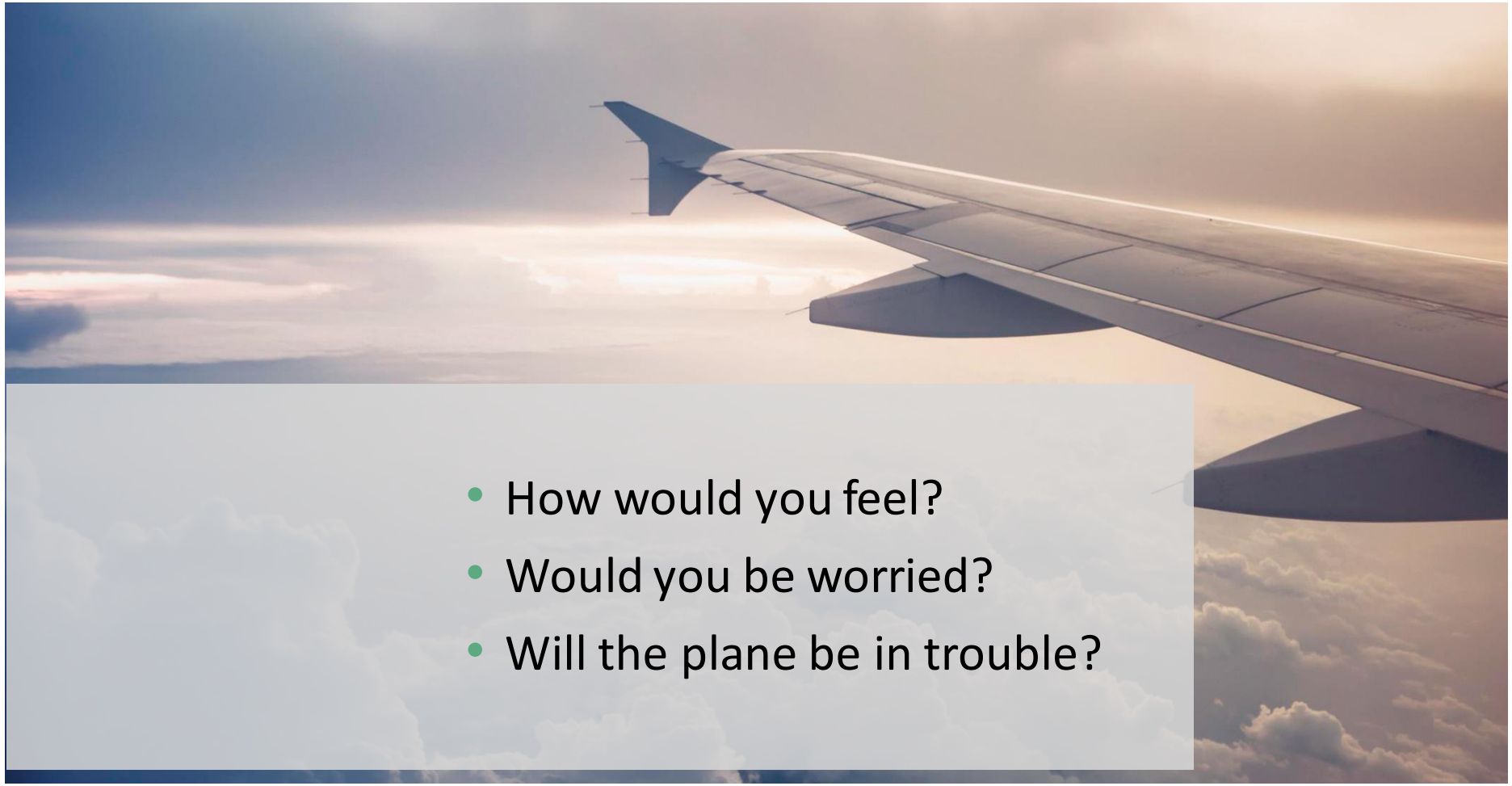
It takes two to Tango: Safety and Security

