AutomationWorld®
www.automationworld.com
SUMMIT MEDIA

SECURITY AND SAFETY FOLLOW PARALLEL PATHS

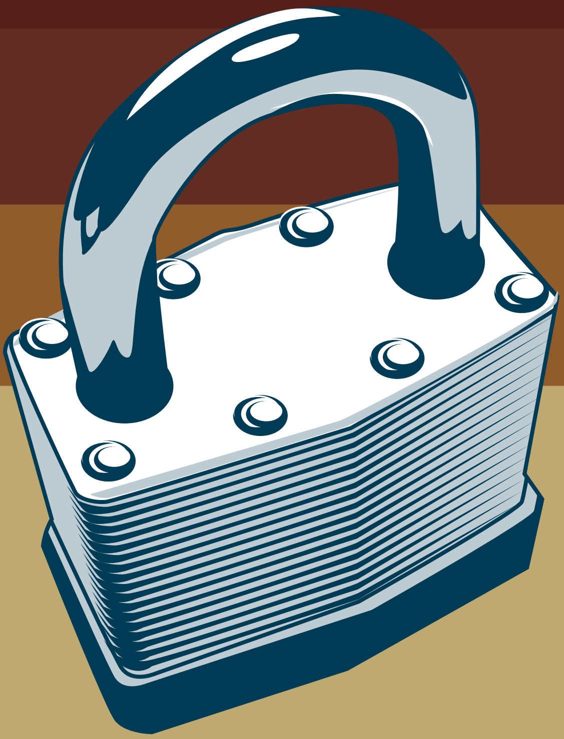
THE German word "sicherheit" means both safety and security, points out John Cusimano, director of security services at exida, a Sellersville, Pa.-based industrial safety services firm that recently added cyber-security services to its bag of capabilities.

That dual definition is just one illustration that safety and security disciplines are intertwined, says Cusimano. And in the industrial world, in particular, there are growing signs that the fields of safety and cyber security are moving into closer alignment.

One driver for the trend is that safety integrated systems (SIS), once totally isolated, are increasingly becoming connected to or integrated with process control systems that connect to the outside world. This is causing concerns in some camps that a hacker could cause safety system problems.

By Wes Iversen, Managing Editor

By picking the brains of functional safety experts, industrial cyber-security standards makers hope to make gains. Meanwhile, some companies are launching new business plans based on a **tighter alignment between safety and cyber security.**



An even bigger driver, according to many, is a growing recognition that there are many similarities between the safety and security lifecycles, and that there are efficiencies to be gained by combining the two approaches.

That's why safety specialist exida, for one, is making the move into cyber-security services. "I firmly believe that the skills, the analysis techniques and experience that we have gained in our functional safety certification work are absolutely directly applicable in security," declares Bill Goble, exida co-founder and managing partner. The company intends to provide "one-stop shopping," for safety and security services—both for vendors looking for safety and cyber-security certification of products, and for end-users looking for help in both disciplines.

"We want to make security as easy to adopt and as easy to implement as possible, and the way to do that is to align with existing safety engineering practices as closely as possible."

Bryan Singer

The perceived overlap between functional safety and cyber-security disciplines was also the driver for one of the latest moves by the International Society for Automation's ISA99 committee, which is charged with developing a security standard for industrial automation and control systems. In May, the ISA99 co-chairs announced the formation of a joint working group to include members not only from ISA99, but also from the ISA84 safety committee. The joint group, known as ISA99 Working Group 7 (WG7), had by mid-June attracted more than 50 participants, including noted experts in both safety and cyber security.

"Some people may jump to the conclusion that this is a working group to try and identify how to make SIS systems more secure. But that's not the case," says WG7 co-chair Mike Boudreaux. "Working Group 7 is focused on finding ways to take a lot of the best practices and concepts from the existing functional safety domain and apply them to the functional security domain," explains Boudreaux, an ISA84 member who is DeltaV SIS product manager at automation vendor Emerson Process Management, in Austin, Texas.

"We want to make security as easy to adopt and as easy to implement as possible, and the way to do that is to align with existing [safety] engineering practices as closely as possible," adds Bryan Singer, ISA99 committee co-chair, who is also co-chairing the WG7 with Boudreaux. "That's why it makes perfect sense to bring in the experts like the ISA84 folks who are more in tune with these engineering disciplines," Singer explains. "They can help us kind of fuse these two together where it makes sense, and where it's needed." By drawing from lessons learned on the safety side, and by borrowing where appropriate, Singer adds, ISA99 also hopes to be able to shorten the time required to develop an effective cyber-security standard and associated work processes.

