before they escalate into significant disruptions. Additionally, tracking strengthens trust between suppliers and customers by providing timely updates and ensuring accountability in the delivery process.

Optimization

Optimization integrates planning, routing and tracking to create a seamless and cost-effective logistics process. It focuses on reducing operational inefficiencies, such as unnecessary transit times or misused resources. Optimization ensures food products move quickly from producers to end-users with minimal waste and cost through continuous data analysis and improved coordination.

Technological Innovations Driving Change

In recent years, technological advancements have greatly impacted the food supply chain. These innovations have brought about significant changes in how businesses manage their logistics processes. The following are some technological solutions that have revolutionized the food supply chain industry:

Image courtesy of Getty Image / BlackJack3D

Artificial Intelligence (AI)

Artificial intelligence has helped businesses automate tasks that are otherwise too complex for humans. AI algorithms improve demand forecasting, optimize delivery schedules and help manage potential disruptions. For instance, AI-powered systems analyze historical data to streamline fleet operations, reducing delays and associated costs. According to McKinsey, companies that use AI have seen up to a 15% reduction in operational costs.

Internet of Things (IoT)

IoT enables real-time monitoring and communication between devices in transportation networks. Sensors installed on vehicles track temperature, humidity and location. Tracking increases visibility, reduces lead times and ensures perishable goods maintain quality during transit. Improved visibility minimizes waste and boosts efficiency. IoT devices also provide instant alerts for changes in delivery conditions, helping logistics teams address issues promptly.

Transportation Management System

Transportation Management Systems (TMS) are software platforms designed to facilitate the planning, execution and optimization of the movement of goods. TMS provide enhanced visibility to shipments and supply chain data, empowering logistics managers with real-time business intelligence.

Predictive Analytics

Predictive analytics utilizes past and real-time data to predict transportation patterns. Analytics helps businesses address disruptions before they occur, minimizing downtime. For example, it predicts weather impacts or road congestion, allowing route adjustments in advance. With a greater focus on optimization, predictive analytics plays a pivotal role in reducing fuel consumption and improving delivery times.

BENEFITS OF ADVANCED TRANSPORTATION MANAGEMENT

Adopting advanced technologies in transportation management brings numerous benefits to the food supply chain industry. These benefits include:

Improved Efficiency

Advanced transportation management systems streamline logistics operations. They enhance scheduling, route planning and delivery coordination, saving time and resources. Automated systems optimize load capacity and minimize empty miles. Automation reduces delays and fuel consumption, leading to faster deliveries. Businesses leveraging these systems experience greater reliability in supply chain performance.

Reduced Waste

Improper handling and delays in transit contribute significantly to food waste. Advanced transportation systems address this issue through real-time tracking, the use of refrigerated transportation and optimized routing. According to the World Economic Forum, 14% of the world's food is wasted along the supply chain. Technology-driven insights help further decrease inefficiencies and waste throughout the logistics cycle.

Enhanced Food Safety

Maintaining food safety during transit is a key challenge. Advanced systems use sensors to monitor temperature and humidity in real-time. This prevents the food from spoiling and preserves the quality of perishable products. Any deviations trigger alerts, allowing quick corrective actions. Enhanced safety not only protects consumers but also upholds industry compliance standards.

CHALLENGES AND SOLUTIONS

Transportation management in food supply chains faces significant challenges that affect efficiency and reliability.

Long Lead Times

Poorly optimized routes, extreme weather, traffic, underutilized resources and damaged infrastructure are major causes of extended transit times. These factors often disrupt schedules, leading to spoilage of perishable goods. For context, the U.S. Department of Agriculture reports that 30-40 % of food waste in the United States occurs during the supply chain stage. These losses not only impact revenue but also strain global food resources.

Players in the food industry can solve this problem by engaging the services of a transport service provider. A third-party provider uses a modern transportation management system (TMS) that utilizes data-driven algorithms to create smarter routing plans and maximize load capacity. This reduces fuel consumption, accelerates deliveries and lowers costs.

Lack of Proper Coordination

Coordinating numerous stakeholders in the supply chain creates another layer of complexity. Miscommunication between suppliers, transporters and retailers can lead to poor handling, lost shipments or delivery errors. This issue can be addressed by leveraging transport logistics technology.

For instance, if you already have an ERP, you can partner with a reliable logistics services provider to help integrate TMS software into your existing system. Using a TMS, stakeholders can communicate effectively via centralized platforms that enable real-time communication. These tools include EDI, APIs and Text. When teams are aligned, errors are reduced and operational efficiency improves.

The use of transportation management systems has become crucial in today's supply chain operations. These systems help mitigate the impact of unexpected delays, improve communication between stakeholders and optimize planning for more efficient logistics processes. With the increasing challenges faced by supply chains, it is clear that investing in these modern tools is essential for businesses to stay competitive.

NEXT ARTICLE

Using Data to Drive Predictive Maintenance Strategies

Food and beverage manufacturers are discovering that machine learning is a vital ingredient in moving to predictive maintenance strategies. Larger food companies have the jump on digital transformations, but smaller companies are starting small and increasing spending to start the journey.

Making a prepared main course in the test kitchen is one thing, but should it be turned into a product offering and, if so, how can the freshness and quality of the components be maintained with problematic suppliers and logistics issues—and if all those things go well, will consumers love your product? AI-based PLM stands ready to help make the right decisions. Image courtesy of Getty Images / yongyuan

BY GRANT GERKE

DOING MORE WITH LESS IS A FAMILIAR REFRAIN IN THE MAINTENANCE DEPARTMENT, but food and beverage manufacturing executives and plant floor personnel are moving toward a full-fledged understanding that capital investments are needed to extend machine lifecycles and production uptime.

What's driving this realization? There are many, but one is a shared understanding of a limited workforce and that more digital tools are needed. A recent report from Deloitte and the Manufacturing Institute indicates manufacturers may need up to 3.8 million new workers by 2033, with nearly half of these positions potentially going unfilled if current labor gaps persist. Plus, fewer workers are coming into manufacturing, and the current average age of highly skilled workers is 56, with nearly a quarter of this workforce set to retire in the next decade.