Peter Sieber
Vice President Norms & Standards, HIMA

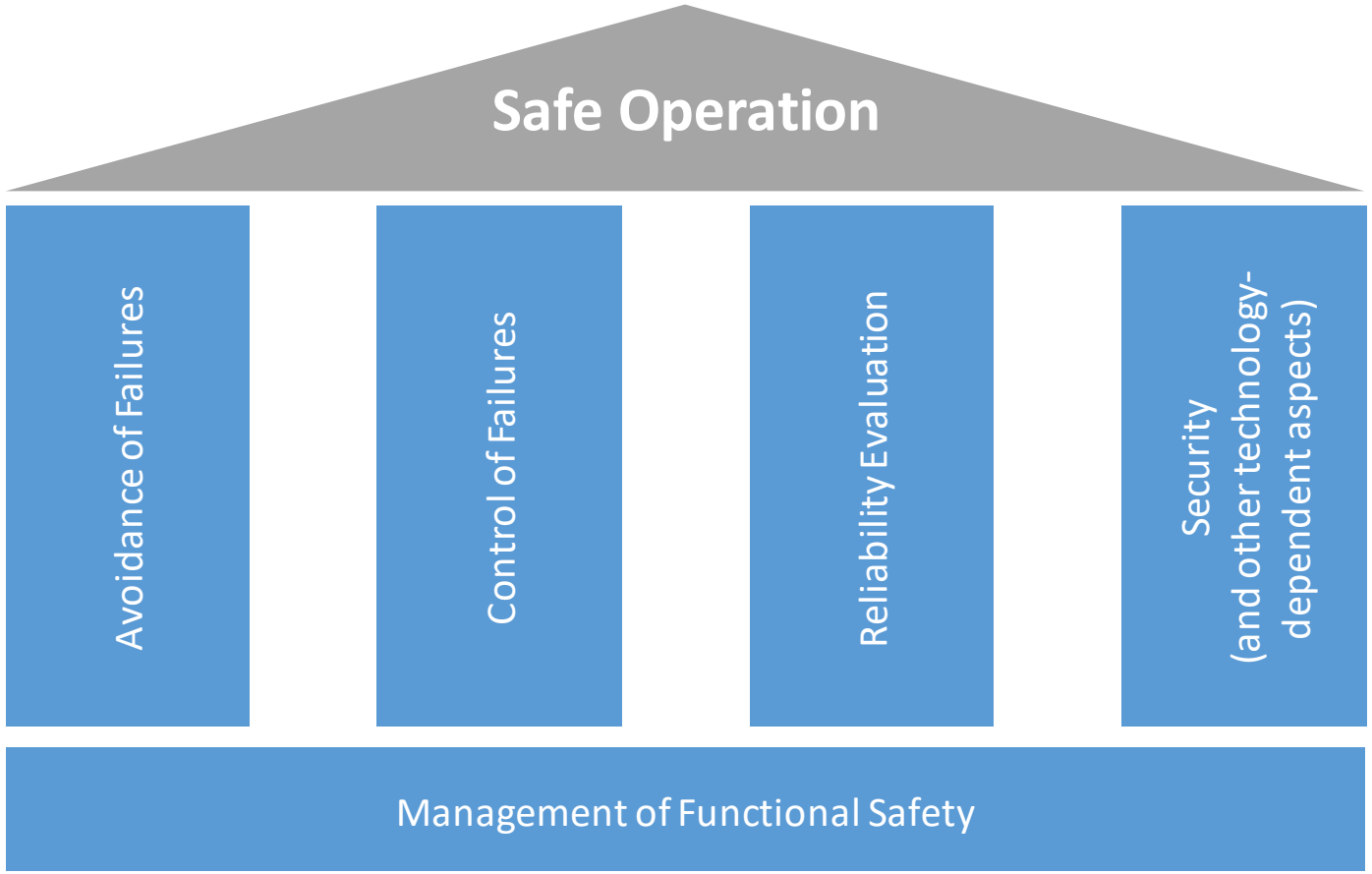
Safety Case
Symposium 2018
Singapore

Experienced recently while being airborne …



- How would you feel?
- Would you be worried?
- Will the plane be in trouble?

How to be prepared to tango



To tango requires common understanding

Safety and security interacting closely, nevertheless

- Both are focused on totally different aspects
- Safety and security recommendations have no automatic correlation
- Alignment of safety and security requires a special strategy

Alignment of both dancing partners

Guiding principles of applying Safety & Security IEC 61508 & IEC 62443

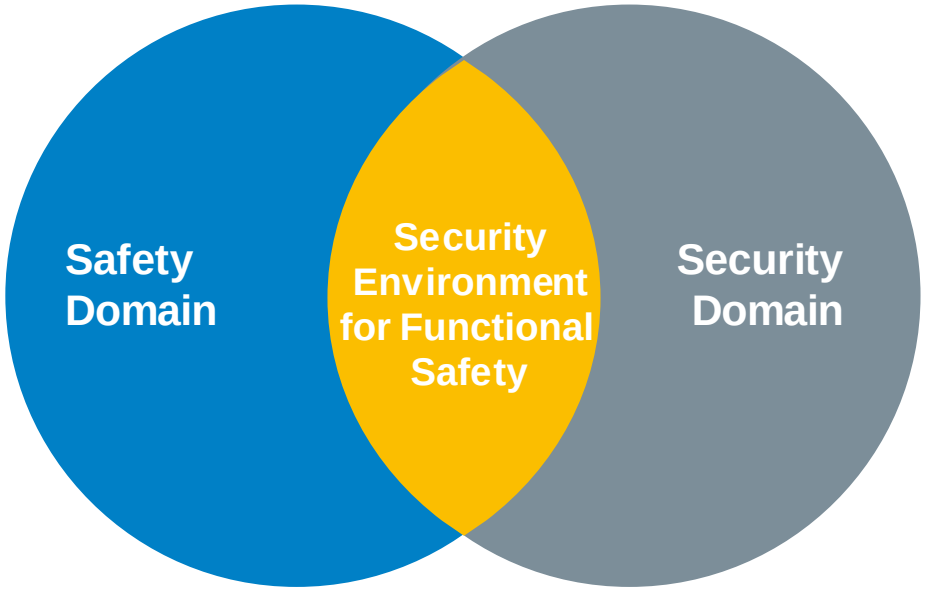
Principle 1: Protection of safety functions
Security effectively prevents safety against negative influences of threats.
Safety evaluations are based on the assumption of effective security measures.

Principle 2: Compatibility of implementations
Security does not interfere with safety and vice versa.

Principle 3: Protection of security countermeasures
The safety implementations do not negatively compromise the effectiveness of security implementations.

Source: IEC/TR 63069

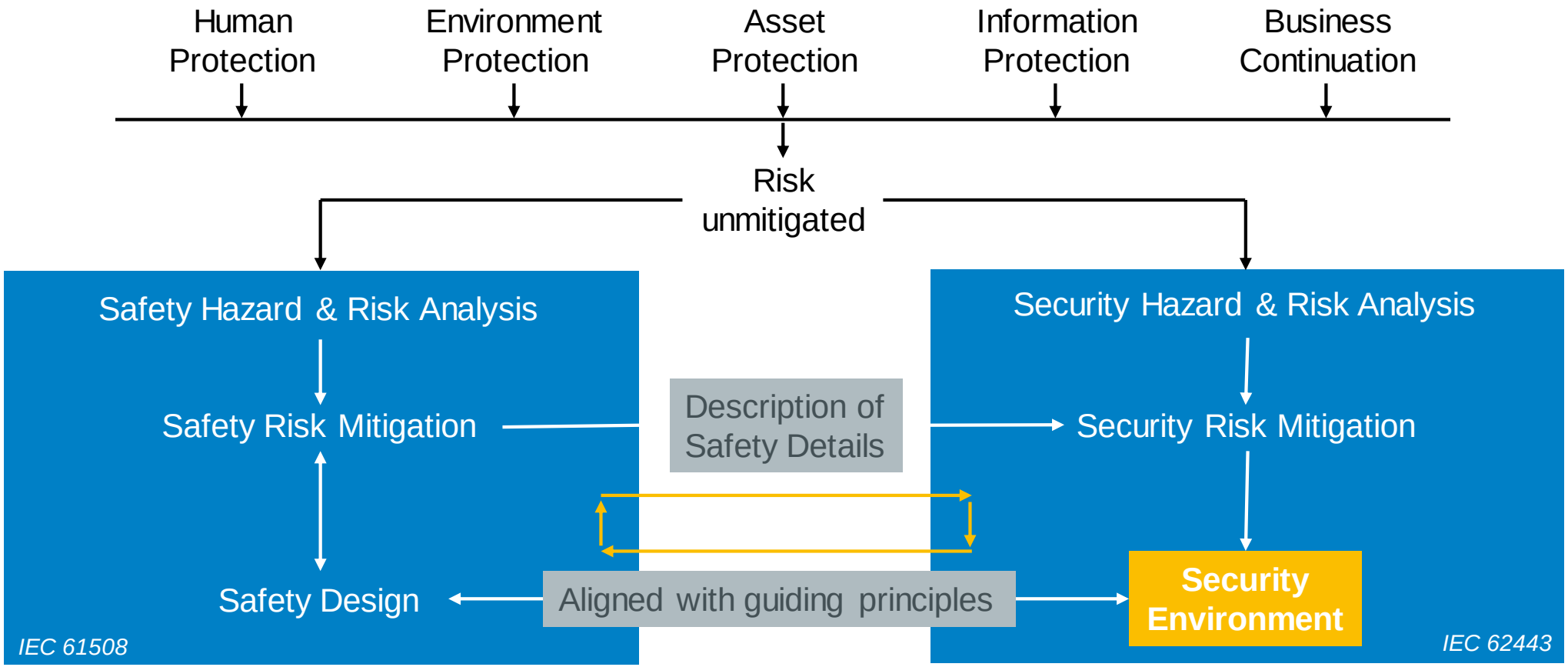
The melody: Security environment for Safety



