




# Security for Safety



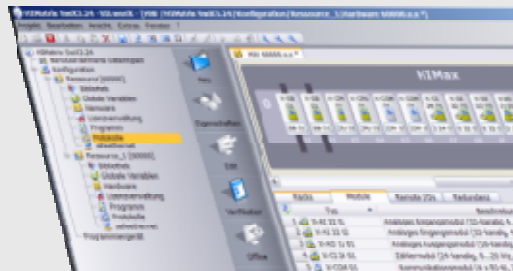
SAFETY  
NONSTOP

- 
- A photograph of three people in business attire. In the foreground on the left is a man with a goatee and glasses, wearing a white shirt and a brown tie. Behind him and to the right are a woman with blonde hair and a man with short brown hair, both looking towards the camera. The background is a light blue gradient.
- 1. Relation between Safety and Security**
  - 2. Organizational Measures**
    - Awareness
  - 3. Technical Measures**
    - Defense in the Depth
      - 1. PC-Protection**
      - 2. PES-Protection**
      - 3. Segregation**

# HIMA. Safety. Nonstop.



Founded in 1908, HIMA develops functional safe solutions for automation for more than 40 years.



Development, production and installation of safety related controllers for Process- and Factoryautomation.



The specialization in safety technology requires open and standardized integration options in 3rd party systems.

Cyber Security is thus also an issue.



SAFETY  
NONSTOP



# Safety = Functional Safety + Cyber Security.

## Functional Safety



Protect Humans health



Machines



and Environment

The installation must not cause any harm.

## Cyber Security



Confidentiality

*Encryption*



Integrity

*Signature*



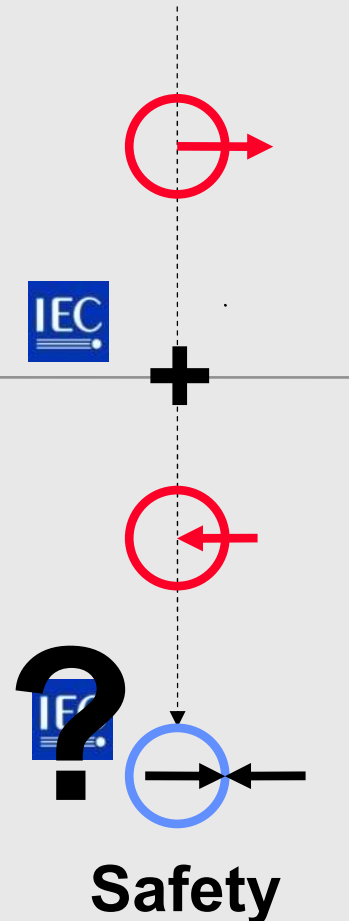
Availability

*Segregation*

The installation has to be protected against harm.

**Safety:** Risk = (probability of an accident) x (extent of damage)

**Security:** Risk = (Vulnerabilities x Threat) x (extent of damage)



# Why Security gains importance in Automation.



HIMA offers now its 4th generation of SIL4 hard wired safety systems called PLANAR 4.

**no Network, no Programming**



In 1997 the HIQuad System was launched. SIL3, high availability and safe**ethernet**.

**segregated Networks, SIL3 Programming**



In 2001 the HIMatrix entered the market. SIL3, small, fast, full distribution via safe**ethernet**.

**Integrated shared Networks, SIL3 Programming**



2008 the HIMax was introduced. SIL3, NONSTOP, extremely fast, full distribution via safe**ethernet**.

**Integrated shared Networks, SIL3 Programming**

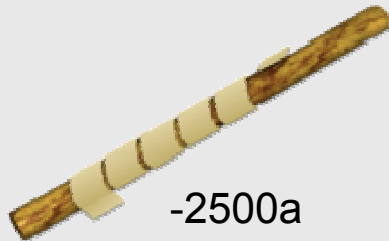
Openness, Flexibility

Robustness



SAFETY  
NONSTOP

# Safety always has been a basic need.



-2500a



-500a



-70a



Time

Source all images [www.wikipedia.de](http://www.wikipedia.de)

2500 years ago the Scytale was used by the Spartans to transferred **secret messages** through a **battlefield**.

Basic Concept of encryption:

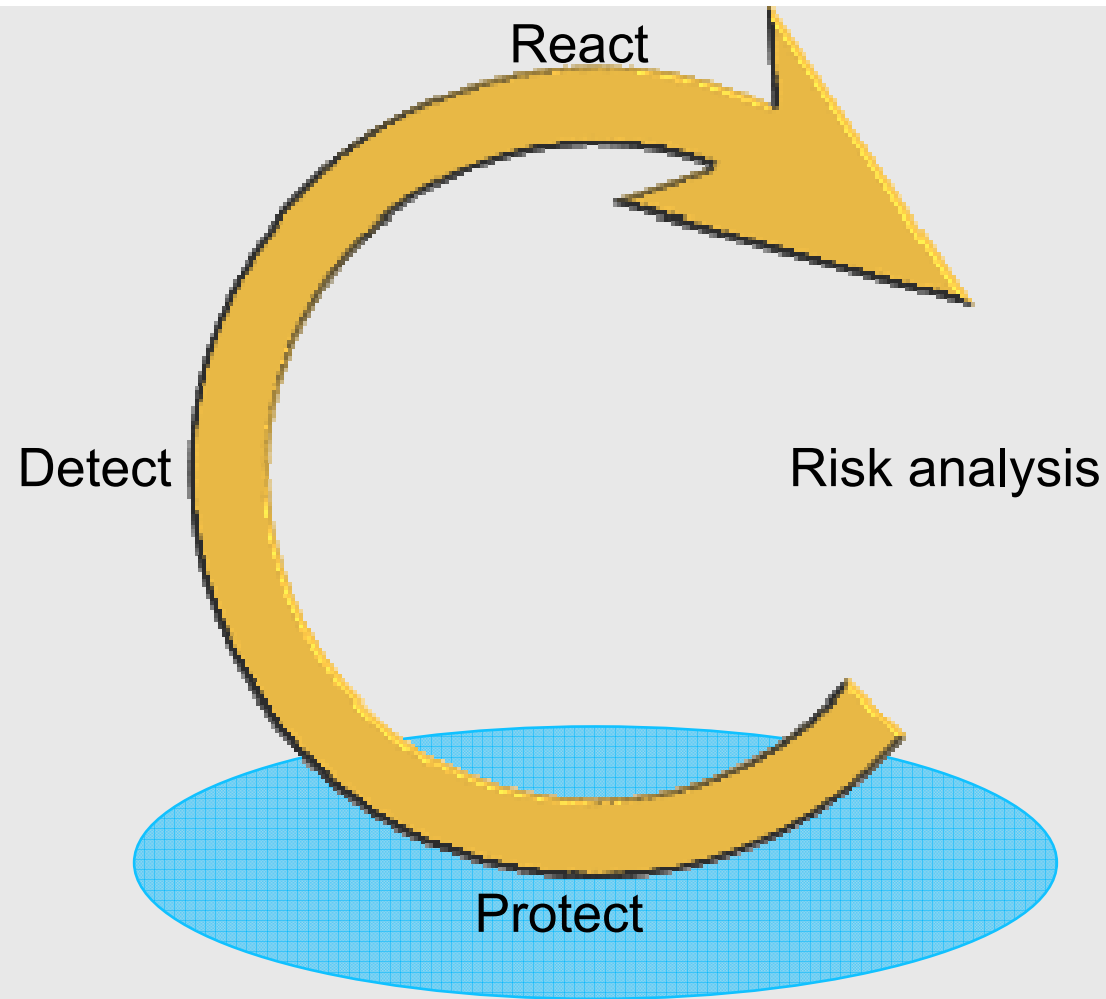
0 1 0 0 1 0 1 1	Basic Text
1 1 1 0 1 1 1 0	Key
XOR	Known Operation
1 0 1 0 0 1 0 1	Encrypted Text

The Methods to guarantee security were improved for generation....

... Just as the methods to circumvent this protection.

→ An ultimate Solution will never exist!

# Security is a process. (Plan, Do, Check, Act)



# Elements of Security.



## ■ Humans

- Awareness
- Education...



## ■ Technology

- Infrastructure (e.g. Firewalls)
- Software protection (e.g. Virus Scanners)
- Devices...



## ■ Operation

- Work instructions
- Updates...



# Future? Standards.



Many organizations are seeking a standard or already have regulations.



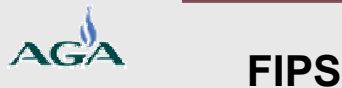
Others strive for a independent test certificates.



→ Both concepts have to constantly respond to the changed situation. (moving Target)



Neither user nor manufacturer will be able to follow several paths.



→ A common solution is essential.