The other driver is machine learning (ML) technology, a subset of AI, and a foundational piece of this revolution in manufacturing. For more than 10 years, food manufacturers have added vibration sensors, gathered equipment data and fed information into data analytics platforms while also adding computerized maintenance management systems (CMMS). Food companies are succeeding, but will executives stay committed to larger capital investments in machine learning and analytics, especially when asset management investments are hard to measure?

WORKFORCE PRESSURES IN MAINTENANCE

For the last 10 years, the race has been to move away from reactive maintenance and toward predictive analytical strategies so maintenance teams can schedule fixes during traditional downtime and optimize uptime.

"Predictive maintenance and related technologies have gained more traction in recent years, but there is a long road ahead as most manufacturers still do not understand this new technology and its potential positive impact on their day-to-day operations," says Ronak Macwan, senior industry marketing manager for manufacturing at Brightly Software, a Siemens company.

"Over the past five years, the roles of maintenance technicians, planners and managers in the food processing segment have shifted significantly," adds Lucie Dahuron, global marketing cross segment leader at Schneider Electric. "They have become much more proactive than merely reactive in addressing maintenance issues."

In 2022, grab-and-go sandwich producer E.A. Sween began using Brightly Software's Asset Essentials CMMS platform that would manage and maintain more than 7,000 parts in the plant.

"We were using a very difficult, paper-driven work order process," says Erik Willams, maintenance planning and purchasing supervisor at E.A. Sween. "Our purchase orders were paper, and technicians used a sign-out sheet in our parts room to order the parts they needed. It was complicated to track and trace everything."

The company ramped up production from five to seven days a week in 2022 due to soaring demand, and preventive maintenance completion rates steadily declined to about 25%. With the new CMMS platform, Williams determined that small preventive maintenance jobs had kept the percentage high, while many of the large preventive maintenance tasks remained uncompleted.

"We had these million-dollar pieces of equipment that weren't getting any preventive maintenance or downtime," Willams says. "The software showed us that our technicians were just inundated."

The data also showed that technicians were needed for 120 hours of preventive maintenance during a two-week period, while they were only at work for 80 hours.

"We were able to use that data to show we needed additional preventive maintenance staff, and it gave us the leverage to get those people," Williams says.

Small and large food manufacturers are adopting digital tools and system software to optimize maintenance while facing workforce challenges. Image courtesy of Brightly Software, a Siemens Company

Brightly Software's Macwan says data analytics is transforming food and beverage manufacturing's maintenance processes in ways that mirror E.A. Sween's experience.

"Historical data plays a significant role in preventive maintenance strategies by providing detailed information on each asset and piece of equipment, such as previous repair history, inventory parts information and current equipment condition," Macwan says.

The software allows E.A. Sween to set short maintenance windows, automatically assign work, update and quickly reassign when something changes, and the software automatically creates follow-up work orders to keep things moving and maintain equipment.

In addition to flexible maintenance schedules, modern CMMS platforms aid technicians with machine data and images via mobile devices.

"Mobile and augmented reality solutions support the workforce with their daily tasks, and all the information is available on the machine," Dahuron says. "The software guides the maintenance technician through their tasks and reduces onboarding of new employees."

MOVING TO PREDICTIVE MAINTENANCE STRATEGIES

While some manufacturers add more digital tools to operations, large food producers and ingredient companies are taking bigger leaps at refining machine data and moving to predictive maintenance strategies. These strategies require a capital expenditure (CAPEX) commitment to data governance and acquisition platforms.

"Food and beverage manufacturers often lack a clear understanding between asset life cycle management and its connection to the capital planning process," Macwan says. "Food executives must realize that the key to overall success is understanding how to maximize equipment life expectancy and leverage current and historical equipment data for the capital planning process."

"Data analytics is a perfect way to analyze a huge amount of data and focus only on the 0.1%, which are relevant," Dahuron adds. "For example, the increase in the feedback time of a valve is a good indicator of the valve's lifecycle. With the right data, you can select 0.1% of the valves where the feedback time increased most."

At the recent AVEVA World 2024, Ajinomoto presented its success in moving to a predictive maintenance strategy and increasing uptime and production at its plant in Eddyville, Iowa.

"There were many times where there has been a problem that has suddenly happened where it be a process upset or an equipment failure that then leads to a process upset, just requires immediate attention to alleviate some of those issues," says Michael Ross, chemical process engineer at Ajinomoto Health and Nutrition North America.

Ajinomoto uses AVEVA's PI historian for data collection and connects to SAM GUARD software, a machine learning solution that connects, contextualizes and monitors data for anomalies.

"The team is notified of any potential process upsets before they happen, and we are able to then make a decision to alter course and schedule maintenance during a planned downtime period rather than taking unplanned downtime, which is costly," says Meg Lashier, senior production coordinator at Ajinomoto Health and Nutrition North America.

Ajinomoto moved forward with this approach:

1. The first step is to have all historical data points sorted hierarchically within the third-party software.
2. Then, it contextualizes the data according to its process flow and assigns different sensors to various assets within the model.
3. From there, Ajinomoto trains the model based on two-plus years of process data.

However, bad data can corrupt data modeling and predictive maintenance strategies. "One thing that we had to be very careful of while we were doing this is to take out any sort of process upsets or any major plant shutdowns that we had," Lashier adds.

With the data modeled, Ajinomoto prioritizes assets and individual sensors by assigning them sensitivity ratings. "A critical asset that we would like to be alerted to and even with small changes outside of what is considered normal data, we will be assigned a very high sensitivity range," Lashier says. "And operators will be notified more frequently on that asset versus an asset that we know has a range of what is considered normal."

At the event, Lashier provided an example of its fluidized bed dryer and how the software sent an alert about a set point issue for a motor. The maintenance team troubleshooted but couldn't find the root cause. "Eventually, we scheduled time to take down the dryer during a normal cleaning day when we had time to do it," Lashier says. "And ultimately, we found a big mess inside the dryer." Ajinomoto realized there was caramelized product that was binding and restricting flow, which eventually would've backed up and had cascading impacts on the rest of production.

