How vulnerable are SCADA systems to attacks?

On 23rd December, 2015, an attack against the Ukrainian power firm, Prykarpattyaoblenergo, put 225,000 Ukrainians into darkness. According to a [BBC report](http://www.bbc.com/news/technology-35204921), the attack was carried out by targeted phishing emails that allowed attackers to get access to the plant’s control system. The malware used in this attack was was very specialised, and was designed specifically for this attack. Although, these kind of specialised attacks are usually difficult to pull-off, the report also discusses how SCADA (Supervisory Control and Data Acquisition) and IC (Industrial Control) Systems might be vulnerable to attacks via other means, as a large number of them are connected to the internet, and have poor security features.

According to the report, direct attacks on such systems are well targeted, because no two installations are the same. The attacking malware is designed with an in-depth understanding of the victim SCADA systems. The need for expert knowledge usually acts as deterrent to prevent such attacks. This was observed at the Ukrainian attacks as well (where this deterrent failed); the analysis report by iSIGHT Partners revealed that the attackers put significant time and effort for crafting the attack. However, according to Sergey Gordeychik, coordinator of the group [“SCADA Strangelove”](https://en.wikipedia.org/wiki/SCADA_Strangelove), a large number of these systems are connected to the internet directly, so as to offer remote control features. But unfortunately, the security standards of these systems are decades old, making them extremely vulnerable to attacks. Usually, these systems are connected to poorly protected corporate IT systems, and the attackers try to access these ICS through these vulnerable systems. SCADA Strangelove is trying to create awareness regarding these issues, and they have certainly received positive response from the community, but a lot of work is still needed.

The lack of proper security in these systems is really concerning, because these systems control some of the biggest infrastructures of our society. As demonstrated by the attack in Ukraine, more attacks like these are definitely possible. With the ongoing trend of connecting everything to the internet, and the “smart-everything” movement influencing these industries, protecting these assets should only get more challenging.