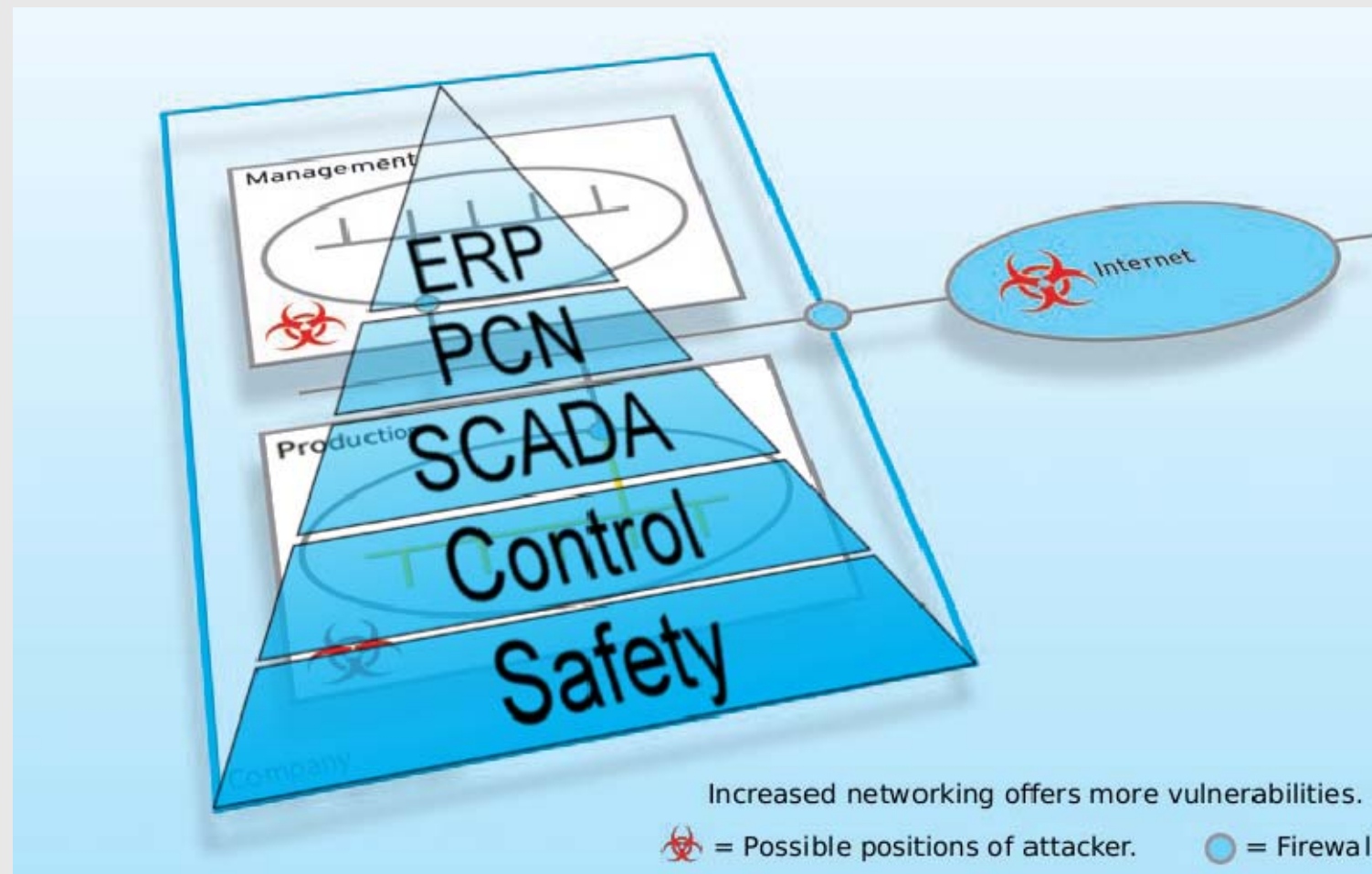


## That's the situation...



source: <http://xkcd.com/927/>

The whole organization has to be involved.



# What now?



Consider what's already been proven in use:

Organizational Measures

→ Awareness

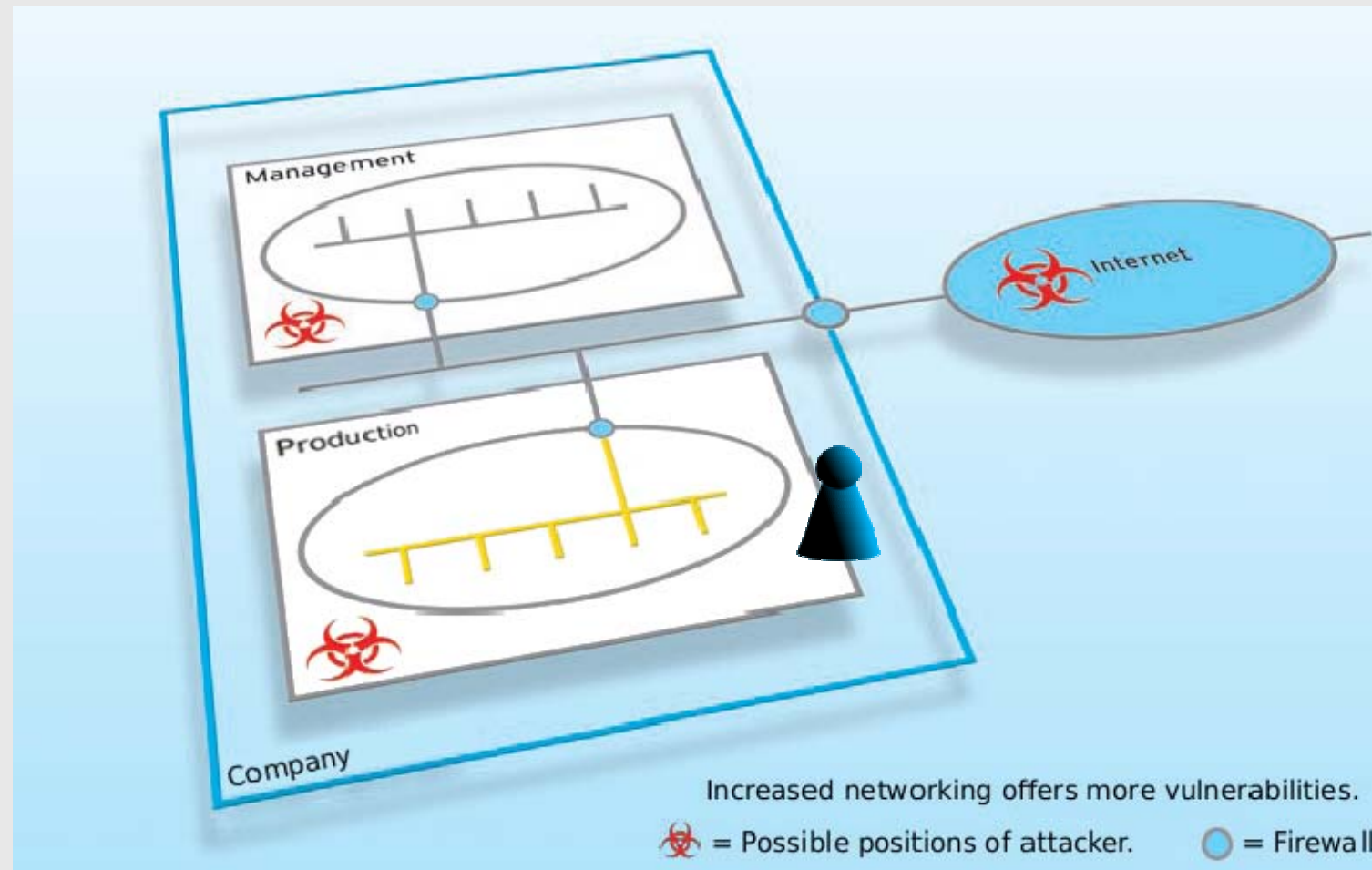
Technical Measures

→ Defense in the Depth

1. PC-Protection
2. PES-Protection
3. Segregation

# Environment.

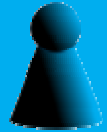
## Organizational Measures (Awareness)





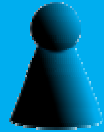
# Creating Awareness !

