I would like to participate and try help improving security in Critical Infraestructure Security by next thoughts.

If i should take care of security on any process, building, information, or something, I should notice about:

1.- It´s a continuous process, it never ends grant security to something because threats, faiulures, as a human system designs are not perfect, so is a processs which must evaluate periodically.

2.- Threats analisys and development in test studies. You have developed a software, how exhaustive tests have you tried on it searching for failures? Sometimes bugs are intentionally created. How can you control that? What audits have you taken over what you wan to protect? Where come threats come from? Natural disasters, internet, human failures

3.- Framework: Are you pretty sure is totally secure where you want to perform/use something or where you want to provide service? You could take Japan nuclear infraestructures with tsunami and earthquakes or talking about ciberthreats, have you consider the posibillity of each function in php or c languages could be vulnerables? (this is frameworks where you develop or provide services). You could consider to hide critical infraestructures which grant some physical and access protection.

4.- Teams and work performed to bring security. How can you trust on them that they are not developing desired bugs on software? Audits on teams, software, buildings, accesss controls, and remember on human failures including performing audits which could end with risks you have no considered.

So with this preliminar thoughts, one posibly approach could be:

a.- Isolation:
As I guess is not possible to stop all software threats, I was thinking in a first approach isolating those infraestructures from internet even getting managemenet servers from that infraestructures with no ethernet cards, no usb or removable media on that servers , physycal access restrictions to a limit and very trust employees. Why should consider this way? I think that avoiding internet tcp/ip packets or removable media (usb, cd, dvd) you avoid ciberthreats and start to consider physical attacks because there is no other way to overcome security policies from a remote machine, the only threats could consider risks is related to internal and physycal attacks inside the infrastructure.

b.- Split networks. As first approach it´s not possibly to perform, do not put all critical services, information or whatever you want to protect over the same place. It´s layered security.So if a malware is aimed against power electrical management software avoid to connect all management software between them so in that way you could mitigate propagation

c.-Tests teams. Must have teams which should perform tests trying to hack those systems, but the problem is that they should known software maybe with reverse engenering. I guess systems as mainframes is harder to hack because not every one knowns that systems.

d.- Infilttration on underground markets to know what kind of threats are being developed even hire some of them to perform previous tests.

e.- Exhaustive audits on critical software, make code not possible to use reverse engineering and not open code to avoid everyone could find bugs (may be you should announce pieces of code searching for possible code improves)

I hope help in some way to improve security.

Jose Pablo Valcárcel Lázaro