Going forward in 2025, small and large food manufacturers can look for quick wins — as well as large CAPEX investments — to help them move toward a predictive maintenance approach.

NEXT ARTICLE

CYBERSECURITY

How Does Your OT Cybersecurity Stack Up?

Tips and Techniques for a Secure and More Secure Operation

While protection from hackers can be complex, many IT and OT managers aren't following the basics.

Emerson promises a complete portfolio of hardware and software products supporting 'five-to-cloud information and automation solutions, and incorporating built-in cybersecurity provisions and compliance with major cybersecurity standards, backed with ongoing support. Image courtesy Emerson Electric Automation

BY WAYNE LABS

WHILE SOME HACKERS ARE TECHNICALLY GIFTED INDIVIDUALS who can find their way into any plant OT and/or IT system using their knowledge of computers, systems, and networking, in many cases, hackers take the easiest route to their destination — that being your data. And that easy route may actually be through your "front door," not the proverbial "back door."

For instance, Infosec reported that its OT Top Security Threat for 2024 is "inadequate authentication and authorization. Inadequate or nonexistent authentication and authorization control measures that can allow unauthorized individuals to gain access to OT systems."

In its 2024 X-Force Threat Intelligence Index, IBM reports cybercriminals are increasingly "logging in" with valid accounts, rather than hacking into networks, tasks accounting for the "most common entry point into victim environments" in 2023, representing 30% of all incidents. IBM's X-Force responded to. Additionally, IBM reports a 71% year-over-year increase in cyberattacks using valid credentials.

THE TROUBLE WITH OT SYSTEMS AND CONNECTING TO IT

There are multiple issues with OT systems that prevent implementation of cybersecurity and integration with centralized authentication and authorization systems, says Steve Ward, director, application specialists, EMEA, Emerson Discrete Automation. OT control systems are commonly installed, used and maintained over the course a long time — 20 years or more.

While cybersecurity has been an issue for many years, older OT control systems often have few or no cybersecurity capabilities. OT practitioners may not be aware of cybersecurity capabilities and even if these capabilities are present, they may not be implemented. If OT practitioners are aware of a security vulnerability, they may consider that the risk of the process is air-gapped from the internet, although in practice there often is a connection, and even if they are air-gapped, risks still exist. OT practitioners also must consider ease-of-use over the lifecycle of the machine or process. If cybersecurity protection is implemented, how will this affect the ability to maintain the machine in case of a failure? A password-protected machine or protection system poses a risk, if the password is lost. There's a simple failure to address into days or years of downtime.

Early on when IT and OT systems became more "connected," it was assumed that the IT system could serve as the gatekeeper for logons to the OT network, which added complexity and degraded overall network performance. According to Dustin Sachse, controls engineer for Atos, a CSIA-Certified System Integrator Association member company, "OT systems are designed with enough bandwidth, the technology changes so fast that it's very difficult to keep ahead of it and keep a plant running. Trying to IT-ify or corporate-ify OT systems (OT makes money EVERY second they're down), which is necessarily a good idea," Dunlap says. "Many operators use a common portal for IT and OT applications, which presents another attack surface. Each vendor has a different OT environment requirement."

"Broad and beverage manufacturers must acknowledge that the core of inadequate authentication and authorization in OT systems stems from legacy infrastructure," says Eric Cosyns, CSIE, Rockwell Automation. "Many of these systems, during an era when connectivity was limited to isolated environments and robust security protocols were unnecessary. This foundational weakness has become a critical vulnerability in today's interconnected landscape, as modern authentication to gain entry. To address this, we need multi-layered strategies. First, implementing role-based access control (RBAC) and multi-factor authentication (MFA) across OT environments is non-negotiable."

While these solutions are standard in IT, their integration in OT is challenging due to system interdependencies and operational requirements. However, modern control systems increasingly support MFA led to centralized identity systems.

HMI/SCADA OT Cybersecurity Issues: From a Supplier's Perspective

The European Union's Cyber Resilience Act (CRA) will lead to changes in implementation of cybersecurity in OT control systems since it will mandate that cybersecurity provisions are implemented by vendors by default. However, OT practitioners may choose to disable cybersecurity protection in favor of ease- of use and to simplify future maintenance. That challenge here is that cybersecurity is inevitably left something happens, and OT practitioners are not rewarded for protecting against a scenario thrived. Yet they are blamed when there is downtime, particularly if the downtime is extended beyond an hour or so. So, systems are not ever cybersecurity protection.

MS/SCADA systems don't tend to be so old as OT control systems. They are often upgraded every three to five years and are usually Windows- based, so they can be integrated with Microsoft Active Directory. This needs willful effort and cooperation between IT and OT teams, as well as a network link from the OT system to the IT system. While this is a best practice for cybersecurity, it's not always done. "Many HMI/SCADA systems are Windows-based, so they can integrate with Microsoft Active Directory (an even more comprehensive cybersecurity since we no longer will now be removed and lack of user maintenance could expose the HMI/SCADA system to remote attack. Issues with linking HMI/SCADA systems with Microsoft's Active Directory include keeping user privileges up to date, as well as handling details of operations and maintenance engineers who may be contractors and not work for the organization.

Note that Microsoft's Active Directory is not the only authentication mechanism available, and some users have implemented alternatives, meaning that OT systems have to conform to these providers as well as Microsoft's, making it more complex for the vendor.

Many problematic issues are possible when securing HMI/SCADA systems. In one case, the end user's IT team locked down the HMI/SCADA server to such an extent that they locked themselves out and had to re-install and re-configure the entire system. The lock-down process added several days to the configuration process in the first case and the reinstallation added several days to the recovery process in the second case. Another HMI/SCADA cybersecurity problem occurs when the end user's IT team could not grant the contractor permission to access the HMI/SCADA system, resulting in reduced capabilities of the HMI/SCADA system and an inability to perform continuous improvement. In another case, a user account was created for the HMI/SCADA to run system-level processes; however as this was not an active user the IT team deleted the account due to inactivity, and the HMI/SCADA system stopped running for several days until the root cause could be determined.

