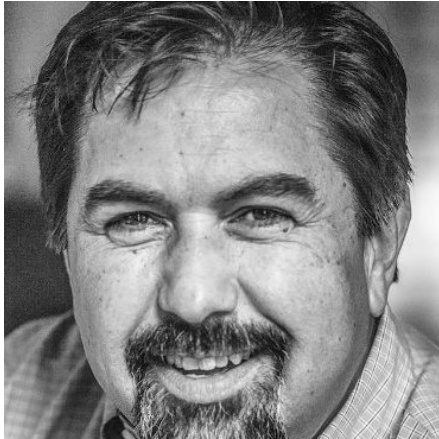>> 2016 hacks caused financial (possibly political) impacts
>> Hacking control systems has kinetic (physical) impacts
>> Brief video discusses importance of defending levels 0&1 in control systems

This [short video](#) features Carlos Solari, Senior VP of Cyber and Services at Mission Secure offering a brief summary of control systems and how hacking the lowest levels 0 and 1 can lead to a variety of adverse *kinetic* impacts.

Hacking email vs. control systems

As 2016 draws to a close and hacking remains on the front page of the news, we are reminded of the important role control systems play operating most everything in <u>all</u> sectors of critical infrastructure. In the military it is the weapons systems, ships, planes and UAVs. In other sectors it is the industrial processes across oil and gas, power, transportation, buildings and more – the kind that sustain life and keep the economy going. These control systems were designed for reliability and safety, not defending against cyber attacks.

Control systems have become increasingly automated and interconnected, often called the Industrial Internet of Things (IIoT) and operational technology (OT) with thousands of sensors and actuators running critical processes, managed by highly automated controllers monitored and run by human operators.

Traditional cyber attacks focus on stealing information for political or financial purposes ([DNC political emails](#), [Pentagon Joint Chiefs of Staff emails](#), [1 billion users at Yahoo](#), [central bank money transfer systems](#)), blocking access to or destroying information ([Medstar health](#), [Shamoon 2](#) in the middle east). Cyber attacks against control systems try to disrupt operations resulting in a kinetic impact ([250,000 customers lose power in the Ukraine](#), [San Francisco train system shuts down](#), cause an [oil rig to tilt and shut down](#), [blow up a plant in Germany](#),

[shut off the heat to residential buildings)](#).

The military speaks of "kinetic," as in physical destruction. Unfortunately, the same description is appropriate for the commercial sector. In addition to military targets, civilian-commercial services are targets like the fuel we use to drive our vehicles, warm our homes and keep on the lights. News surfaced earlier this week about another possible cyber attack on the grid in the [Ukraine](#). We should all be paying attention to level 0 and 1 in control systems in 2017.

The Mission Secure team wishes you all the best during the holidays, and a happy, safe and secure 2017.