All measures ensure secure operation of a safety system, including:

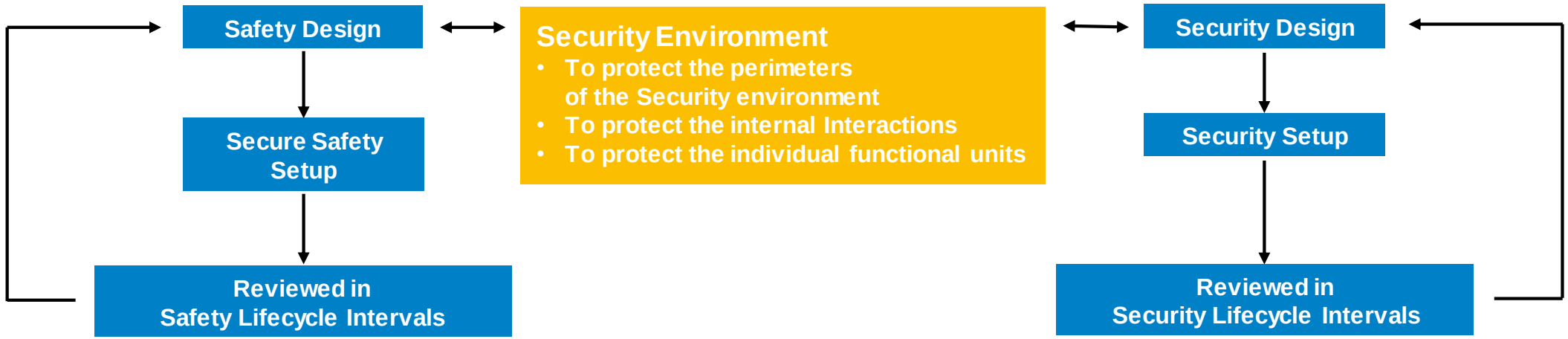
- Protection of the perimeters of the safety domain
- Protection of the interactions inside the safety domain
- Protection inside the individual functional units

To compose: Safety & Security Risk Management



Our tango lasts longer

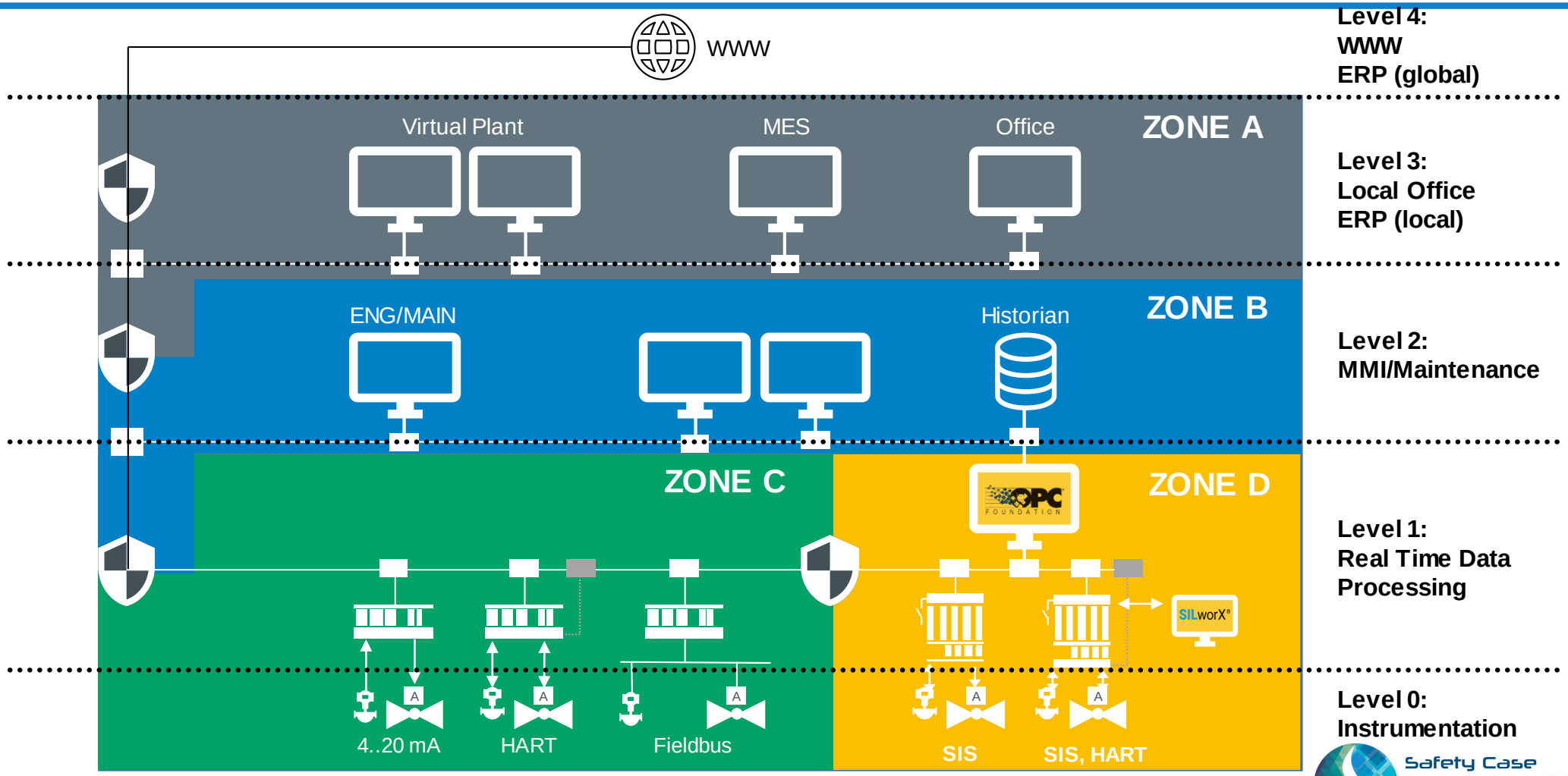
Coordination of Safety and Security Lifecycle