—Steve Ward, Director, Application Specialists, EMEA, Emerson Discrete Automation

Zero Trust Maturity Model Pillars illustration by CISA. This illustration was inspired by an illustration from the American Council for Technology (ACT) and Industry Advisory Council (IAC) "Zero Trust Cybersecurity Current Trends." Image source: CISA

"Manufacturers can overcome inadequate authentication and authorization in OT systems by implementing the Zero Trust Architecture (ZTA) framework outlined in the CISA guide," says Mike Yoder, engineer for the E-Tech Group, a CSIA certified member. ZTA emphasizes building security around devices and networks, including device authentication mechanisms. Manufacturers can start by identifying and categorizing their OT devices and networks to determine the appropriate level of access control and authentication. For centralized authentication and authorization, manufacturers can use Identity and Access Management (IAM) or Privileged Access Management (PAM) solutions. While many existing OT systems were not designed with security in mind, implementing ZTA and using IAM or PAM solutions can help manufacturers build robust authentication and authorization mechanisms into their OT networks."

—Dan Torres, Controls Engineer, Egan Company / Industrial Controls, a CSIA member

What is Zero Trust and How Does It Work?

Zero Trust assumes that any user, regardless of location, inherently is not to be trusted. To allow a user access to systems, devices or applications, their identity, authentication and authorization should be verified on the initial access request and continuously while they are accessing protected resources. In an IT setting, this can be accomplished with a Zero Trust Broker acting as an intermediary between a user and the resources they are trying to access, for example, an application on a server. This Trust Broker may be one or several hardware and/or software solutions. A key part to this is ensuring that the Trust Broker is the only way to access the resource. Typically, this is done by implementing software with the Trust Broker during the authentication process. In an OT setting, this model might encounter roadblocks as it may not be feasible or possible to install such an agent on each device to be protected. As we start to see more devices and systems designed with security in mind, an awareness of Zero Trust and the required exchanges between device, Trust Broker, and user should be considered during the development lifecycle.

—Dan Torres, Controls Engineer, Egan Company / Industrial Controls, a CSIA member

THE "CLOUD" AND SAFE OPERATION

IIoT System Implementation and Certification Based on ISA/IEC 62443 Standards (ISA, May 2024) points out four example use cases for IIoT-based cloud architecture:

1. Cloud-based data analytics – non-operational (view data only)
2. Cloud-based data analytics – operational (operator could make a change influenced by data and trends stored in the cloud
3. Cloud-based operator view and manipulation (operator can view and manually manipulate the physical state of the equipment under control from the cloud zone)
4. Cloud-based non-essential control (cloud can automatically send a setpoint to a controller in the edge zone, but not changing the setpoint to a controller, asking a physical change to the equipment under control.

While ISA doesn't make the case for or against the cloud/control applications cases 1-4 shown above, based on bad actors obtaining valid login/access credentials for cloud or plant/business management, what practices can be applied to keep these bad actors out of control loops and systems without causing negative consequences to those (e.g., staff engineers, system integrators) who should be connected?

Organizations should adopt and observe OT and manufacturing IT philosophies appropriate to asset plans, says Jason Pennington, Endress+Hauser OA director of digital solutions. "Our most mature digital customers are leveraging the idea that digital assets require a maintenance plan and set of policies that are regularly reviewed, included in onboarding/offboarding procedures, and administered on an ongoing basis, rather than as a one-time departmental or divisional level."

Regarding cloud-based services, which are run by experts, a user can generally be confident that the cybersecurity provided by the cloud vendor is better than the cybersecurity that processors could implement themselves, says Emerson's Ward. Cloud vendors implement secure practices that protect information in transit, including user details and passwords. However, user account management remains the responsibility of the user, and they must ensure that user accounts are maintained along with a suitable password policy — and that departing users are deleted.

While ISA does not make cases for or against cloud-based integrations in industrial environments, individual enterprises and OT departments should consider the inherent risks associated with cloud deployment and evaluate the impact on the business if there were a breach, says TM Process and Controls' Yong. In general, proper architecture and network segmentation can help minimize risks, cloud-based platform integrations that reside mainly in the data analytics or data heading up into the cloud category.

For cloud-based operator viewing and manipulation, an organization should question the need since there should already be onsite viewing and manipulation on the plant floor or operator room, Yong adds. If there is a valid justification, the next question should be what data must be viewed and manipulated from the cloud platform. The data sets should be reviewed along with how a cloud data breach could impact operations.

Once vetted, Yong says, intermediary industrial software/hardware must be put in place so as a middleman to get the data from OT to the cloud platform and vice-versa. One key component of the intermediary software/hardware is that there must be manual data mapping to ensure the entire OT dataset is not exposed to the cloud. Lastly, there must be code put in place at the PLC/DCS level to disregard manipulations exceeding the system's safe and allowable range.

CLOUD OR NOT: IT'S ALL ABOUT USER ACCESS CONTROL

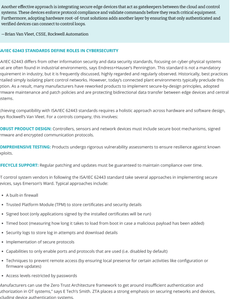
Aidas OT's Dunlap points to the basics — once a system has gone through FAT and is up and running in production, all those hard-a-vide s setting up the system no longer need to be kept on a login list. "Remove back doors, and that means removing all back doors," Dunlap says. "Hacks have occurred as third-party suppliers are compromised and the attacker gains access to many of the supply chain's customers. Make sure control systems' log-in access is limited to the licensor's partners, the systems integrator, terminated employees and various service providers were still provisioned. Set up complex time and multifactor access to remove these attack vectors."