Organizational Measures (Awareness)

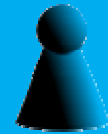


# Creating Awareness !

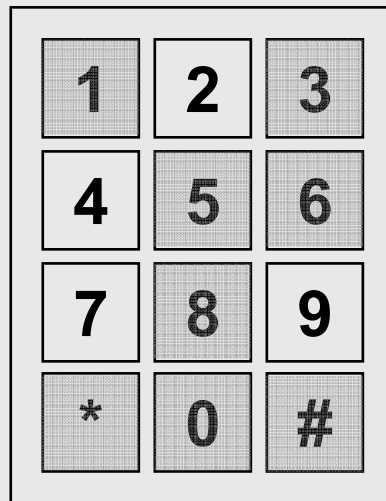
## Organizational Measures (Awareness)



# Humans cause failures.



## Organizational Measures (Awareness)

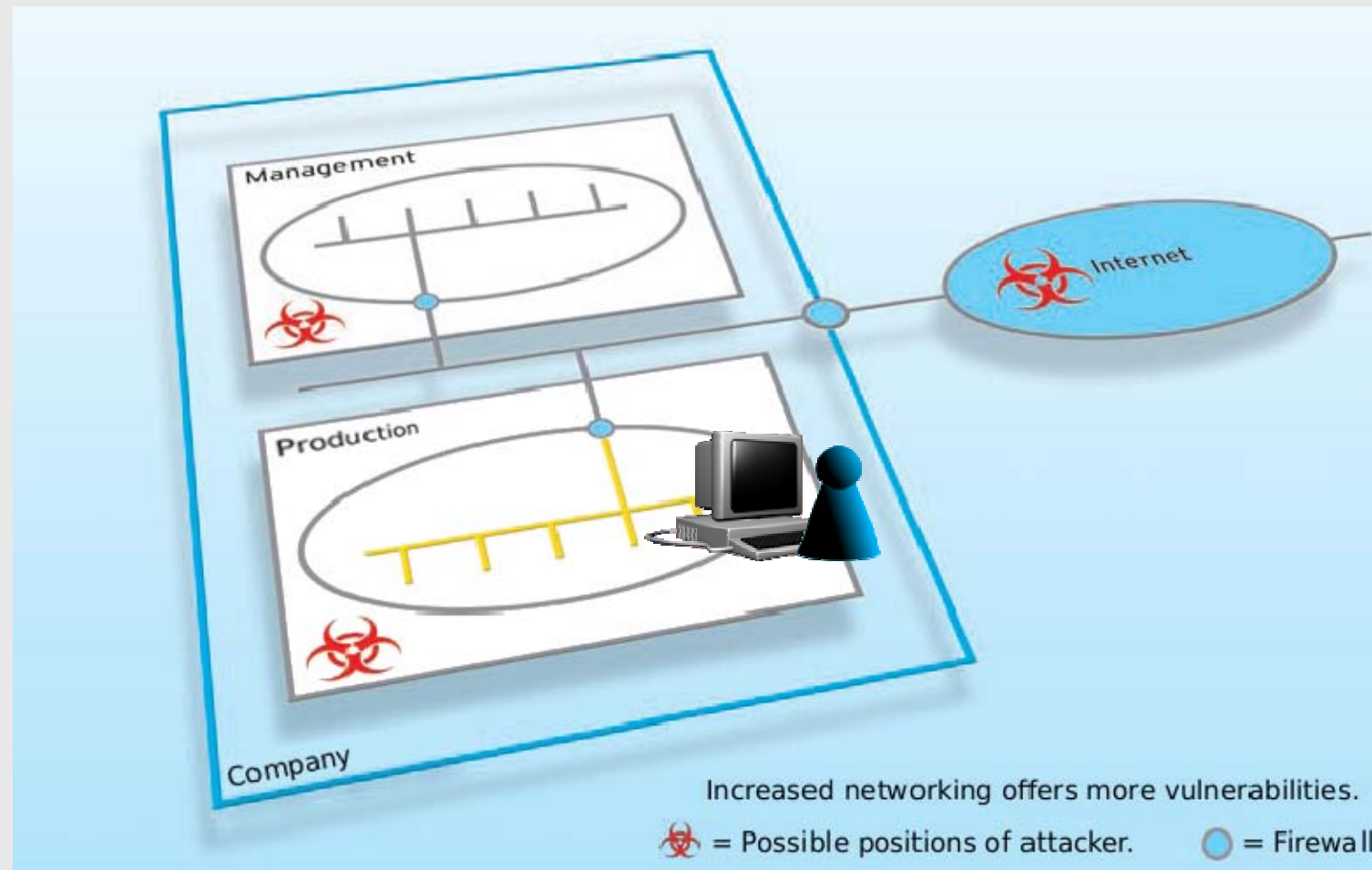


- |   |                              |
|---|------------------------------|
| 1. A combination lock on a door offers endless possibilities.                       | $n = \infty$<br>$t = \infty$ |
| 2. As the code should be usable it is limited in length.                            | $n = < \infty$<br>$t = ?$    |
| 3. Often an acoustic signal is generated to confirm that a button has been pressed. | $n = 4$<br>$t = 20736$       |
| 4. The unused buttons get grey (dirty) in the course of time.                       | $n = 4$<br>$t = 24$          |

→ Organizational Measures to defense the System are mandatory!