There is much that the industrial cyber-security community can learn from the safety side, says Singer, principal consultant for Kenexis Security, based in Pelham, Ala. Safety standards and associated engineering work practices are mature and well established, based on decades of learning, he points out. And while safety and security disciplines do have significant differences, many safety processes and procedures have parallels in security, Singer says.

Boudreaux agrees. For example, he says, "On the front end of the security lifecycle, where you're trying to figure out what your risks are, the kind of risk analysis that you do is very similar to the type of risk assessments that you do for safety, where you're identifying unwanted consequences, evaluating the likelihood that those might occur, and based on that, you have a level of risk that you need to implement safeguards against."

In the safety world, standards such as the International Electrotechnical Commission's IEC 61508 and IEC 61511 describe methods for assigning Safety Integrity Levels (SILs) to designate different levels of risk reduction provided by a safety function. Similarly, the ISA99 committee is working on a parallel concept for security known as SAL—for Security Assurance Level. Just as Safety Integrity Levels range from SIL 1 at the low end to SIL 4 for the highest integrity level, the SAL approach, as currently contemplated, will cover SAL 1 through SAL 4, designating ascending levels of cyber-security protection.

The simplicity of that concept is something that has been lacking to date in industrial cyber security, Singer says. He tells a story about one recent evaluation interview that he went through for a security consulting job. During the interview, a potential end-user customer called him a witch doctor. "You come in here and shake chickens on the system and you make it look like this is really complex stuff, and I really have no idea what you're doing," the end-user told him. "And I have no capability to understand whether or not I actually got anything decent out of it."

Singer says he first took offense. But after contemplating the statement, he decided that the end-user was right. In the cyber-security world, "we've all been so banked up on this idea that this is so complex, and we can't possibly boil it down to something consistent and repeatable," Singer allows. When end-users hire a cyber-security consultant, they are forced "to rely on the credibility of the person," he says, with no testable, repeatable or understandable way to confidently know that the solution delivered is reasonable and will provide needed protection.

In the safety world, the SIL model "does nothing to negate the fact that safety is a very complex technical topic," Singer says. "But it is something that can be understood very quickly by anybody at any level of an organization, from the shop floor all the way up to the top floor." He is hopeful that the SAL model can do the same thing for security, while at the same time—as in safety—providing a clear, repeatable and efficient engineering-based process that cyber-security practitioners can use both to assess and design processes.

While many agree that safety and cyber security have similarities in the upfront portions of their lifecycles, there are also some notable differences between the two disciplines. A big one involves the nature of the threats. "One of the major differences between safety and security is that safety does not take into account malicious intent," observes Bradford Hegrat, lead security consultant, Network and Security Services, for vendor Rockwell Automation Inc., in Mayfield Heights, Ohio, and a member of the WG7.

Others are quick to agree. "The focus in the safety world is on designing devices that have predictable hardware failure rates. So when I install a device out there, I can predict how frequently it's going to fail throughout the life of the process for the next 20 years," says Boudreaux. "But the concept of predictable, random failures doesn't apply as well to security," he continues, because the threats come from hackers, criminals and terrorists. "With security, when you put a protective measure in place, you can't predict what its useful life is going to be."

Some believe these differences will likely preclude an effective alignment of safety and security methodologies. "Safety is all based on general statistics. So if I have 1,000 instruments, I know how many failures I will have per year, based on demonstrated MTBF (mean time between failure) rates. And when I know that, I can calculate a SIL," says Ted Angevaare, global manager of process control security and architecture at oil-and-gas giant Shell Global Solutions International B.V., in Rijswijk, The Netherlands.

But security is based on a completely different approach, says Angevaare, involving factors such as how well your system is hardened, how well your people are trained, whether you have firewalls in place, and how fast you are patching your systems. "This is what determines the risk that you have in your facility, and there is no way that you can compare that to statistical analysis of breakdowns [used in safety]," Angevaare declares. Security has nothing to do with MTBF, he asserts. "So I think it will be extremely difficult to develop a tool for doing security assessments that is like what we have done with SIL for safety."

The threat difference also has major implications for the operational and maintenance phase of the security lifecycle, which differs notably from the corresponding phase of the safety lifecycle. "Safety is somewhat of a fixed process. Once you've got the risks figured out and the processes in place and you put the safety system in, it doesn't change," observes Bob Huba, DeltaV product manager and security architect at Emerson Process Management.