Dunlap suggests other steps that can be taken to keep unneeded people out of the system:

- Set up implicit deny to all users and services, including non-human users;
- There are still control systems being built that use insecure protocols. One popular vendor has systems that use a potentially compromised hash algorithm.
- Understand how network and access keys are generated and update the algorithms if possible.
- Find bad certificates and update them.
- Update older equipment to ensure that the newer is not forced into using older standards to maintain compatibility.
- If a device has a hard-coded, unchanging network key, upgrade as soon as possible.

Manufacturers can also use access controls, network segmentation, behavioral analytics and multi-factor authentication (MFA) to keep bad actors out of control loops and systems with legitimate logins and passwords, says E-Tech's Smith. MFA gives the login process an additional layer of security, and network segmentation reduces the chance that a malicious actor could do if they were to get access to the system. Access controls restrict who can access the system and what they can do, while behavioral analytics identify anomalous network activity.

MFA is recommended, but this may be complicated to implement in OT situations, says Emerson's Ward. For example, operators may not be allowed to take their mobile phones into the production environment and so MFA apps will not be available to them. Also, operators may be in a hurry to get a process back up and running after a shutdown or other process anomaly. A shuffleboard user could also interfere with operations by "tossing" a physical device so that they can't work until it is replaced.



Endress+Hauser's Netilion cloud-connected enterprise management platform integrates with MES through Microsoft Authenticator and other SSO (single sign-on) providers. Image courtesy Endress+Hauser Process Solutions AG, Endress+Hauser Group Services AG

"Once an IT system that is quite pervasive is now impacted by the use of common patterns in system and device compatibility," says Egan's Torres. This is usually seen on devices that are networked but are not able to utilize systems like Active Directory to manage access. Assuming a default login is changed at all during commissioning of a device, it is often set to a common login used around the plant. Or, if not identical, it is very similar, not complex and easy to guess. As a result, if one such account is compromised, an attacker might easily access other devices and systems once this pattern is recognized.

Safe Cloud Practices

In scenarios where cloud-based data and control applications intersect with physical systems, the risks are heightened by the possibility of compromised credentials. Practical safeguards must focus on reducing the risk of misuse without hampering authorized access.

The first step is to deploy conditional access policies and behavior-based analytics, which can detect anomalies such as unusual login times or locations and restrict access automatically. Additionally, food manufacturers must adopt network segmentation strategies that isolate critical OT assets from direct communication. This ensures that if a breach occurs, it gains entry, their movement is limited.

Another effective approach is integrating secure edge devices that act as gatekeepers between the cloud and control systems. These devices enforce protocol compliance and validate commands before they reach critical equipment. Furthermore, adopting hardware root-of-trust solutions adds another layer by ensuring that only authenticated and verified devices can connect to control loops.

— Brian Van Vleet, CSIE, Rockwell Automation

ISA/IEC 62443 STANDARDS DEFINE ROLES IN CYBERSECURITY

ISA/IEC 62443 differs from other information security and data security standards, focusing on cyber-physical systems that are often found in industrial environments, says Pennington. Endress+Hauser's Pennington. This standard is not a mandatory requirement in industry, but it is frequently discussed, highly regarded and positively observed. Historically, best practices entailed simply isolating plant control networks. However, today's connected plant environments typically preclude this approach, so the 62443 standards are a good starting point for developing a defense-in-depth strategy using practices such as firmware maintenance and patch policies and zero-trust segmentation that transfer between edge devices and central systems.

Achieving compatibility with ISA/IEC 62443 standards requires a holistic approach across hardware and software design, says Rockwell's Van Vleet. For a controls company, this involves:

ROBUST PRODUCT DESIGN: Controllers, sensors and network devices must include secure boot mechanisms, signed firmware and encrypted communication protocols.

COMPREHENSIVE TESTING: Products undergo rigorous vulnerability assessments to ensure resilience against known exploits.

LIFECYCLE SUPPORT: Regular patching and updates must be guaranteed to maintain compliance over time.

ISA/IEC 62443 system vendors in following the ISA/IEC 62443 standard take several approaches in implementing secure devices, says Emerson's Ward. Typical approaches include:

- A built-in firewall
- Trusted Platform Module (TPM) to store certificates and security details
- Signed boot (only applications signed by the installed certificates will be run)
- Timed boot (measuring how long it takes to load from boot or case a malicious payload has been added)
- Security logs to store log in attempts and download details
- Implementation of secure protocols
- Capabilities to only enable ports and protocols that are used (i.e. disabled by default)
- Techniques to prevent remote access (by ensuring local presence for certain activities like configuration or firmware updates)
- Access levels restricted by passwords

"Manufacturers can use the Zero Trust Architecture framework to get around insufficient authentication and authorization in OT systems," says E-Tech's Smith. ZTA places a strong emphasis on securing networks and devices, including device authentication systems.

HMI/SCADA vendors running on Windows or Linux operating systems have a slightly easier life since many of the cybersecurity provisions come from the operating system's hardware layer, but they still have to implement user management and integration with Microsoft's Active Directory or equivalents, Ward says. HMI/SCADA vendors also have to regularly update their software to deal with any new vulnerabilities, often by updating the underlying components they use (for example Microsoft's .NET and open-source software). Ward says.

The advantages of ISA/IEC 62443 compliance are clear: improved security posture, regulatory alignment and customer confidence. However, challenges like increased development costs and the complexity of certification processes exist. Ultimately, these standards provide a framework that aligns the food industry with a security-first mindset, Van Vleet says.

Building towards ISA/IEC 62443 Compliance

Vendors can provide ISA/IEC 62443-compatible hardware/software that can withstand attacks on the industrial sensor networks by outsourcing their software to meet the following standards:

- Firmware/software updates for improvements in operation and security
- Authentication and authorization mechanisms with controllers and personnel avoid unauthorize configuration changes
- Encrypted network traffic so network packets are harder to decipher

The advantages to having ISA/IEC 62443-compatible controls hardware are

- Prevent sensor/actuator tampering that could result in downtime or quality problems
- Prevent man-in-the-middle attacks on controls hardware
- Improvement in monitoring/administering and operations of controls hardware

The disadvantages to having ISA/IEC 62443-compatible controls hardware are

- Requires trained tool skilled technicians to install and confirm functionality when it required electricians to complete the job normally
- May increase maintenance budget due to different skills required to carry out instrumentation work

— Hai Yong, ICS Cybersecurity Engineer, TM Process and Controls / OT and ICS Cybersecurity

NEXT ARTICLE

FOOD AUTOMATION AND MANUFACTURING

FA&M

SYMPOSIUM AND EXPO

April 14-16, 2025

Hilton Downtown Tampa
Tampa, FL

WHY ATTEND FA&M?