1. Updates in years
2. Focus on malfunctions
3. Looking at (own) operational experiences

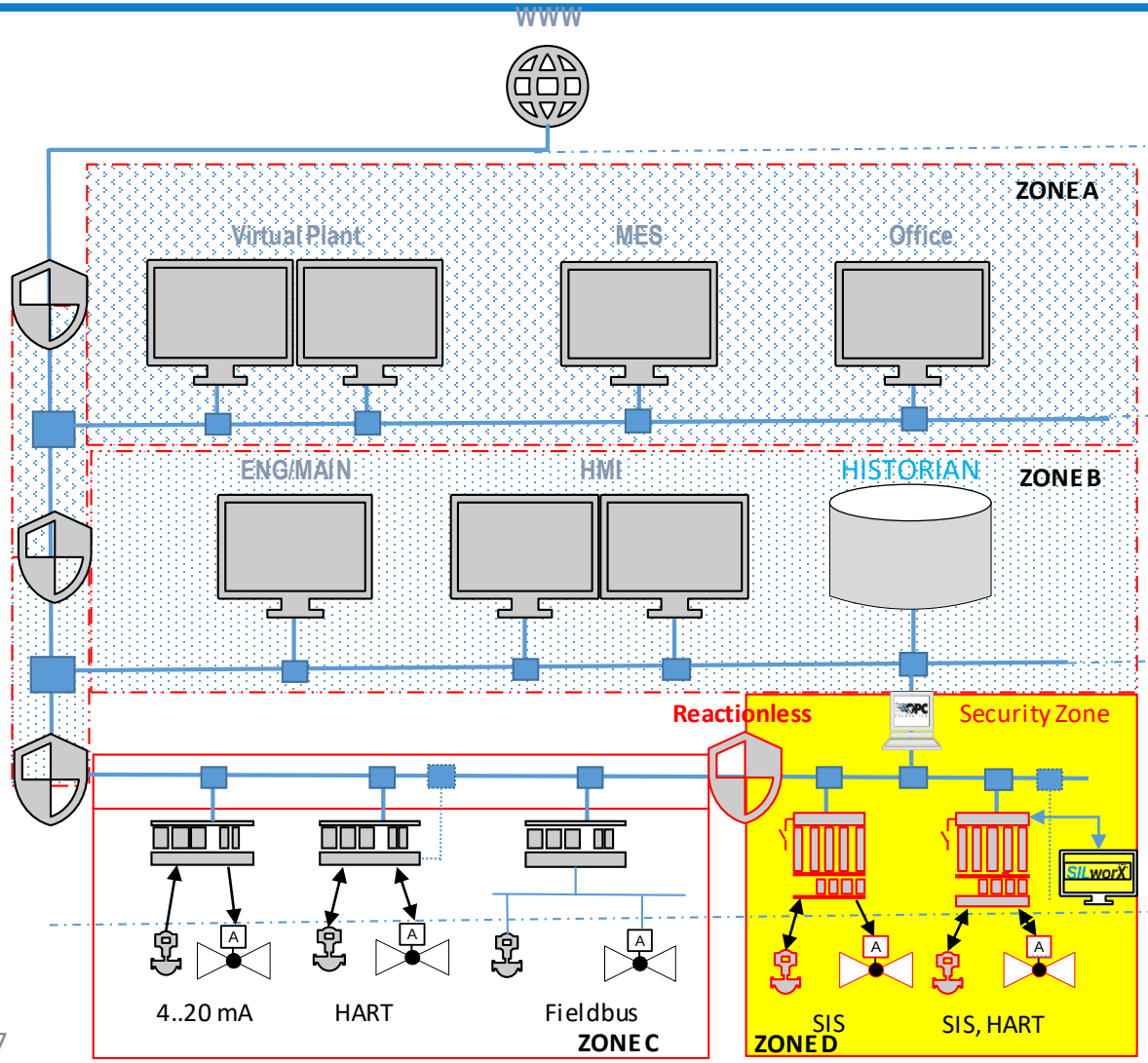
I. Updates in weeks
II. Focus on vulnerabilities
III. Looking at community experiences

Zones & Conduits (IEC 62443)