Mike Boudreaux

"Personally, I think security is where safety was about 10 years ago, maybe even longer. But I think security is likely to move faster than safety did."

This contrasts to security, in which new threats are continuously emerging, Huba says. "You put in antivirus software and its life is measured in days, because there's always something new—the next conflict, or the next Sasser worm," he notes. "So it's constantly evolving, and the management on the security side is much more complex and onerous, in my opinion, than it is on the safety side."

Despite the major differences in some areas, the proponents of a combined approach to safety and security believe that the overlaps make the idea well worth pursuing. At exida, for example, Goble agrees that statistical analysis of the kind used in safety is unlikely to have a role to play in the security lifecycle. "But the rest of it is really pretty much the same," he says, especially in the upfront risk assessment and design phases of the processes.

Beginning this year, exida added cyber-security services to its longstanding portfolio of safety services, both for vendor product certification and for end-user consulting services. On the vendor side, exida in March announced a partnership with Wurldtech Security Technologies, of Vancouver, British Columbia, Canada, by which exida is licensing Wurldtech's Achilles cyber-security certification program. This will complement exida's IEC 61508 certification work for vendors on

Bill Goble

the safety side, says exida's Cusimano. Only two weeks after announcing the Wurldtech deal, exida made a move to beef up cyber-security services for end-users as well, announcing a deal to acquire Byres Research, of Lantzville, British Columbia, Canada.

The benefits to exida customers—both vendors and end users—will come through cost savings born of a more efficient approach, says Goble. "I envision a combined [safety and security] risk analysis, so you don't have to go through the process twice," he explains. This means hiring a single third-party, instead of two separate companies, to handle both the safety and security processes.

Singer envisions a similar "one-stop shopping" approach at Kenexis Security, a company that he formed last fall with Kenexis Consulting Corp., a Columbus, Ohio-based safety services firm, to provide end-user focused services in both safety and security.

Eric Byres

"If we know we have to address both of these challenges (safety and security) through the design of a plant, the worst thing that we can do is go through our existing engineering disciplines, design the plant, commission the plant, and then go back and say, 'Well now, we need to worry about security,' " Singer notes. "And that's the way it's been getting done for years." By addressing both safety and security fundamentally from the beginning, asset owners will be able to head off the need to perform a second costly process later to find and address security vulnerabilities, he says.

Wurldtech likewise is looking toward combined cyber-security and safety processes. As part of its partnership with exida, cyber-security specialist Wurldtech also gains access to exida's safety expertise. Until now, the company has focused on providing cyber-security product certification services for vendors through its Achilles program. But according to Tyler Williams, Wurldtech president and chief executive officer, the company is also looking to expand into end-user services, with an ultimate eye toward aligning security and safety processes, both for vendors and for end-users.

Among other things, says Williams, Wurldtech is working with major oil-and-gas customers on developing criteria for a process by which plant site acceptance testing (SAT) would incorporate a component for cyber security, corresponding to SAT safety requirements that companies already have in place. Then, going forward, he says, "we'd like to see a continual process where safety and security are monitored, managed and updated in the same process, on a quarterly, annual or biannual basis."

As various ideas are advanced, it is important to remember that control system cyber security is still a relatively immature market compared to safety, many point out.

Cyber Security = Safety. Get It?

There is a growing realization that cyber security—once considered primarily an information technology (IT) problem—has different ramifications on the plant floor than it does in the office. "If you look at cyber security from the enterprise perspective, there is no safety element. If, say, a Web server or a SQL server get compromised, you might lose data or you might have a financial loss, but nothing blows up, nobody dies and nobody gets hurt," points out Bradford Hegrat, lead security consultant for Network and Security Services, at vendor Rockwell Automation Inc., in Mayfield Heights, Ohio. But that's not necessarily the case on the plant floor.

"The reason we do cyber security is to have safe systems. Safety could be compromised by cyber-security vulnerabilities," says Eric Cosman, an engineering solutions IT consultant at The Dow Chemical Co., Midland, Mich. That's why the trend toward a closer alignment between safety and security disciplines is a good thing, says Cosman, who is co-chair for the International Society for Automation's ISA99 Industrial Automation and Control Systems Security committee.