TOP-NOTCH EDUCATION

FA&M offers a robust schedule of educational sessions covering essential topics such as manufacturing efficiency, sustainability, plant design, and automation.

EXCLUSIVE NETWORKING OPPORTUNITIES

With a smaller, focused group, FA&M provides direct access to industry leaders and peers, ensuring that each conversation can lead to actionable results.

EXPO HALL

Engage with innovative suppliers in an expo designed to provide practical solutions to your company's operational challenges.

PRODUCED BY
FOOD ENGINEERING

2025 SPONSORS

*AS OF 1/8/25

PLATINUM

Blentech Corporation
Burns McDonnell
WT Whiting-Turner

GOLD

The Austin Company
FOODSAFE DRAINS
handtmann Ideas for the future.
UPG

REGISTER TODAY AND SAVE $100!

We look forward to seeing you this April in beautiful Tampa, FL

FOODAUTOMATIONSYMPOSIUM.COM

Cannabis flower must reach a stable water activity in a shorter time than meat or cheese to prevent microbial and mold growth.
Image courtesy of Cannatrol

ADAPTING DRYING AND CURING TECHNOLOGY FOR CANNABIS

Building on principles for drying and curing meat and cheese, Cannatrol has developed technology to control water activity in cannabis, leading to higher yields, improved terpene retention and reduced labor.

BY ALYSE THOMPSON-RICHARDS

On the surface, it seems like meat and cheese wouldn't have much in common with cannabis, but there is one thing that unites them: water activity.

Specifically, it's about controlling water activity to prohibit — or in the case of some meats and cheeses, encourage — mold and microbe growth. Building on experience with the food industry, David Sandelman, CTO, COO and inventor of Cannatrol, adapted this principle to serve the cannabis industry.

Sandelman covers the basics of drying and curing, how the process differs between meat, cheese and cannabis, and how the cannabis industry benefits from controlling water activity.

FOOD ENGINEERING: What is your background in drying and curing?

David Sandelman: My engineering background was always focused on innovative environmental control systems. The opportunity to enter the food space happened while I owned a restaurant in Vermont that was farm to table. When my wife, Jane, and I were in the restaurant business, we met many cheese makers who expressed the challenges of maintaining proper cave conditions. As I dug into the problem — simulating the conditions in a traditional cave — it became apparent that conventional cooling equipment was not suited for drying and curing. That was the beginning of development of our technology for drying and curing.

David Sandelman, CTO, COO and inventor of Cannatrol

Image courtesy of Cannatrol

FE: How would you describe the drying and curing process for meat and cheese?

DS: The physics are the same, but the parameters are different. In a cheese installation, one might require higher vapor pressure to achieve desired results, while in meat, a lower vapor pressure is required. Both meat and cheese require accuracy in vapor pressure control to manage water loss over the drying and curing period.

FE: What characterizes a successful drying and curing process?

DS: Drying is a function of reaching a specific water activity over a specified period of time. Once that target water activity is reached, curing can begin while the product is maintained at equilibrium in the space. Different products require different curing times — this is where the expertise of the maker comes into play.

FE: How does the same process apply to cannabis? What are the differences?

DS: The physics are the same in this process of adjusting vapor pressure and achieving a specific water activity, whether it's cannabis or meat and cheese. The critical part of cannabis is getting flower to a stable water activity (0.6aw) in a shorter time than meat or cheese. This ensures that mold and microbes do not grow. Whereas, in meat and cheese, we are balancing the environment to encourage desirable molds (in many cases).

Cannabis cultivators and dispensaries are reporting improved outcomes while storing flower in a controlled environment.
Image courtesy of Cannatrol

FE: How does the Cannatrol system work? How does the Vaportrol technology come into play?

DS: Unlike conventional comfort cooling systems and conventional refrigeration, Cannatrol independently controls sensible and latent heat. This creates a very precise and repeatable environment — with consistent and repeatable outcomes. Vaportrol technology is a unique approach to environmental controls that can be applied to not only meat and cheese, but cannabis and other industries where water activity and controlled removal of unbound water is critical to product quality.

FE: What's the importance of the storage aspect of this system?

DS: Storage in a controlled environment where vapor pressure is maintained will keep the product at a constant water activity. This means that products that are sold by weight — like cheese, charcuterie and cannabis — will not over dry and lose weight, thereby losing topline value. Overdrying can also seriously impact product quality. The critical piece of storage is proper, consistent control.

FE: What factors need to be considered when installing a drying and curing system?

DS: The system needs to be installed in a vaportight space. We do offer turnkey systems that include vaportight walls and ceiling, which have proved to be very popular with customers that need a quick startup or have limited infrastructure.

FE: When it comes to retrofitting existing facilities, what factors need to be considered?

DS: When it comes to retrofitting an existing facility, a vaportight space is paramount. We look at the construction of the room, ensuring that the space can be properly sealed. We also work closely with the client to review harvest cycles, wet weights and other factors that can influence how we size a specific system.

FE: What has been the response from the cannabis industry?

DS: We have had an incredible response from clients that have installed a Cannatrol system. Cultivators are reporting higher yields, improved terpene retention and reduced labor, while dispensaries using our technology are seeing increases in consumer demand and longer shelf life for flower. **FE**

Cannatrol independently controls sensible and latent heat, creating a precise and repeatable environment.
Image courtesy of Cannatrol

NEXT ARTICLE

fm food master

Start your search today

Find everything you need , right here!