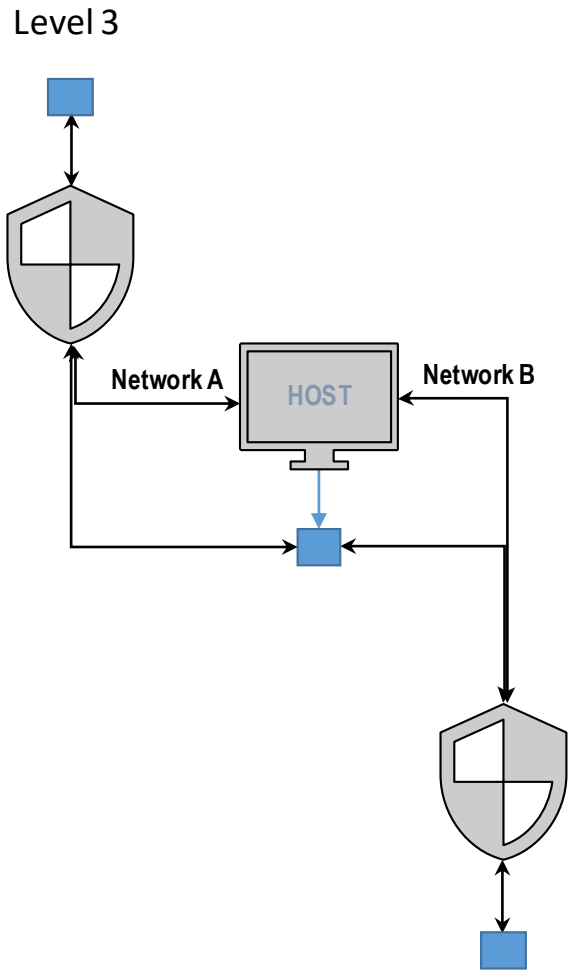


Use cases and best practices

Zones & Conduits (IEC 62443)



Network Segregation



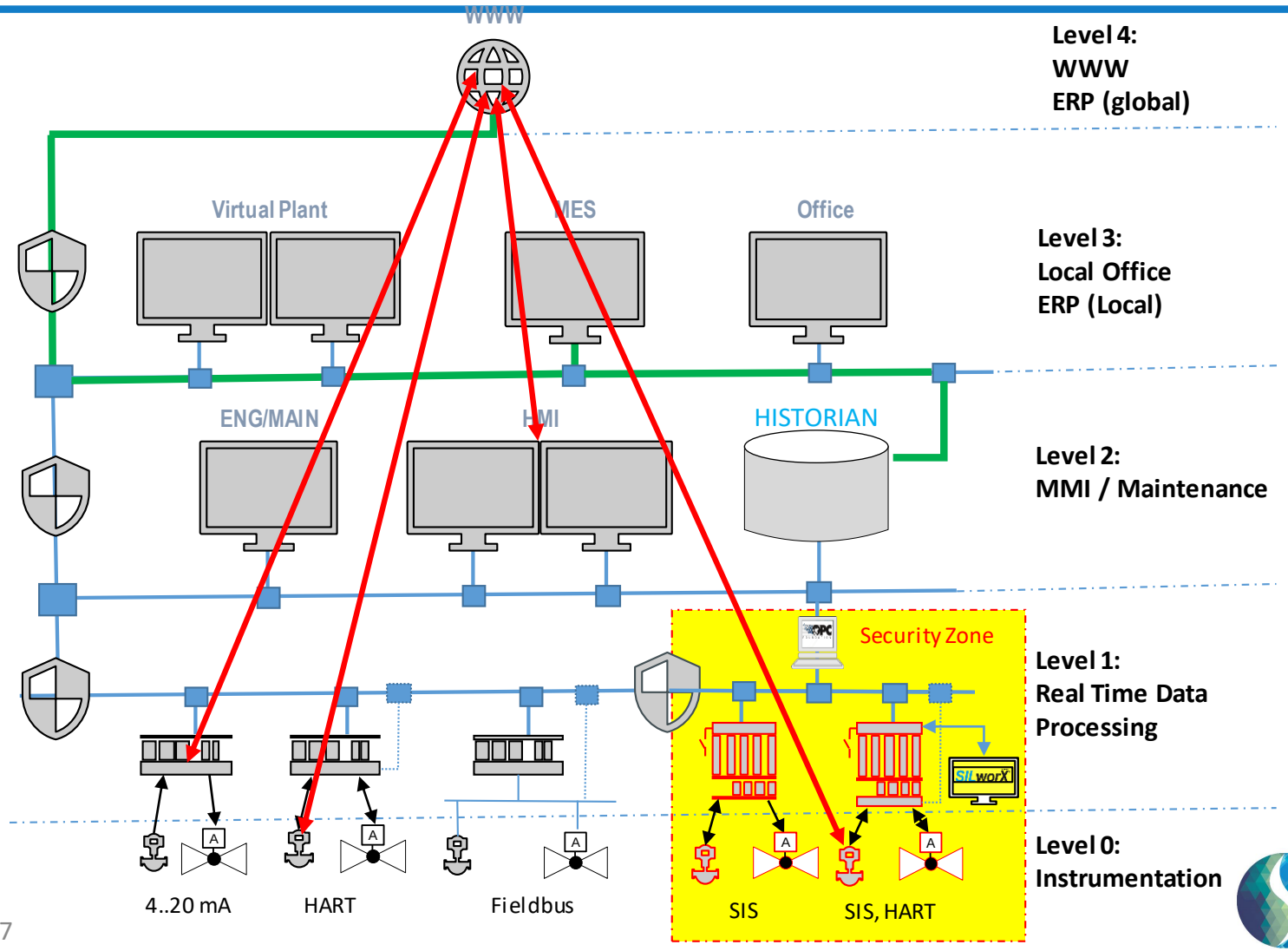
Firewalls

- Closes certain communication Channels (Ports)
- May or may not monitor flow of Data
- May restrict the addresses permissible
- May do a deep package inspection of data going through