# Environment.

## Technical Measures (Defense in the Depth)



# Windows Access.



Technical Measures (Defense in the Depth)



Passwort  $\Sigma \rightarrow \#$

$\# \ ? \rightarrow$  Passwort



**Rainbow Tables**

Passwort 1  $\rightarrow \#1$

Passwort 2  $\rightarrow \#2$

Passwort 3  $\rightarrow \#3$

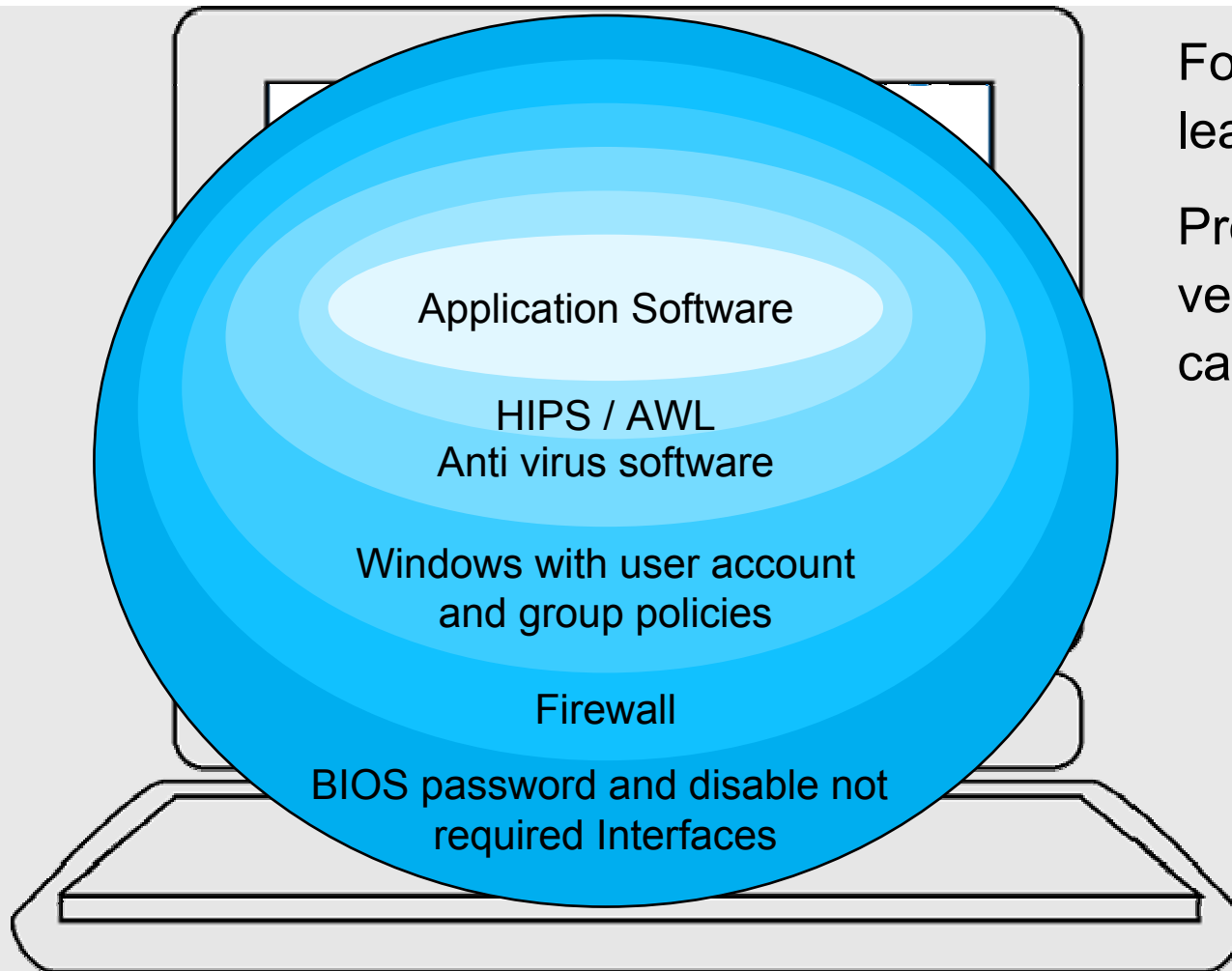
.....