- Cannabis Equipment
- Engineering Design & Construction Services
- General Plant Equipment
- Used Equipment
- Dry Processing Equipment
- Food Industry Associations
- Instrumentation, Automation
- Packaging Equipment & Materials
- Refrigeration, Cooling, Chilling/Freezing Equip.
- Services

www.foodmaster.com

MUST SEE **PRODUCTS**

A compilation of the newest food engineering technology and plant products.

FANUC

CRX-20*i*A/L Cobot

As one of the latest additions to the CRX family of collaborative robots, the CRX-20iA/L has a 20 kg payload and 1,418 mm reach, with an under-flip motion that works for applications requiring a higher payload in a small footprint. The CRX-20*i*A/L features six controlled axes and has a mechanical weight of 41 kg. The CRX 20-iA/L serves applications including palletizing, welding, machine tending, inspection, material removal and more. The CRX Series of cobots are 8 Years Zero Maintenance.

ENDRESS+HAUSER

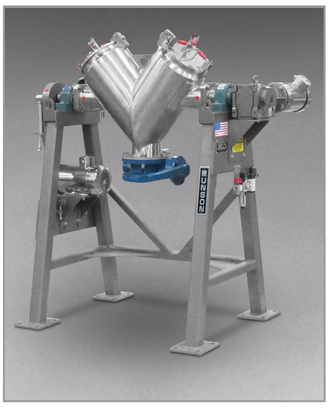
Sensors for level and pressure measurement

The new Cerabar PMP43 offers a range of sensor variants with fully welded, hygienic process connections, which are used in the food and beverage industry and the life sciences sector. Meanwhile, with the Liquiphant FTL43, point levels in almost all pumpable liquids can be detected using vibronic technology. Endress+Hauser also presents the new Micropilot FMR43 free space radar sensor for continuous, contactless level measurement. The measuring device ensures reliable measurement under rapidly changing or turbulent process conditions. The hygienic industry's requirement for even smaller process tanks was also considered during the development of the new devices. In addition to the 80 GHz technology, a one-half-inch process connection can be realized thanks to a 180 GHz frequency option, which allows use in the smallest process tanks.

MUNSON

VB-1-SSIS Vee Cone Blender

With a capacity of 1 cu. ft. (28 liters), the VB-1-SSIS Vee Cone Blender for laboratory and pilot applications features an intensifier bar and air brake. Constructed and finished to sanitary standards, it is equipped with an internal spray line with intensifier bar for rapid dispersion of liquid additions throughout the batch, and a pneumatically-actuated brake to stop rotation for loading or unloading the batch. Two inclined cylinders with smooth internal surfaces rotate end-over-end, allowing complete discharge through a lever-operated butterfly valve. The absence of residual material, combined with easy internal access through the cylinder doors and discharge valve, allows rapid sanitizing and visual inspection of all material contact surfaces, preventing cross-contamination between changeovers. The gentle tumbling action achieves uniform blends in 15 to 30 minutes. Mixing chamber rotation is driven by a 3/4 HP (0.55 kW) stainless steel wash-down motor with a shaft-mounted gear reducer, while the intensifier bar is powered by a 1 HP (0.74 kW) stainless steel wash-down motor.



C. GERHARDT

N-Realizer Protein Analyzer

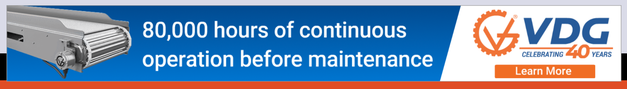
The N-Realyzer from C. Gerhardt Analytical Systems ensures high throughput, is low-maintenance and intuitive to operate. It owes this to a valve block from Festo, which offers high tightness in gas distribution. With N-Realyzer, proteins from food, animal feed or fertilizers can be analyzed using the Dumas method. Whether solid or liquid, with a high or low nitrogen content, N-Realyzer delivers results for up to 100 samples in series for any sample matrix. Its patented autosampler prevents samples from being mixed up. Thanks to the two-stage water separation, the water content of aqueous samples is completely removed. Unlike its predecessor model, N-Realyzer is cubic and no longer rectangular. It is also mounted on a turntable so all parts are easily accessible.

CHARLES ROSS & SON COMPANY

ROSS 42N-10 Ribbon Blender

ROSS Ribbon Blenders are used throughout the process industries for mixing powders, granules, pellets, grains and other bulk solids. Available in lab scale to full production models, these machines are built to handle a range of bulk densities and can be customized for heavy-duty and sanitary applications. The ROSS Model 42N-10 has a working capacity of 10 cu. ft. and is designed for free-flowing materials with bulk densities up to 100 lbs./cu. ft. The double ribbon agitator is powered by a 10HP TEFC motor and features a solid stainless steel type 304 shaft with heavy-duty ribbon support arms. This custom-made blender includes a bag dump/powder filling station per the end user's preference, as well as a 6-in. tube vent port that attaches to a dust collection system. The base legs offer 56 in. of clearance for an elevated product discharge at the bottom center of the trough.

NEXT ARTICLE



REGULATO

FDA Issues Guidance on Lead Action Levels for Processed Baby Food

Photo courtesy of Getty Images Plus / Almaje

FDA considers the following action levels to be achievable by the food industry when control measures are taken to minimize the presence of lead.

The U.S. Food and Drug Administration (FDA) has issued guidance on action levels for lead in processed foods intended for babies and young children.

The agency's Closer to Zero initiative is a science-based, iterative approach to decreasing toxic elements, including lead, in foods over time. FDA considers the following action levels to be achievable by the food industry when control measures are taken to minimize the presence of lead. Although action levels are levels at which FDA may regard a food as adulterated, the agency's Closer to Zero initiative outlines other actions it will take to further reduce lead (as well as other toxic elements) in food.

The FDA has also issued a document that presents background and rationale for its action levels for lead in processed food intended for babies and young children. Processed food in this guidance refers to packaged food (e.g., in jars, pouches, tubs or boxes) represented or purported to be for babies and young children younger than two years old. It may include ready-to-eat foods (e.g., purees), as well as semi-prepared foods (i.e., dry infant cereals).

