Control Is Not Data

Andrew Ginter, Waterfall Security Solutions

IT gurus tell us that control system security is essentially the same as IT security, and that both are about "protecting the data." The gurus tell us that, yes, there are two kinds of "data" in control systems - monitoring data and control data - but "data is data." They tell us that all we need to do is protect the CIA, or AIC, or IAC, or something, of the data and we're done - we're secure.

They are wrong.

These IT people do have one thing right - monitoring data is just data. The consequences of stealing or interfering with monitoring data are comparable to the consequences of stealing or interfering with other kinds of IT data.

The IT people have it entirely wrong when it comes to "control data." The consequences of mis-controlling physical, industrial processes are almost always completely disproportionate to the consequences of stealing monitoring data. Most of the time, IT protections are entirely inadequate to ensuring correct control.

In fact, correct control is almost always so much more important than monitoring data or IT data, that it's very misleading to call both "data." We should really be talking about "data" and "control" as two entirely different things.

Think about it - SCADA practitioners generally care very little about who is looking at their gauges through binoculars. Looking at gauges through binoculars doesn't kill people, cause environmental disasters, or trigger plant shutdowns. SCADA practitioners generally care enormously about who is standing at the controls, turning the dials. They care even more that the dials are turned to safe, correct settings. Control is enormously more important than monitoring data at the vast majority of large industrial sites.

The third law of SCADA security states that all attacks are information, and every bit of information can constitute an attack. The only way an industrial process can change from an uncompromised to a compromised state is if attack information crosses a physical or network perimeter. Every message entering a network, even a benign-seeming query, alters the behavior of the CPU receiving the message, otherwise there would be no point in sending the message into the network in the first place. Every message entering a control network, even a message intended only to retrieve monitoring data, is therefore a kind of control, capable of compromising the control network. In the worst case, every CPU in a compromised network will issue every unsafe instruction to the physical process that the CPU is physically, electrically able to issue.

Increasingly, new standards and guidelines recognize this vital difference between monitoring and control, even if the terminology lags. Advice such as the French ANSSI standards, the new Industrial Internet Consortium Security Framework, and the recent DHS NCCIC ICS-CERT Defense in Depth document, all recommend or require network designs using unidirectional

gateways. Unidirectional gateways support monitoring of industrial networks, while physically preventing misoperation or compromise of those networks from less-trusted networks.

Monitoring data deserves IT-class protections, but control is enormously more important. Our security advice and security programs need to say this much more clearly. An essential step towards greater control system security is to stop talking about "protecting the data," and start talking about the vital differences between data and control.

Andrew Ginter is the VP Industrial Security at Waterfall Security Solutions, an Adjunct Assistant Professor at Michigan Technological University, and the author of "SCADA Security - What's broken and how to fix it."