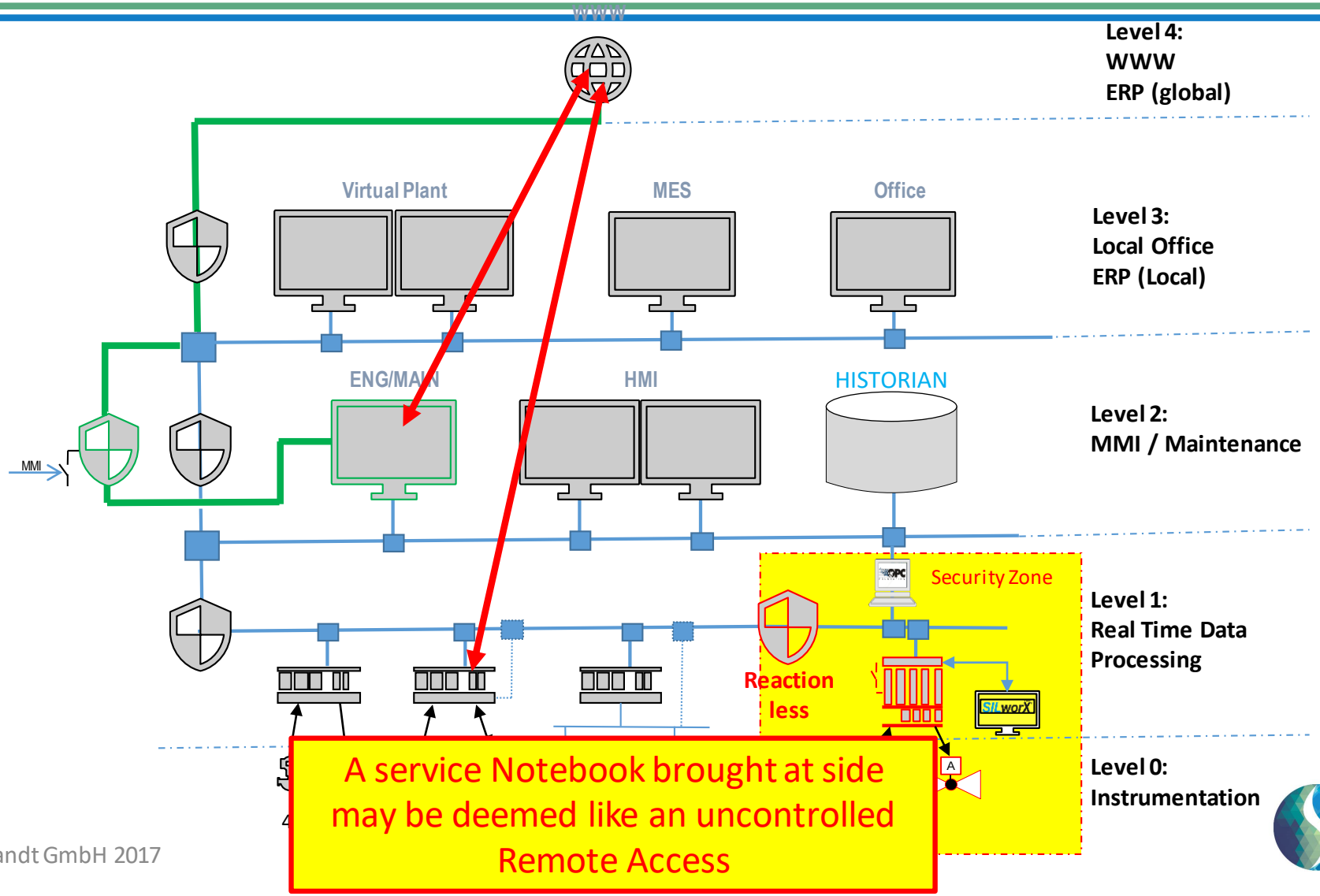
Demilitarized Zone

- Having 2 **independent** Firewalls (physically!)
- Having 2 **independent** Network (physically!) Connections
- Having a **HOST** preferable changing Data formats, Communication processes and Ports

