The Gizmo Society

George Holling

It is hard these days to find any device that is not IoT-compatible or WiFi-connected. I recently had a new well pump installed that requires an iPhone for setup, which makes it hard for me to check or change the setup since I do not own an iPhone. In Olden Times, you had potentiometers or RS-232 connections — and that was fine.

When I came out of engineering school, the microprocessor had started to take over. With a microprocessor we could do everything, and when I graduated I was eager to prove it. But I quickly learned that my senior co-workers were focusing on many other features and design aspects. While performance and flexibility were important, the focus on safety was even more important.

So a few valuable lessons were quickly instilled in me:

- There always is a safety shutoff (red mushroom button) that kills the power
- Never, ever rely on the computer to shut the drive off
- Always have safety features; e.g. — a watch dog timer (WDT) to check the computer along with a hardware path (external hardware WDT) that will cut the power when things go wrong
- If anything does not check, turn it off

And while I initially may have considered this a waste, it turns out that these features saved myself trouble quite a few times. All it takes is one incorrectly entered number and things quickly fall apart — in some cases quicker than you can imagine. That is where the red button comes in handy.

I will readily admit that, in a lab environment, we do not always follow these requirements as religiously as we do in an actual industrial application. And there are times when you quickly reach for the OFF button on a power supply when things do not go as planned. But these are typically small motors with little chance to do any damage in the event of failure.

As the motors become larger, or the potential speed become higher, our lab tests are fully set up with multiple E-stop buttons and multiple personnel — especially in situations where the loss of control or a run-away condition poses a physical threat to the people or the facilities.

One such experience was when we installed a starter/generator on a newly developed turbine engine that was started for the first time with about 20 personnel present in the "bunker." A chain of command was established that could initiate an E-stop and determine which conditions warranted an emergency shutdown. The actual test was much less impressive. Everything ran fine and no intervention was needed, except for a normal shutdown command.

Today everybody has a fascination with connectivity, which is not inherently a bad thing, but it can quickly turn bad if safety is ignored. For instance: Who/what controls the drive and what safety features are present? A bad command, just like a bad number entry in my younger days, can have disastrous consequences without the proper safety mechanisms. Do you solely rely on sensorless feedback or do you have a secondary hardware loop for added safety?

Even if things go well on the drive level and the drive is network-connected, the question remains: "Are we properly protected against network failures?" How do you detect a network failure and how do you respond? A processor can easily lock up while the LAN connection may still appear to be functional.

Now we make the problem worse by adding WiFi into the equation.

A few years ago we completely rewired our wireless office with all name brand commercial equipment and switched back from WiFi to a hardwired LANs. Since then our productivity has soared, data losses were almost completely eliminated, our central servers are now instantly updated and our network could no longer be easily monitored or manipulated from the outside. Even though we would like to think our standard network encryption is well protected, that is not the case; WiFi encryption keys are easily discovered and bypassed. Wireless networks are simply not as reliable as hardwired networks — and they may never be. They are susceptible to interference from other HF sources, electrical noise, etc. I remember the times when my PC network locked up when all I did was use my cell phone. And yet I do believe the newer frequencies have fixed that issue.

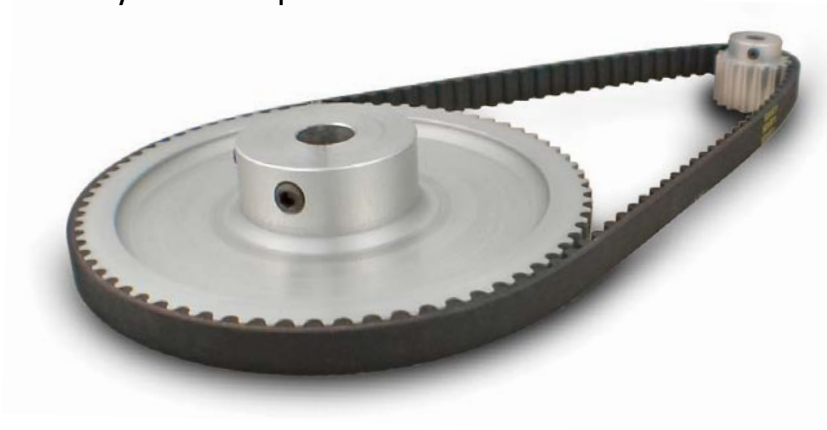
Now we add the smartphone into the mix, where the apps may simply

SDP/SI

STOCK DRIVE PRODUCTS/STERLING INSTRUMENT

SETTING YOUR DESIGNS INTO MOTION

Stock Drive Products/Sterling Instrument is a Contract Manufacturer for synchronous drive system components and sub-assemblies



Get the NEW Inch Master

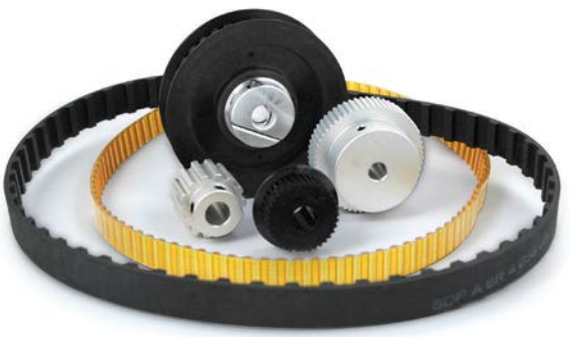
Catalog D820

Large Off-the-Shelf Selection of Timing Belts

We offer a wide selection of timing belts from stock in different widths and materials. Available profiles are: Miniature FHT, MXL, 40 D.P., XL, L, HTD, GT2, GT3, and T.