Primary imperative

It has only been within the past couple of years, Cosman believes, that many in the industrial cyber-security community have truly begun to recognize the link between cyber security and plant floor safety. "One of the things we have struggled with for the last several years is explaining to people why we are so serious about security in control systems," he observes. "It's almost like, in the case of control systems, somebody had to come up with a primary imperative—the compelling reason for cyber security. And

The SAL concept, for example, "is really in the early, early stages," notes WG7 member Graham Speake, who is a risk management consultant, Information and Technology Services, Digital Security, at energy company BP, in Houston. "I think we've probably all got different views, and we have to perhaps throw everybody's idea in the ring and say, 'OK, let's discuss these on their merits,' and then try to develop things that are not so complicated that nobody will ever do it, but accurate enough that everybody will say, 'Yeah, this is something I can hang my hat on.'"

"Personally, I think security is where safety was about 10 years ago, maybe even longer," adds WG7 co-chair Boudreaux. "But I think security is likely to move faster than safety did."

Ditto for Eric Byres, chief technology officer at Byres Research, now part of exida. Byres says he has noticed a recent change lately in the pace of cyber-security standards development. "ISA99 has really started to get a head of steam behind it. There's more rigor going into the way that security standards are being developed there, and I think that's because of this transfer of good safety practices into security," he ventures.

For his part, Byres says he even expects to see some "new mathematical techniques" developed to deal more effectively with some of the vagaries of the cyber-security field. "All of the math in the safety world is very probabilistic," he notes, an approach that won't work with security. But by borrowing from other fields—maybe computer software and aviation, for example—security practitioners may be able to develop better mathematical models for looking at control-system cyber threats, Byres believes. "It's not just simply taking everything from safety and applying it directly to security. We have to modify it to make it work."

"One of the major differences between safety and security is that safety does not take into account malicious intent."

No matter what the ultimate outcome, current efforts to more closely model and align cyber security with well-established functional safety standards and practices are nearly certain to produce positive results, concludes Eric Cosman, engineering solutions information technology (IT) consultant at The Dow Chemical Co., in Midland, Mich., who co-chairs the ISA99 committee with Singer.

"I don't claim to be a definitive expert in that area, but I do know that there are people like Bryan [Singer] and others who are determined to press this concept as far as it will possibly go," says Cosman. "And there are other people who are skeptical about how far we'll be able to go with this, because unlike with safety, you can't statistically predict what a determined adversary is going to do."

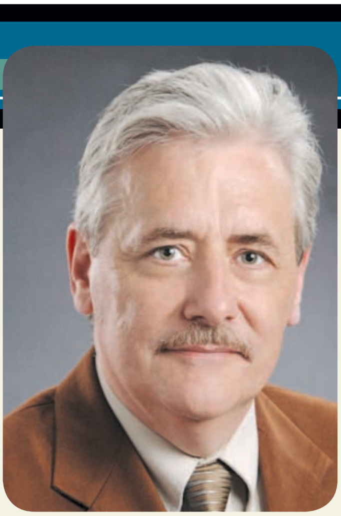
But Cosman says he is personally unconcerned with all of that. One of the biggest benefits, he believes, will come from engaging safety experts and taking advantage of all that they've learned during the past 10 to 20 years. "As we engage them, we as an industry will find out how far this model will take us, as applied to security," Cosman notes. "And even if we run into a brick wall down the road, we're still going to be further ahead than we are today."

while safety may not be the only compelling reason, it's certainly a major compelling reason."

Many industrial companies today have ingrained safety cultures. "We have gotten to the point where everybody 'gets it' at some level. We wear hard hats. We wear steel-toed shoes. We know about protective personal equipment," says Hegrat. But typically, a corresponding "cyber-security culture" has not yet developed. People still bring in Universal Serial Bus (USB) sticks and plug them into plant floor devices, despite the fact that this could infect control system networks with harmful viruses or cyber worms. And they still write their passwords on sticky notes attached to their terminals, despite being told repeatedly not to do so.

Can vs. should

That's why the big winners in the trend toward safety and security convergence are likely to be asset owners, says Hegrat. "That's really where the biggest benefits are going to happen because people will start to realize that just because they *can* do something doesn't mean they should," he asserts. "It's technically feasible to surf the Web from an HMI (human-machine interface)," Hegrat observes. "But I don't recommend it; just because you *can*, it doesn't mean you should."



Safety is a major compelling reason for control-systems cyber security, says Dow Chemical's Eric Cosman, who is ISA99 co-chair.