Security Controls for the Most Effective Cyber Defence in the Industrial Control Space

One of the biggest concerns for critical infrastructure managers towards security is to know whether a particular solution is effective to protect their assets and production. Several efforts have been carried towards this purpose, from which the most relevant are the 20 Critical Controls for Effective Cyber Defense supported by several US Federal Agencies or the Australian Government's Defence Signals Directorate 35 Strategies to Mitigate Targeted Cyber Intrusions.

Most of the controls and priorities out there are not focused in industrial cyber security and therefore they need interpretation and adaptation in order to be an effective solution for the particular characteristics of the industrial control systems that automates the operation critical infrastructure. There is information out there but it is not always easy to make sense of the huge amount of data available.

So, I am the operator of a critical infrastructure, what should I do to protect my assets and guarantee the availability of the system? For a start, it is paramount to understand that security is not a one-off project; it is an on-going activity. Cyber security must be a programme involving technology, processes and people. You probably couldn't conceive a power plant without a fenced perimeter, check points for access control, alarm systems, safety procedures and people responsible and accountable, could you?

Francisco Gomez, CISSP – Senior Security Consultant at Industrial Defender Inc. – fgomez@industrialdefender.com