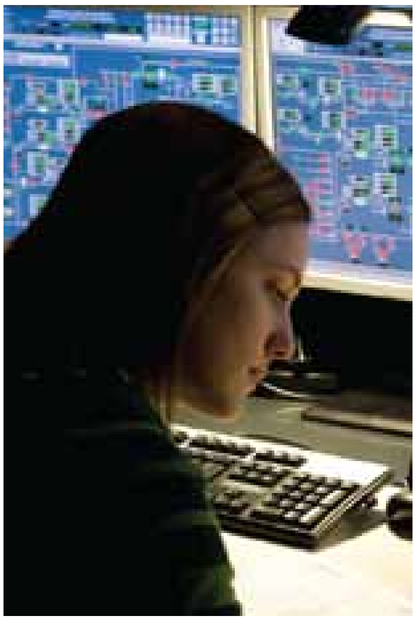
indra

CYBERSECURITY FOR INDUSTRIAL PROCESSES



Facing Digital Threats

In the 90s computer attacks were mere anecdotes of people seeking notoriety creating annoying virus without any benefit. In the past decade, the cybercrime made his way through complex programs in order to steal large sums of money.

In the last years we have experienced attacks on different critical infrastructures as nuclear power plant control systems, or government organizations. We have gone from computing vandalism two decades ago to Cybercrime and everything suggests that in the coming years we must prepare our infrastructure against cyberterrorism and cyberwar.

Digital control systems are a critical component of the energy plants. Nowadays, users need to increase the availability of process data and thereby to define connections to theprocessing network. The technology used is changing and the design of the plant evolves from isolated proprietary systems, to systems based on open technologies of common use and well documented in Internet as well as to an increased system integration.

This situation has emerged new risks. The number of incidents has grown, which have been committed not by mere individuals seeking notoriety and personal satisfaction but by organized groups that have big budgets and even interests in governments of some countries.

Cybersecurity is not an just a technical issue. It requires engaging the organization and the definition of new activities and responsibilities.

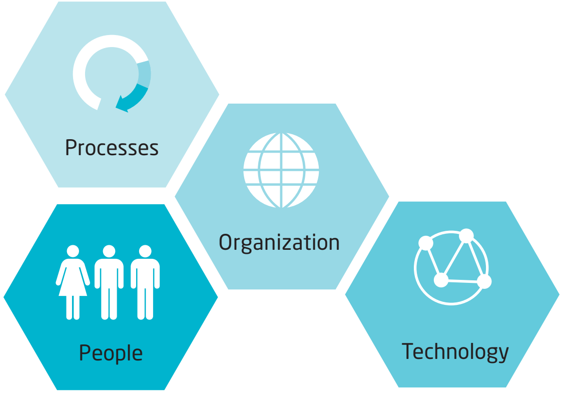
To achieve an acceptable level of cybersecurity in an organization, it is required to have knowledge and experience on Industrial Control Systems and Security for traditional Information Systems.

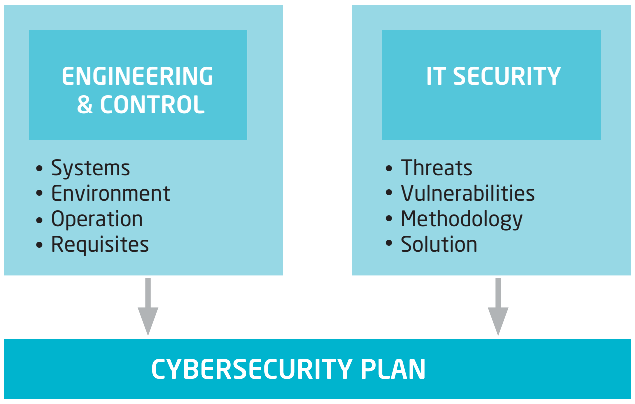
IT security processes cannot be exported directly to control systems processes. Neither safety requirements are the same nor is security technology applicable.

Indra, has an extensive capabilities and experience in both worlds (Systems Industrial Control and Security Information Systems) will help you to set a cybersecurity plan taking into account the organizational structure definition, identifying threats and risks and proposing a work program to ensure the Control System from a cybersecurity point of view.

13 measures to reduce risk

1. Adopt a reference framework.
2. Define the organization cybersecurity roles, activities and responsibilities.
3. Inventory and classify the systems from a cybersecurity point of view.
4. Analysis and risk management.
5. Define a management procedure for cybersecurity incidents.
6. Include cybersecurity requirements in any project from the beginning.
7. Raise awareness and create culture.
8. Defense in Depth.
9. Implement perimeter defense systems.
10. Schedule cybersecurity audits.
11. Monitor and correlate systems events.
12. Properly manage system configurations.
13. Collaborate actively in forums and specialized working groups.





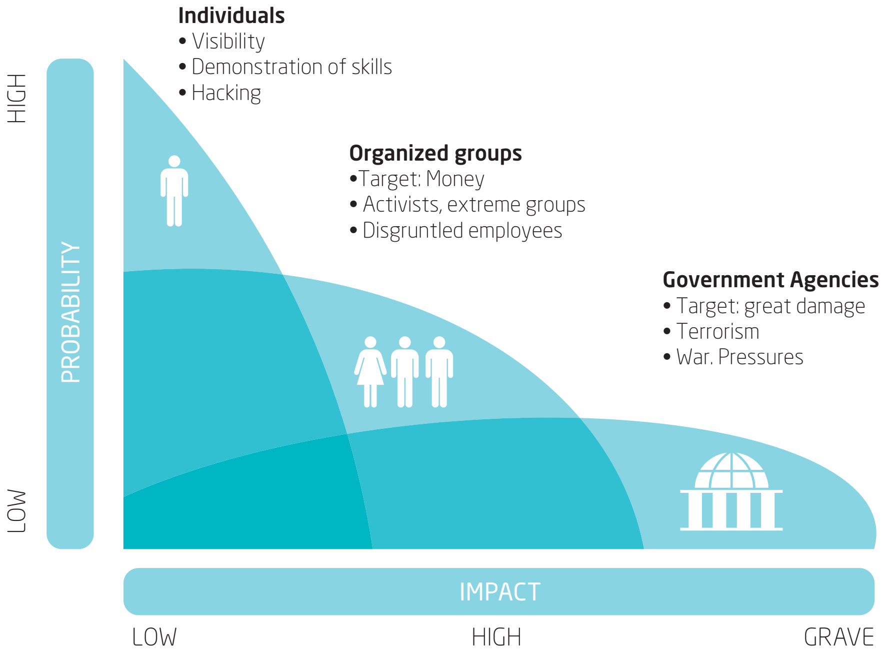
ENGINEERING & CONTROL

- Systems
- Environment
- Operation
- Requisites

IT SECURITY

- Threats
- Vulnerabilities
- Methodology
- Solution

CYBERSECURITY PLAN



Individuals

- Visibility
- Demonstration of skills
- Hacking

Organized groups

- Target: Money
- Activists, extreme groups
- Disgruntled employees

Government Agencies

- Target: great damage
- Terrorism
- War. Pressures

indra

Avenida de Bruselas, 35
28108 Alcobendas,
Madrid, (Spain)
T+34 91 480 50 00
F +34 91 480 60 31
security@indracompany.com
indracompany.com

Indra reserves the
right to modify
these specifications
without prior notice.