# PC-Schutz.



## Technical Measures (Defense in the Depth)

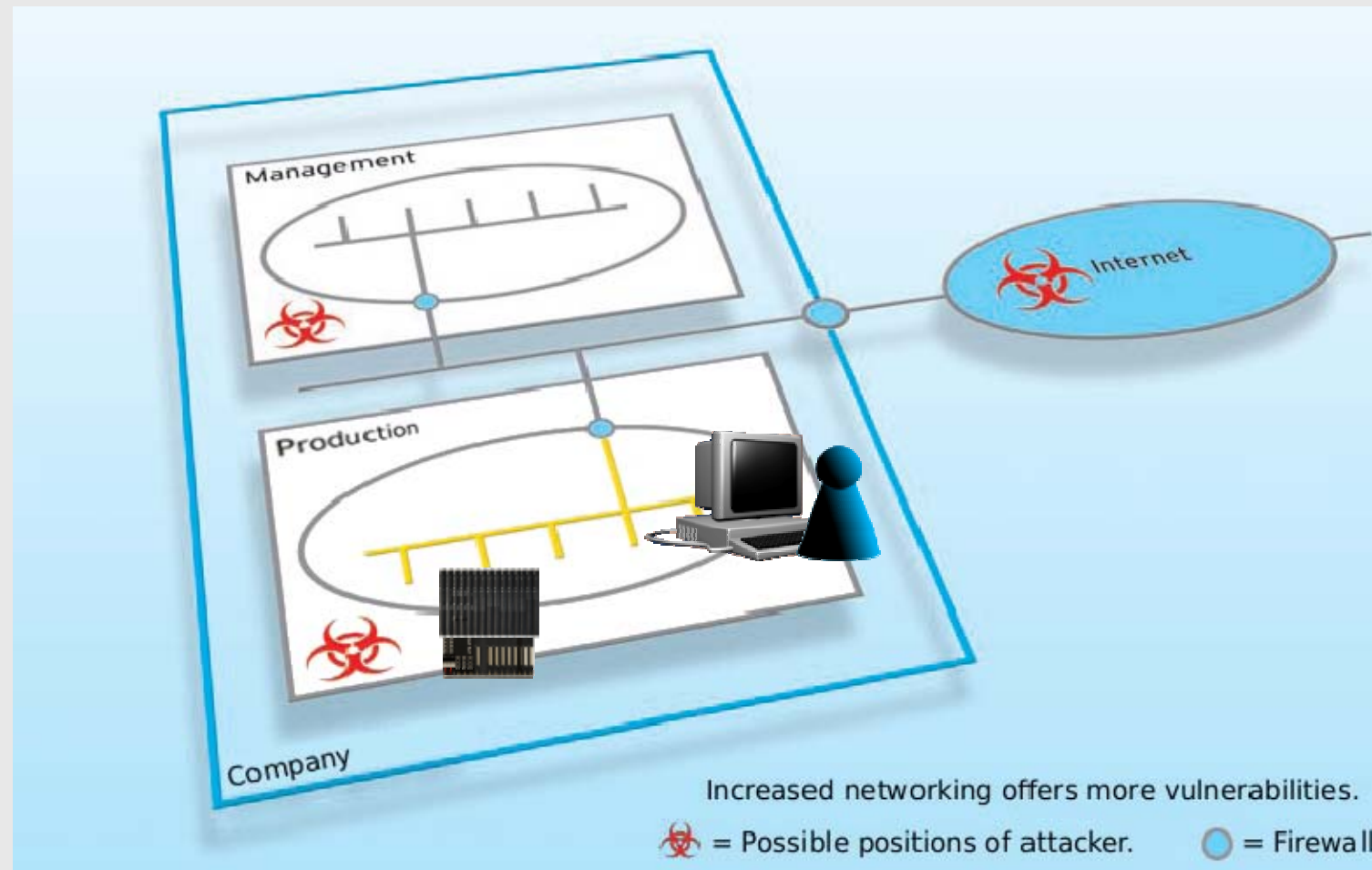


Follow the principle of least privilege!

Products of different vendors avoid common cause failures.

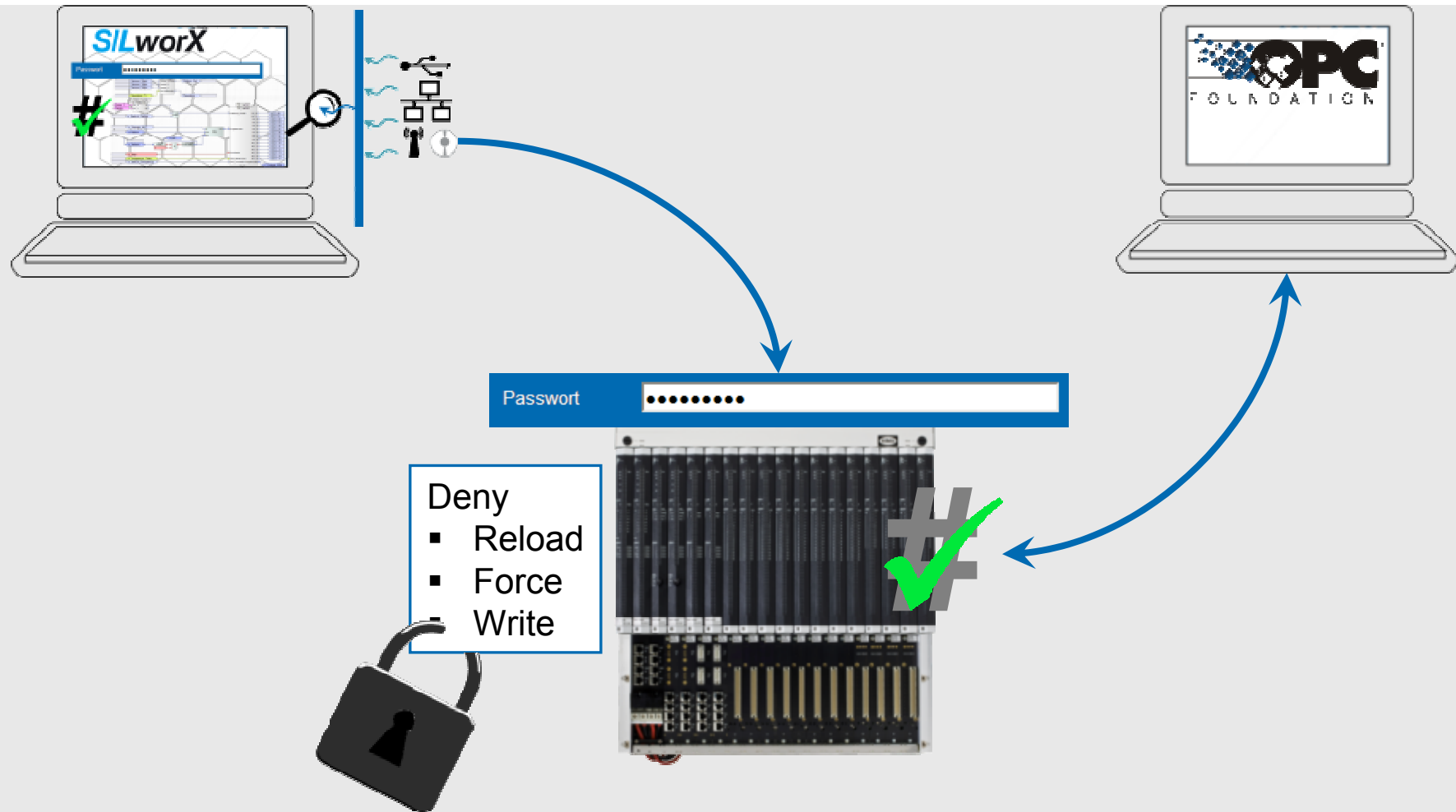
# Environment.

