Non-Technical Summary

* The field of DCS/SCADA for non-technical people and what it does
* How there were security problems were notorious until upgrading to the cloud
* How data is the main important part now, especially data historians and the arrival of the cloud.
  + Cake analogy
  + Toray plant
  + Data is the important priority
* What approaches to take to preserve data security
  + Current/Future industry requirements
  + Technologies that can be used to protect
  + End goal of data protection

Distributed Control Systems are a significant part in the daily lives of citizens across the world. DCS handles the production and consumption of wastewater treatment, electricity generation, and other large-scale processes. Across decades of technological improvements, the scalability of DCS went from large city production to regional distribution. However, the computers and machines over the years of progress were not replaced every time with up-to-date security improvements resulting in long-term infrastructure vulnerabilities.

In the post-cloud era, companies managing DCS now have incentives to replace outdated hardware to connect devices within the Internet of Things. Holes in network security are filled with new updates and greater importance on cybersecurity in DCS plants. Typically, data in DCS is stored on the data historian—a computer that records all processes occurring within a plant. While the historian is kept under tight network security, the data must be moved around throughout the plant for operations and in the cloud for performance analysis.

Unfortunately, the data inside the data historian holds key aspects of production processes that business would want to protect against intellectual theft through business espionage. An analogy of the process can be described as baking a cake. Let us say there is a special cake that we wish to make but keep the ingredients a secret. Now suppose that by just knowing at what temperature and time the cake is baked in the oven for we can reverse engineer what ingredients are in the cake. Data historians store time, pressure, temperature and other statistics about the industrial process between different machines, therefore one can reverse engineer the process by knowing this information.

The scenario above is exactly what happened to a plant in Morgan County, Alabama owned by Toray Industries. The plant in question produced military-grade carbon fiber that is put on watch-lists for export by the United States to prevent terrorists and foreign entities from reverse engineering and selling copies. The Yokogawa data historian, Exaquantum, used on the plant had known vulnerabilities that were exploited to gain access to the data housed in the facility. The Department of Homeland Security notified the company and the relevant notice was issued in 2014 resulting in Yokogawa Electric applying patches to the vulnerable software.

The Toray plant gives an example of information espionage in the DCS field today. Software vulnerabilities will be abundant yet decreasing with new iterations. However, the data retained in these systems will exponentially grow in the future. Research into data privacy and security relations of DCS environments are still in the early stages of development with standards like NIST Smart Grid Security 3.0 and frameworks like OPCv3.0 Data Access. Creating a framework that can obfuscate, disclose, or otherwise protect the data with industry requirements would represent a crucial step in industry theft.