SEE OUR TIMING BELT SELECTION

www.sdp-si.com/products/details/timing-belt-detail.php



Cutting Timing Belts to Your Specifications

As a Gates partner we stock an assortment of timing belt sleeving giving us the ability to cut custom widths on demand.

CONTACT US FOR A QUOTE TODAY

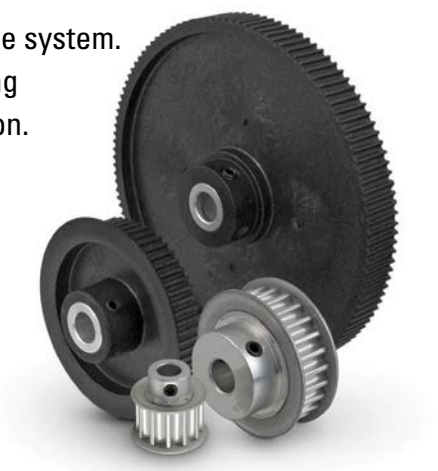
www.sdp-si.com/contact/quote.php

Manufacturing Pulleys for More than 50 Years

Get high-quality machined and molded pulleys to complete your drive system. Corresponding pulleys are in stock to match with our complete timing belt offering. Discover the parts that will work best in your application.

USE OUR CENTER DISTANCE TOOL

www. sdp-si.com/eStore/CenterDistanceDesigner



Custom Drive Systems

If a stock item won't meet your need, our engineers can offer cost-effective solutions, from simple modifications to a custom part.

SEND US YOUR PRINT FOR QUOTING

Stock Drive Products / Sterling instrument

Phone: 800.819.8900 | Email: sdp-sisupport@sdp-si.com | Buy Online: https://shop.sdp-si.com

not have the required safety features to deal with the loss of connectivity, as they were written by young college grads who may know about networking but who have little understanding of the physical dangers of operating industrial drives and plants, where even small errors can quickly have devastating consequences.

True, some of these thing can also happen in stand-alone equipment or when using a hardwired LAN — but they are less likely to happen.

I hear the firestorm already; but I stand by my opinion for the reasons outlined above.

I am all for automation and I believe that automation and AI will continue to proliferate, which is good and beneficial. But that does not mean every piece of equipment has to be controlled via smartphone. My answer is, and will be, NO for the foreseeable future. There still is — and will be — a need for dedicated controllers or PCs and safe, hardwired networks that do not allow for any inadvertent access.

Yes, our lives evolve around our smartphones. But do we want to stake our business on it? How do we insure that the system works reliably? How can I be sure that hackers do not gain unauthorized access? And how do we make sure that someone is not simply goofing off or trying out something that can inadvertently result in major damage?

We are currently trying to set up a new building with smart light bulbs. All of the manufacturers push their mobile control apps, and we had to exclude several products that do not offer PC applications. Why? Because building codes have special requirements and the building must continue to run and lights must turn on and off — even when a specific smartphone is somewhere else. So while it may work for one-room recreational use, it doesn't work for any large-scale practical use.

Do we really need smartphone apps to control industrial networks or is it just a lazy "shortcut" that adds risk without significant benefits? After all, whose smartphone will be in charge of the plant and its equipment? If you simply wanted to know how the plant is running, you could use your smartphone to look up the current production reports and status information online without having access to individual machinery instead. That is why we intentionally create boundaries that keep key systems safe and then use information tools to share this information with those that need to know.

With our lives playing out on Facebook, and living in a household managed by Amazon's Alexa, we are way too focused on the cool gadgets and gimmicks. Gizmos control our lives, but when we apply these designs for gizmos to industrial automation, then the gizmos may truly control our lives and wellbeing.

Technology offers great opportunities, but it also demands respect. Just because we can do something does not mean we should. On the way to an airport, I was listening to an interview where a truck driver was testing autonomous vehicles for his employer — a company that develops self-driving technology. This company wants to run autonomous trucks from town to town, and when they arrive in a town a remote-controlled driver takes over. I do not know about their networks, but the ones I know suffer from regular and occasional hiccups. What do you do if the connection to the remote driver disconnects — hit the brakes and stop without warning and have everybody slam into the truck?

Why am I nervous about this concept? Because I have my concerns about self-driving cars; yes, statistically they may be safer, as opposed to a distracted human, especially when we have the dangers of texting and driving. But a hybrid system that relies on wireless technology makes me feel uncomfortable. Nothing will go wrong — right?

George Holling holds significant influence in two companies — as technical director of Electric Drivetrain Technologies (2011–present) Moab, UT and as CTO of Rocky Mountain Technologies (2001–present), Basin, MT; *George.Holling@RockyMountainTechnologies.com*