All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Mobility and industrial control systems

The ICS community, as well as other communities, have been increasingly concerned about mobile applications being granted control to controls. This is essentially the same as the issue of remote control over critical IT infrastructure like routers and firewalls, remote control over telephone switching centers, and the list goes on. Typical concerns are things like drunk operators controlling things from a local bar, someone stealing the remote control device and using it, someone breaking into the remote control device and exploiting it, and so forth.

What are the real issues?

It seems to me that mobility is not the issue here, and neither is remote control. We daily trust mobile control systems and would not have it any other way. Our cars, for example have mobile control devices (steering wheels, etc.). Co-location, not mobility is the issue in this case. Airplanes have non-collocated controls (i.e., remote control of aircraft for emergency landings have been around for some time). So do missiles. And drunk operators can be at the plant just like at a bar. Mobility is not the problem here, it's the mental state of the operator. Before you jump up and tell me that you can better control drunkenness at the plant, let me save you the time.

The issue at hand, as always, is the protective architecture and the control scheme that implements it. Simply adding mobile devices to existing SCADA systems likely creates an architectural change not anticipated and properly architected by the folks who put the ICS in place. It also likely requires a different control scheme in order to achieve the same operational properties. As a result, in simply adding mobile devices to an existing system, it is highly likely that the new architecture doesn't have the same protection and safety properties as the old architecture and that the control scheme doesn't properly provide for adequate control over the new overall architecture.

Think of it like a building. If you add an extension onto the 2nd floor of your house (say it goes 100 ft out above the street your house is located near) and do so without proper architecture and design (we're going to use a 2x4x1200 board glued to a window to hold it up), it is likely to fall and break something. Fortunately, we have building codes and inspections and architects, and builders, etc. that help make sure we don't do such things.

I am pretty sure I can architect for mobile access to nuclear weapons controls (the US President apparently has one). Whatever you have likely doesn't have more severe potentially negative consequences than that. But you might not like the costs of gaining adequate surety for your application (no failures of the President's control system in 50 years or more).

Conclusions

Today, companies tends to build devices and programs that can be connected through IP with minimal effort. They normally don't have well defined properties, and we don't have an engineering discipline for building composites with desired properties out of components with properties. I think we need to build the building, engineering, and architectural trades and require their use if we want IT systems to operate as composites with desired properties.