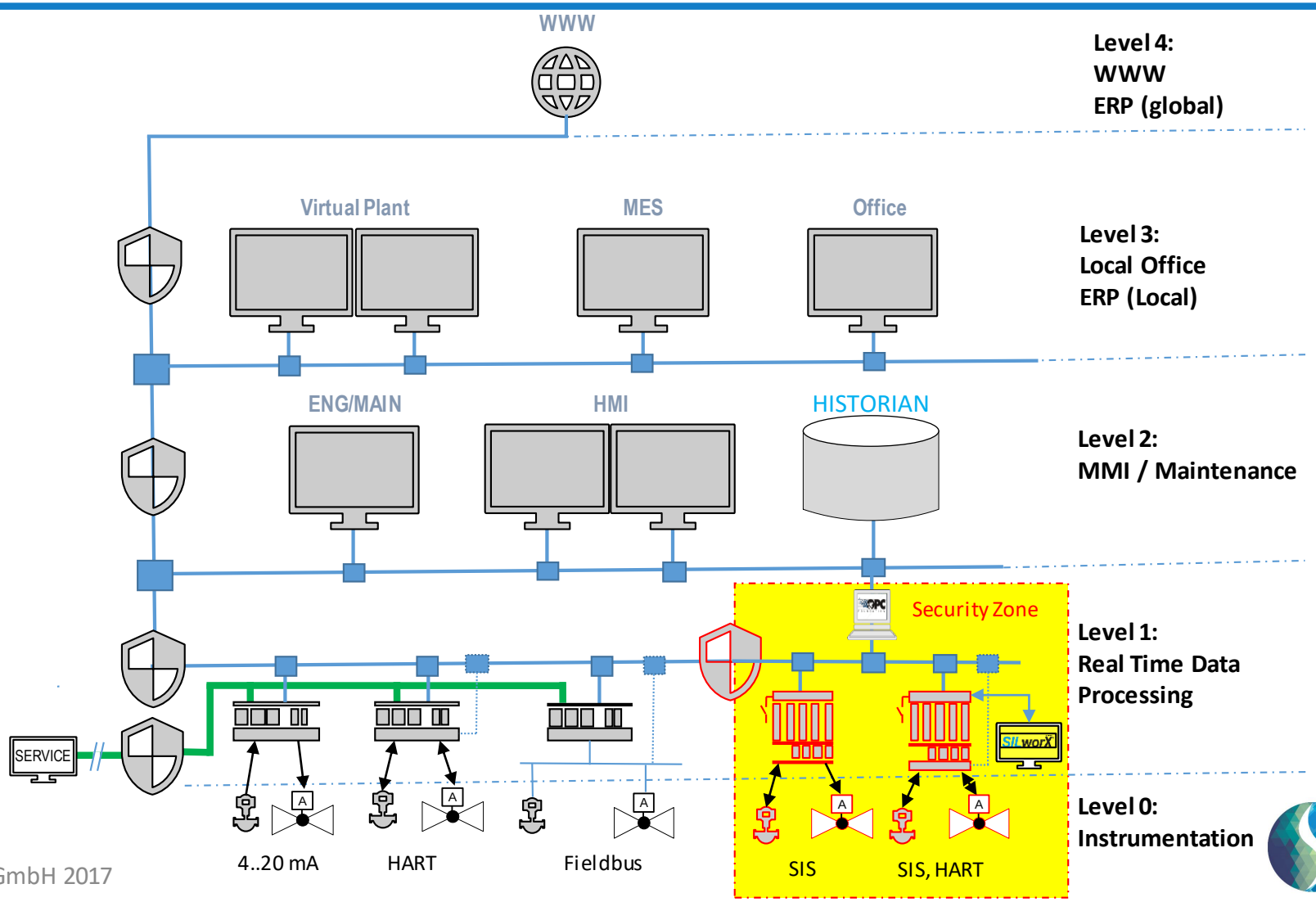
Use Case: ERP Access



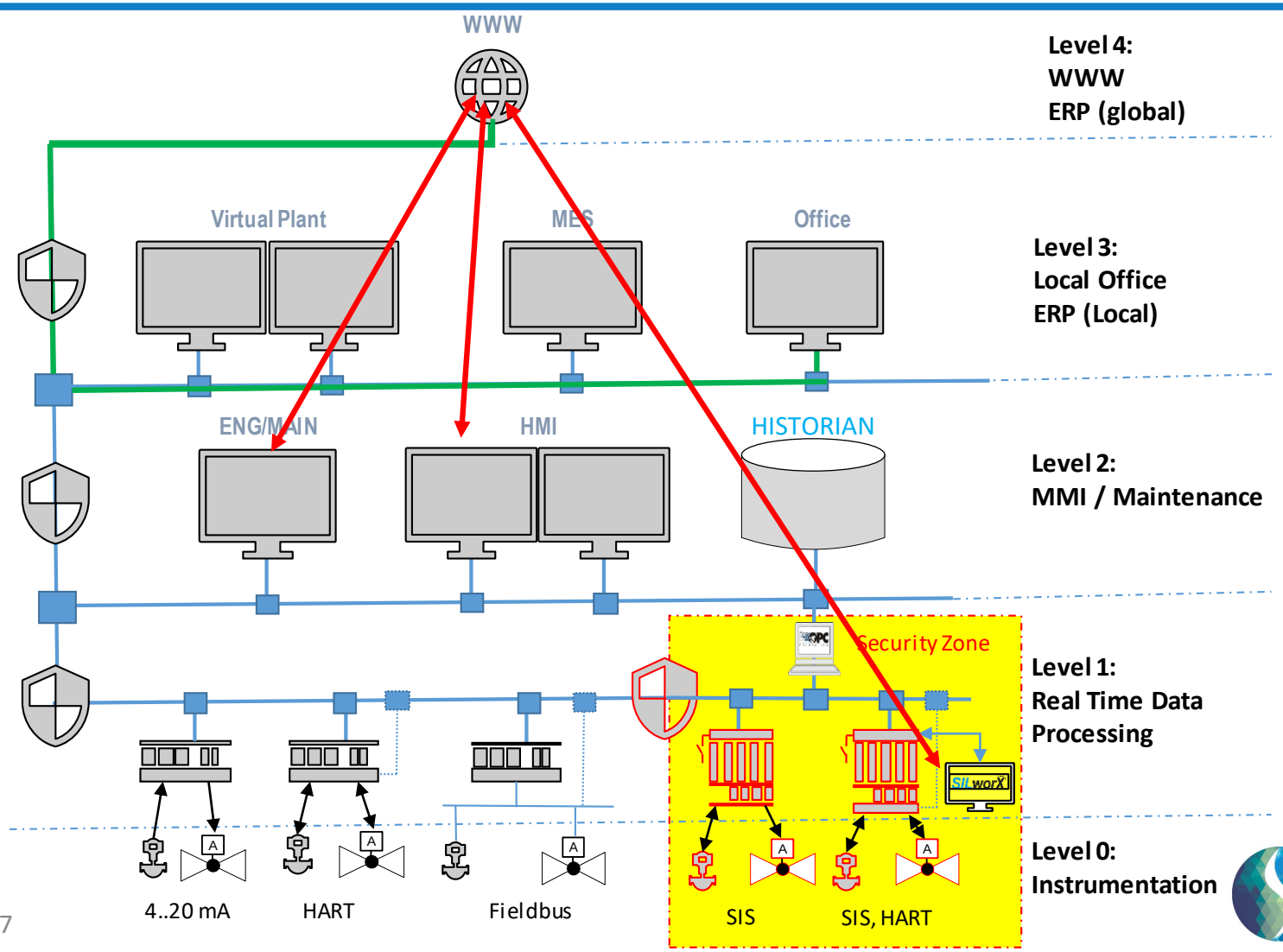
Use Case: Remote Access