## Technical Measures (Defense in the Depth)



# Protection of Control.

Technical Measures (Defense in the Depth)



# Update documentation .

Technical Measures (Defense in the Depth)



## HIMax

- Port Settings
- Protocols
- Network access

## PC

- Network access
- Windows minimal configuration
- Project protection

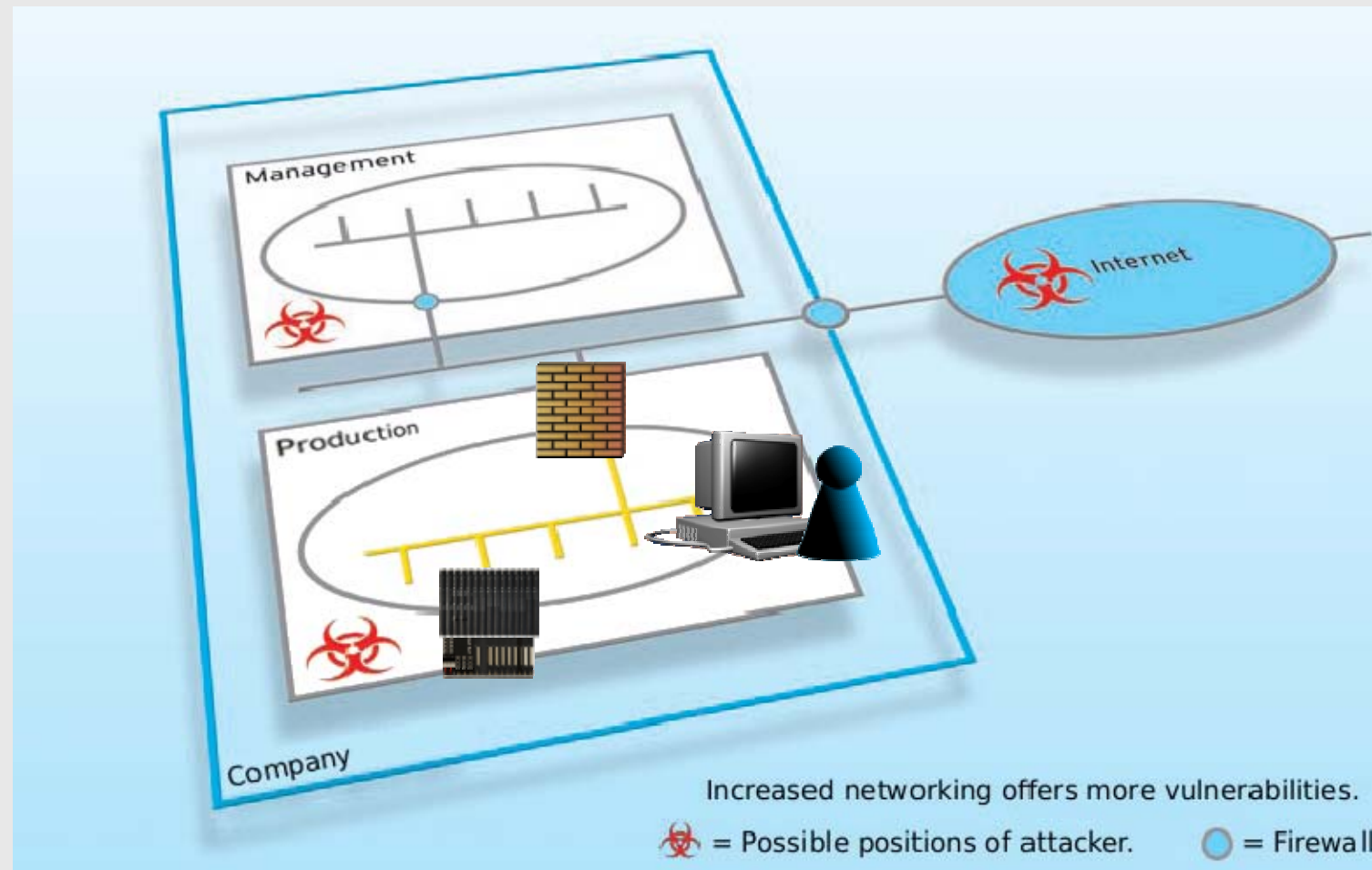


## Checklist

→ **Avoid systematic Failures !**

# Environment.

## Technical Measures (Defense in the Depth)



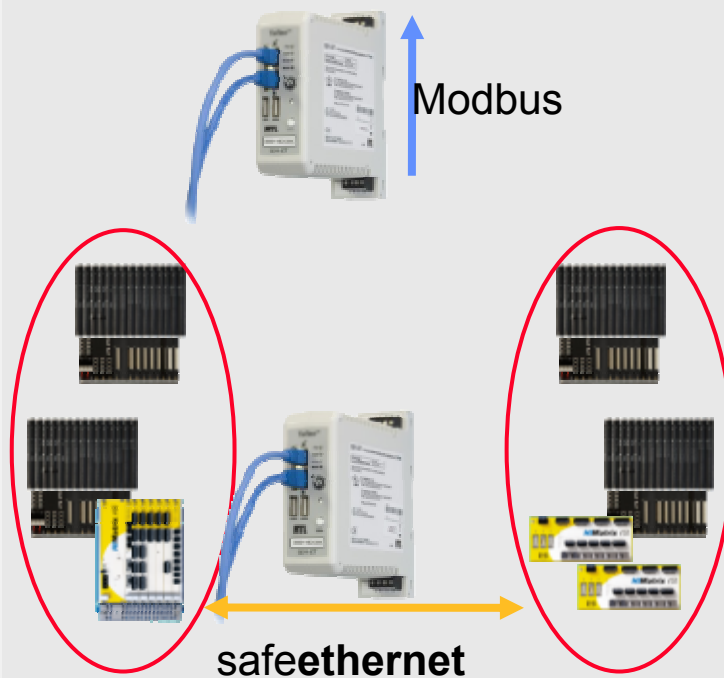


## e.g. special Industrial Firewalls.

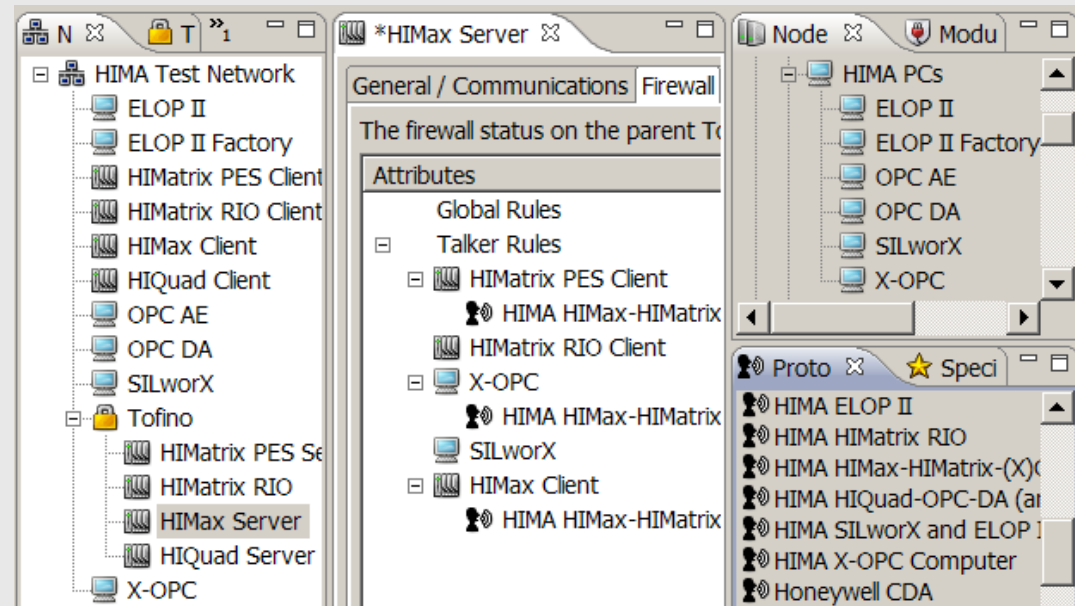


### Technical Measures (Defense in the Depth)

#### DCS-System



Tofino Modbus TCP-Enforcer enables read access and denies write access (to HIMax).



→ Additional measures: IDS, IPS, Honeypots...

# The efficient way to Security for Safety.



- Organizational Measures

- Educate Employees
- Access Protection
- Emergency plans
- ....

- Technical Measures

- Password protection on each Level
- Segregation of Networks
- Multilayer protection concept for PC and Control
- ....

**Although there are no established industry standard,  
you can already implement a lot of security for safety.**

# Thank's for your attention !



Stefan Ditting  
Product Management  
Phone +49 6202 709-426  
Fax +49 6202 709-6426  
E-Mail: [s.ditting@hima.com](mailto:s.ditting@hima.com)

[http://www.hima.com/Solutions/Integration\\_solutions/Security\\_default.php](http://www.hima.com/Solutions/Integration_solutions/Security_default.php)  
[security@hima.com](mailto:security@hima.com)



SAFETY  
NONSTOP