Best's Insurance Professional Resources

# Best's Insurance Law Podcast

## Mitigating System Control Failures - Episode #219

Posted: Thur., Sept. 26, 2024

**Hosted by:** John Czuba, Managing Editor
**Guest Expert:** Rob van Akelijen from S-E-A
Qualified Member in *Best's Insurance Professional Resources* since: 2021

**John Czuba:** Welcome to "Best's Insurance Law Podcast," the broadcast about timely and important legal issues affecting the insurance industry. I'm John Czuba, Managing Editor of *Best's Insurance Professional Resources*.

We're very pleased to have with us today Robert van Akelijen from Qualified Member expert service provider, S-E-A. Rob earned his Bachelor of Electrical Engineering from the Georgia Institute of Technology.

He has more than 27 years of experience as an automation specialist, with a demonstrated history of working in the oil and energy industry. He is skilled at analyzing losses, failures, and developing optimization strategies by evaluating control systems design, including hardware specifications, design drawings, installation, and source code.

Prior to joining S-E-A, Rob worked in a wide range of process plants and manufacturing facilities. His responsibilities have included estimates and proposals, front-end engineering design, detailed control panel design, program development, commissioning, startup, as built documentation and project management.

Rob is a registered professional engineer in the states of Illinois, Indiana, Kentucky, Michigan, Missouri, Ohio, Pennsylvania, West Virginia, and Wisconsin. His professional affiliations include, the International Association of Arson Investigators, the National Fire Protection Association, and the National Association of Fire Investigators.

Rob, we're very pleased to have you with us today.

**Rob van Akelijen**: Thanks for having me, John. I appreciate the opportunity to speak to your listeners.

**John**: Thank you, Rob. Today's discussion is mitigating system control failures. Rob, for our first question, what is an industrial automation and control system? Where do you see these systems in use in everyday life?

**Rob**: Well, control systems are everywhere. The human body has some excellent control systems. A good example is how we're able to regulate our body temperature. If we get hot, we sweat to cool off. If we get cold, our body will concentrate our body heat to our core and keep our vital organs functioning.

Our homes are full of control systems, from a coffee machine regulating the temperature of the water, to a washing machine going through the batch process of washing your clothes, to an HVAC system heating and cooling your home.

In a more traditional sense, an industrial automation and control system can be found in almost every manufacturing environment, from chemical plants to car manufacturers and everything in between. The hierarchy of a control system starts at the field level with the end devices.

These are your inputs and outputs. These can be level temperature flow, pressure transmitters, or switches. They can be analog control valves. They can be simple open and close valves. They can be variable speed drives or constant speed motors.

An example would be a tank that has an incoming production line. It may have an end device such as a control valve on that line to regulate the flow into the tank. This would be via another end device, a flow transmitter. That same tank might have a discharge line that contains a pump which is another end device to move production out of the tank.

Let me tie this into an example in your home, and I'm going to focus on a home HVAC system since it's quite similar. On an HVAC system, these end devices can be a pressure switch to detect air flow or a gas control valve that regulates gas flow to the burners.

The next level in a control system hierarchy deal with the actual controller. Going back to the HVAC unit in a house, this is typically a printed circuit board that has all the circuitry to tell the unit when to turn on or off, when to cool or heat. In an industrial setting, these are typically programmable logic controllers or PLCs which are industrial computers. There're many suppliers of PLCs, and they typically come with supplier provided software to configure the program to plant specifications.

These PLCs are typically housed in racks that can accommodate different input and output cards, which are dependent on the design of the system. It makes these PLC configurations very modular to design and also easier to make changes or additions to a system.

The next level in a control system hierarchy deal with plant supervision. Once again, using the HVAC system in a house, this is typically the thermostat where the temperature can be monitored, temperature set points can be adjusted, or complete schedules can be set. Similarly, in an industrial setting, plant supervision is typically done with human-machine interfaces or HMIs. These HMIs are screens visualizing a plant, as well as alarm notifications. HMIs are typically housed in a plant central control room. This is where operators can monitor production, adjust set points when needed, and respond to plant upsets and alarms as necessary.

The final level in a control system hierarchy is production control or data collection and analysis. Thinking back to your HVAC unit in your house, this is akin to a smart thermostat, like a Nest, where a homeowner can see usage history and decide whether to make changes to the schedule to save money, or maybe they see something in a trend that's indicative of an inefficient or failing unit, perhaps not being able to maintain temperature in the house.

In an industrial setting, this production control may be called a historian. This can be built into an HMI or can be a third-party piece of software collecting data from the automation and control system. Operators and engineers can use the historical data to analyze an incident and see if they can diagnose the root cause. Business management can use the data to analyze the efficiency of their operations.

**John**: Rob, can you describe some different automation and control system failures?

**Rob**: Yeah. I want to start off by saying that a component failure in an industrial control system does not constitute a control system failure. It's how that control system reacts to the component failure that would determine a control system failure. As an example, and of course, we'll go back to that home HVAC system.

If a pressure switch fails, the proper response would be that the unit does not turn on. The pressure switch would need to be replaced. However, what happens if that pressure switch fails in a way that the HVAC unit can still start with, say, a clogged intake line? What if the wiring was modified to bypass the pressure switch? If the unit is able to start without proper airflow, there could be a fire.

