Implementation of SCADA in Energy Industries: Vulnerabilities, Case Studies and Best Practices

Mike Bingle-Davis[1]

[1]Kirkwood Oil & Gas

Abstract

Supervisory control and data acquisition (SCADA) were first implemented in the 1960s as a means to monitor and control automated processes. The evolution and expansion of computer systems, interconnectivity via the internet and accompanied technological advancements occurred at a slightly faster rate than SCADA. This stepwise integration and employment of SCADA has increased efficiency across many industries and within the context of this presentation a focus will be made on energy generation industries regarding upstream, midstream, and downstream. As SCADA is a hybrid of hardware and software while also integrated into existing network infrastructure there can be some difficulty in adequately determining vulnerabilities from threat actors both internal and external. A small sample of these vulnerabilities include legacy hardware capability with communication protocols, correct configuration, properly trained operators, and over reliance. The one of the most well-known shock to reliance on SCADA was witnessed in the 2010 Stuxnet attack against the Iranian Natanz uranium enrichment facility. In addition to this attack there are a multitude of others including Night Dragon in 2010, Duqu, Flame, and Gauss in 2011, Shamoon in 2012, Bowman Dam in 2013, Ukrainian power grid in 2015, CRASHOVERRIDE (Industroyer) in 2017. This list is not complete and attacks are ongoing throughout energy industries. Knowing that these risks are present it is important to understand what a company do to protect itself from these types of attacks. Following a set of best practices, understanding the penetration methods used in evaluating SCADA systems become essential. The hardware-software gap seen in SCADA system in conjunction with the lack of industry professionals make this information imperative as we move forward in implementation.