All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Safety better win!

You want to connect that operational technology (OT) to your IT network for lots of good reasons. And we support you. However…

- Safety must always win

It may seem obvious, but apparently, it is not. Here's an example. There is an elevator that carries heavy things and people into and out of a mine. It is fed by a conveyor belt except when people are using it.

- The conveyor belt has controls that allow it to run at different speeds, from STOP through MAXIMUM.
  - It has a BIG RED BUTTON a person can press to emergency stop the belt.
    - Until the button is pulled back out, the belt will not move.
- The elevator has controls that allow it to go up or down at the one speed it operates.
  - It has a safety mechanism that prevents it from running when it's over loaded.
    - Until the weight is reduced.
  - It has a BIG RED BUTTON a person can press to emergency stop the elevator.
    - Until the button is pulled back out, the elevator will not move.

Pretty good – yes? Pretty safe – yes?

No!!! - The Devil is in the details

There no doubt remain failure modes. Here are some examples:

- It's a mine! If we overload the elevator while there are people inside the mine, they cannot get out until they unload the elevator. That's because the "safety mechanism" won't let them use the elevator.
- Nothing here prevents people being in the elevator when the belt is running, dumping mining material on the people.
- How is the elevator being prevented from moving? If it is being clamped down by a brake, that doesn't prevent the cable from trying to pull it up. What if the cable and motor are strong enough to overwhelm the brake? What if the next cable replacement is stronger and the motor gearing is changed? That doesn't make the elevator safe from the higher loads… suppose the floor falls out?
- How is the belt stopped from moving? What if a motor for the belt is switched on and off repeatedly, causes the belt to shake even though it move forward or backward, and what if the shaking causes something to fall off the belt onto the back of the big red button, un"STOP"ing it.

There are always failure modes. The question is:

 Copyright (c) Fred Cohen, 2019 - All Rights Reserved

What do we do about them?

We need to think about them! It's not just a design issue. It has to run through the lifecycle. And it implies lots of other things. Some of the notions shown above include:

- **Fail safe modes:** Failures should produce safe modes where anticipated. This also implies no "undefined" states for machines.
- **Emergency stops:** Where the consequences are high enough (e.g., loss of life, harm to the environment, etc.) emergency stops should be tied to the physics of the mechanisms and locally controllable without override.
- **Safety not overpowered by controls:** The sum of all controls should never be able to override a safety mechanism. Unless of course that is the design intent.
- **Design intent:** Somehow, the intent of design should be codified so that those who maintain, upgrade, operate, etc. the system know about it. Otherwise, how will the crew repairing the elevator know not to use the better cables now available and the different motor and gearing setup?
- **Maintenance processes:** Of course, for maintenance processes to work properly, they need to keep design intent in mind AND be able to use the safety mechanisms so as to keep the maintainers safe as they crawl around the gears that move the belt. Please don't pull this stop out or you will kill me! Lock out tag out!

Remember Fukushima!

Do not misinterpret my desire for local safety mechanisms to imply that you should not have the ability to remotely control dangerous things. One of the reasons Fukushima lasted so long and did so much harm was apparently (I have not done a thorough analysis of it) that there was no remote control mechanism for the plants when they became uninhabitable. If there had been an emergency mode to allow remote control to be enabled when the control rooms were abandoned, it might have been possible to mitigate more of the harm.

Which is to say, in addition to the efficiencies or remote control, even in high consequence situations, there is also a value to the redundancy of remote as well as local control, when there is a need for it. Invoking that need only under the right conditions then becomes the safety and security issue.

Mine safety also involves things like gas that can kill the miners and cause explosions. It's pretty important to know when there is gas present, and these days we use sensors instead of canaries. Having remote access to the sensor data and the ability to control the fans that send in the new air and take out the bad air is all the more important when the miners cannot do it themselves. We cannot count on miners throwing the "HELP" switch to enable remote control when trapped in an air pocket in an explosion. But that doesn't mean we want workers at the beach to turn off the fans by accidentally butt dialing the plant while on vacation.

Conclusions

Horses for courses. Safety systems and controls that have safety-related effects have to be designed and thought through, implemented with proper surety, and taken in the specific context of the OT environment they are designed for. IT efficiency is great, but OT caution is also extremely important. There's no one "right" way, but there are plenty of wrong ways.

 Copyright (c) Fred Cohen, 2019 - All Rights Reserved