It's the same situation in an industrial environment. What happens when the level gets low in a tank? Maybe that pump I mentioned earlier needs to turn off. What happens if that level transmitter fails and stops changing values, but the actual level gets low? That pump would continue to run without fluid flow and damage the pump. That would be a failure of the control system.

**John**: Rob, what can be done to help mitigate these potential failures?

**Rob**: OSHA has a process safety management regulation for plants using hazardous materials. While it's a regulation for highly hazardous chemicals, it's a great practice to voluntarily use this OSHA regulation for any facility. The regulation consists of 14 different elements. We don't have time to get into all of them, so I wanted to focus on a couple that I think are most critical to the success of an automation and control system.

The first is a process hazard analysis or PHA, for short. A PHA is critical to the successful operation of the facility. I like to call it a “what-if” analysis. There are different ways to perform a PHA, but typically, there's an impartial facilitator with representatives from management, engineering, and operations.

The facilitator goes through the plant drawings and control narratives, reviewing each piece of equipment, including all the instrumentation and process lines, and asks the group, what if this fails? The answers go into a risk matrix along with the likelihood of it occurring and the estimated damage cost to determine the severity of the risk to human life, the environment, equipment, and production.

Based on the outcome of this risk matrix, additional safety layers may need to be added to an automation system to prevent the loss of life, environmental damage, etc. This could be as simple as adding an alarm to alert operations of a plant upset.

It could be a little more complex such as adding an additional redundant instrument, say a temperature sensor to a piece of equipment to ensure that the system is getting an accurate reading. It could be complex enough where a second independent control system, one that is safety-based instead of process-based, needs to be added to protect the plant from a catastrophic disaster.

The next item is training. Training is so important to a plant's success. This goes beyond having operating procedures, which is also one of the 14 elements. The operators need to have proper training to truly understand the process and what dangers may be present when something goes wrong. This helps them quickly recognize when something is not right, and the steps needed to mitigate the problem.

Lastly, and this isn't one of the 14 process safety management steps, but the programmer of a control system is vital. A PLC program is only as good as the programmer. If you gave 100 programmers a control narrative and told them to create a program, you would get 100 different programs, and they may all work.

Like the operators, a good programmer will want to understand the process and not just when things are functioning. System testing before going live is critical. A good programmer, in collaboration with engineering and operations, will come up with plant upset scenarios to test the robustness of a program. Simulation software can be configured on top of the PLC program to simulate responses to the control actions of the controller.

I've been asked to review PLC code in the past and all too often the feedback I give is that the program will work per the control narrative as long as nothing goes wrong, and that's not good enough.

These are just a few causes of mitigation but there are so many more things that factor into failures such as proper installation, preventive maintenance, and environmental conditions, just to name a few.

**John**: Rob, one final question for you today. What type of cases do you investigate as relates to automation and control systems?

**Rob**: We at S-E-A can investigate almost anything in a manufacturing or a process environment if it's suspected to involve the control system of a plant. It could be in relation to an injury to a human, environmental damage, equipment failure/damage, or loss of production. Automation and control systems leave a footprint that can be analyzed after the fact. A PLC program can be reviewed for its robustness.

Many plants have an archive of old PLC programs with descriptions of the revisions so we may be able to tell if a recent program change is the cause. Operators, engineers, and programmers can be interviewed to develop a timeline of events as they saw them. Many facilities have the historical data, which can be filtered to investigate the exact timing of a plant upset and what factors contributed.

A couple of examples; I've seen where an operator was performing maintenance on a control valve and they placed the valve in manual to check that the actual position of the valve matched the commanded position of the valve. After the operator was done, they mistakenly left the valve in manual control, and in this case, it was adding water to a tank. That tank eventually spilled water over the top of the tank.

We were able to look at the historical data and pinpoint the time when this maintenance started, how long it took until there was an overflow, what alarms were missed or ignored, and what additional safety layers should have been implemented that could have prevented the spill. In this particular case, there was no override in the program to close the valve on high level when the valve was in manual. This protection was added after the incident.

In another case, an operator opened a safety door to fix a jam on a piece of conveyor. Unfortunately, the safety switch on the door didn't disable every single possible movement of the conveyor, and the operator was injured by the conveyor moving unexpectedly. The PLC program allowed for the movement of the conveyor under certain conditions. We were able to analyze the PLC code and show exactly where in the program that this was possible.

I've looked at some cases in an industrial environment where it ends up being something other than the control system failure, and I've needed to utilize another engineering discipline to investigate that failure. Other times, I've been called in by another engineering discipline when the failure ended up being control system related. Luckily, at S-E-A, we have every discipline that can cover the investigative needs. If any of your listeners have any questions for me, they can go to S-E-A's website and they can find me.

**John**: Rob, thank you so much. That was a very informative podcast today.

**Rob**: Thanks so much for having me today, John. I appreciate the opportunity.

**John:** You were just listening to Robert van Akelijen from qualified member expert service provider, S-E-A. Special thanks to today's producer, Frank Vowinkel. Thank you all for joining us for “Best's Insurance Law Podcast.” To subscribe to this audio program, go to our web page, www.ambest.com/professionalresources. If you have any suggestions for a future topic regarding an insurance law case or issue, please email us at lawpodcast@ambest.com.

I'm John Czuba, and now this message.

Transcription by CastingWords