The action levels for processed foods intended for babies and young children are as follows:

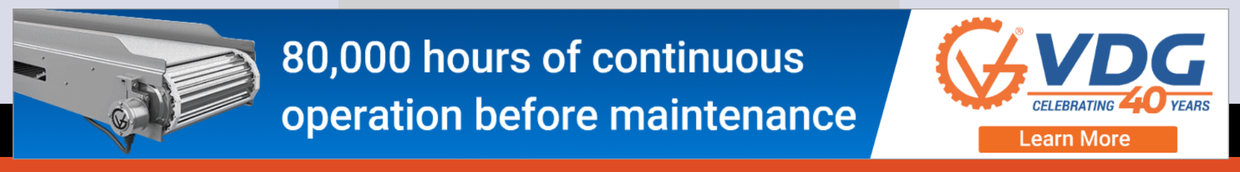
- 10 parts per billion (ppb) for fruits, vegetables (excluding single-ingredient root vegetables), mixtures (including grain- and meat-based mixtures), yogurts, custards/puddings and single-ingredient meats
- 20 ppb for single-ingredient root vegetables
- 20 ppb for dry infant cereals

Consistent with 21 CFR 109.6(d), these action levels reflect levels of lead at which FDA may regard the food as adulterated within the meaning of section 402(a)(1) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). The agency says it intends to consider these action levels, in addition to other factors, such as its confidence in a measured analytical value, when considering whether to bring enforcement action in a particular case.

In general, FDA's guidance documents do not establish legally enforceable responsibilities. Instead, guidances describe FDA's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word should in FDA guidances means that something is suggested or recommended, but not required. **FE**

NEXT ARTICLE

Masthead



FOOD ENGINEERING

Volume 97, Number 2

For subscription information or service, please contact

CUSTOMER SERVICE:
Phone: (800) 952-6643
foodengineering@omeda.com

EDITORIAL

EDITOR-IN-CHIEF
Alyse Thompson-Richards
847-405-4050

SENIOR CONTRIBUTING TECHNICAL EDITOR:
Wayne Labs

NEW PRODUCT SUBMISSIONS:
feeditors@bnpmedia.com

EDITORIAL ADVISORY BOARD

Anthony Doss, MBA, P.E.
SVP Engineering
Smithfield Foods

Samara Heaggans
Director Process Quality Engineering
Feastables

William R. Aimutis, Ph.D.
Executive Director
NC Food Innovation Lab

Dan Stauft
Director Operational Technology
SugarCreek

Hugh Roddy
Vice President Global Engineering & Project Management
Chobani

Christie Lagally
CEO
Rebellyous Foods

Bob Wolpert
Chief Administrative Officer
Golden State Foods

Gail Becker
Founder and CEO
Caulipower

Wayne Labs
Senior Contributing Technical Editor

PRODUCTION

PRODUCTION MANAGER:
John Talan

ART DIRECTOR:
Cory Emery

ADVERTISING

PUBLISHER:
Michael Leonard - Southeast
AL | AR | GA | LA | MS | OK | TX
(847) 315-0577

ASSOCIATE PUBLISHER:
Sam Wilson - Midwest
IA | IL | IN | KY | MI | MN | MO | ND | OH
SD | TN | WI | Manitoba | Saskatchewan
(847) 405-4075

SALES STRATEGIST:
John Brandt - Northeast
CT | DC | DE | FL | ME | MA
| MD | NC | NH | NJ
NY | PA | RI | SC | VA | VT | WV
Quebec | New Brunswick Ontario/Toronto
(201) 412-7060

SALES STRATEGIST:
Wayne Wiggins Jr. - West
AK | AZ | CA | CO | HI | ID | KS | MT | NE | NV
NM | OR | UT | WA | WY | Asia | Australia
British Columbia
(415) 387-7784

CLASSIFIED ADVERTISING:
Jennifer Izzo
(847) 226-6729

MARKETING

MARKETING:
Rachel Beaubien
Sr. Advertiser Marketing Manager
(248) 786-1269

AUDIENCE MARKETING:
Karen Talan
Senior Audience Development Strategist

Leigh Wendinger
Associate Director Audience Growth & Retention

Adriene Cooper
Food Automation & Manufacturing Symposium and Expo Manager
(847) 405-4120

LIST RENTAL

Please contact your sales representative.

VOLUME REPRINTS

Email **reprints@bnpmedia.com** for information.

DIRECTORIES

DIRECTORY DEVELOPMENT MANAGER:
Erin Mygal

BNP MEDIA CORPORATE

CHIEF HR & INFRASTRUCTURE OFFICER
Rita M. Foumia

CHIEF MARKETING OFFICER
Ben LeDonni

CHIEF PRODUCTION OFFICER
Vincent M. Miconi

CHIEF FINANCIAL OFFICER
Lisa L. Paulus

CHIEF CREATIVE OFFICER
Michael T. Powell

CHIEF OPERATIONS OFFICER
Nikki Smith

CHIEF EVENTS OFFICER
Scott Wolters

PANEL AND RESEARCH DIRECTOR
Ariane Claire

BNP Media Helps People Succeed in Business with Superior Information

CONTACT FOOD ENGINEERING

Phone: (248) 362-3700
Fax: (248) 362-0317

550 W. Merrill St.
Suite 200
Birmingham, MI 48009-1443

foodengineeringmag.com

FOOD ENGINEERING Volume 97, Issue 2 (ISSN: Digital 1937-4429) is published 12 times annually, monthly, by BNP Media II, L.L.C., 550 W Merrill St., Suite 200, Birmingham, MI 48009-1443,Telephone: (248) 362-3700, Fax: (248) 362-0317. Copyright 2024, by BNP Media II, L.L.C. All rights reserved. The contents of this publication may not be reproduced in whole or in part without the consent of the publisher. The publisher is not responsible for product claims and representations. **Change of Email Address:** Send an email to: foodengineering@omeda.com

For subscription information or service, please contact Customer Service at: Phone: (800) 952-6643
Fax: (847) 291-4816