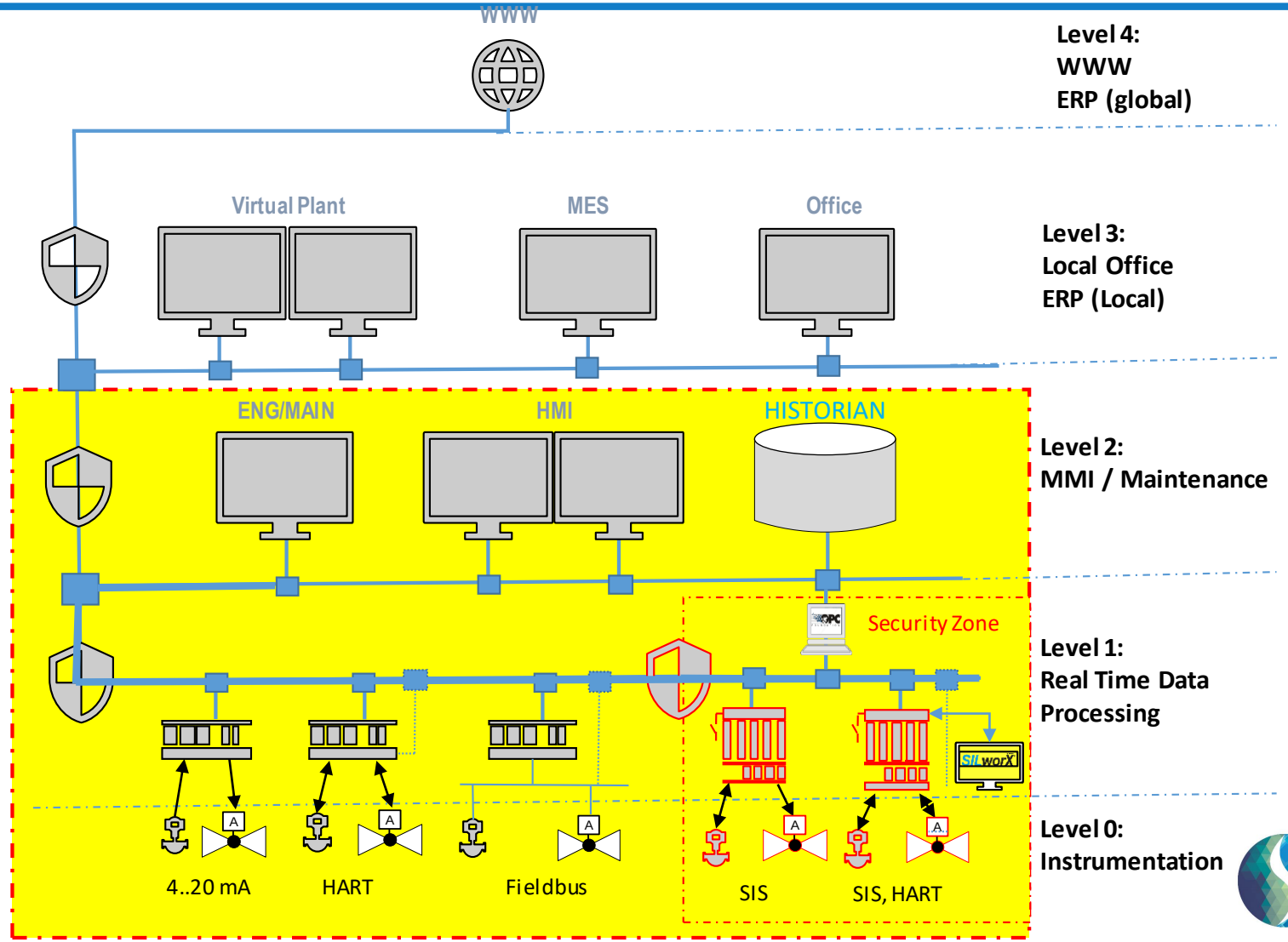
Use Case: Service Notebooks



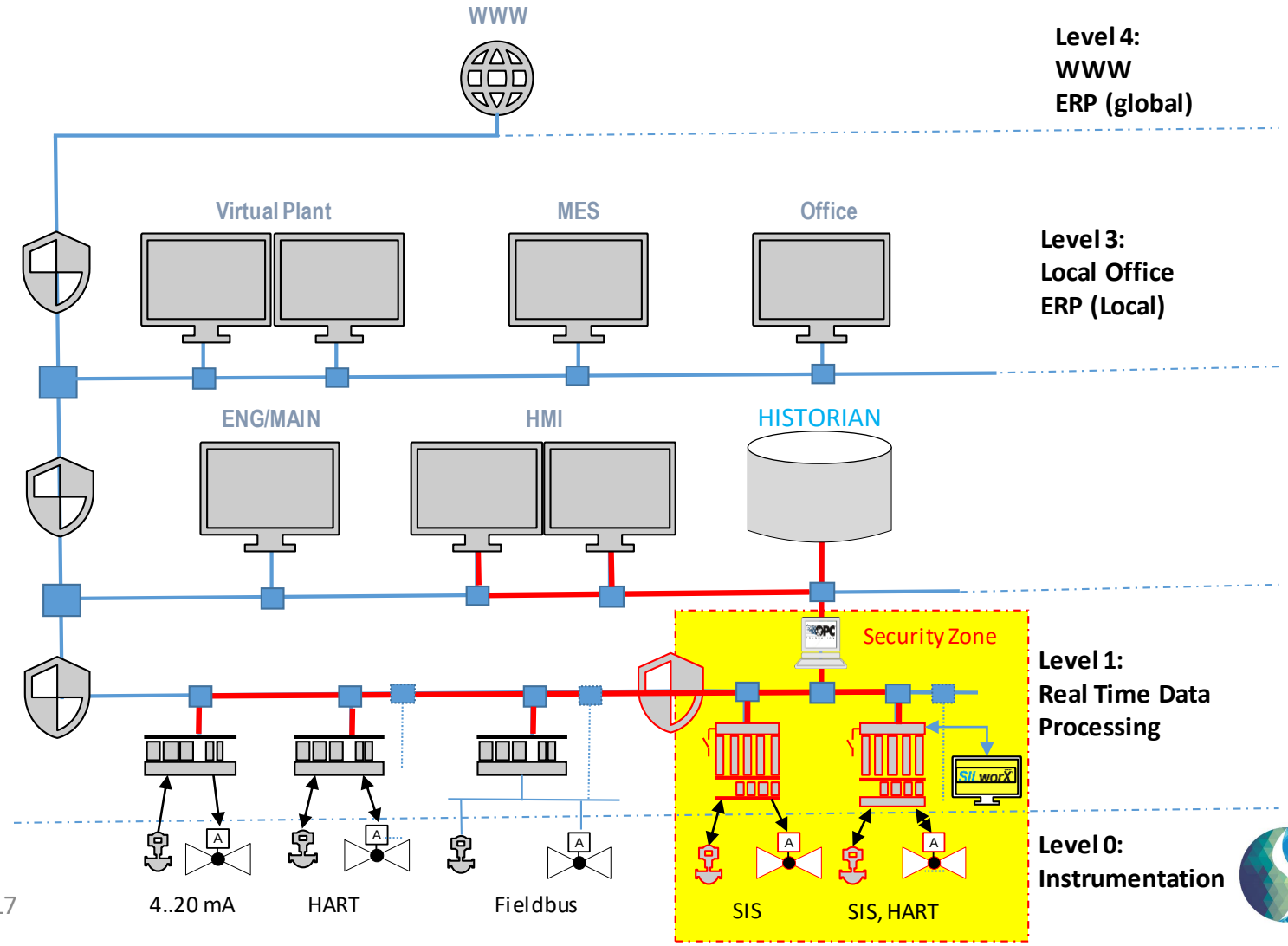
Use Case: Internet Access



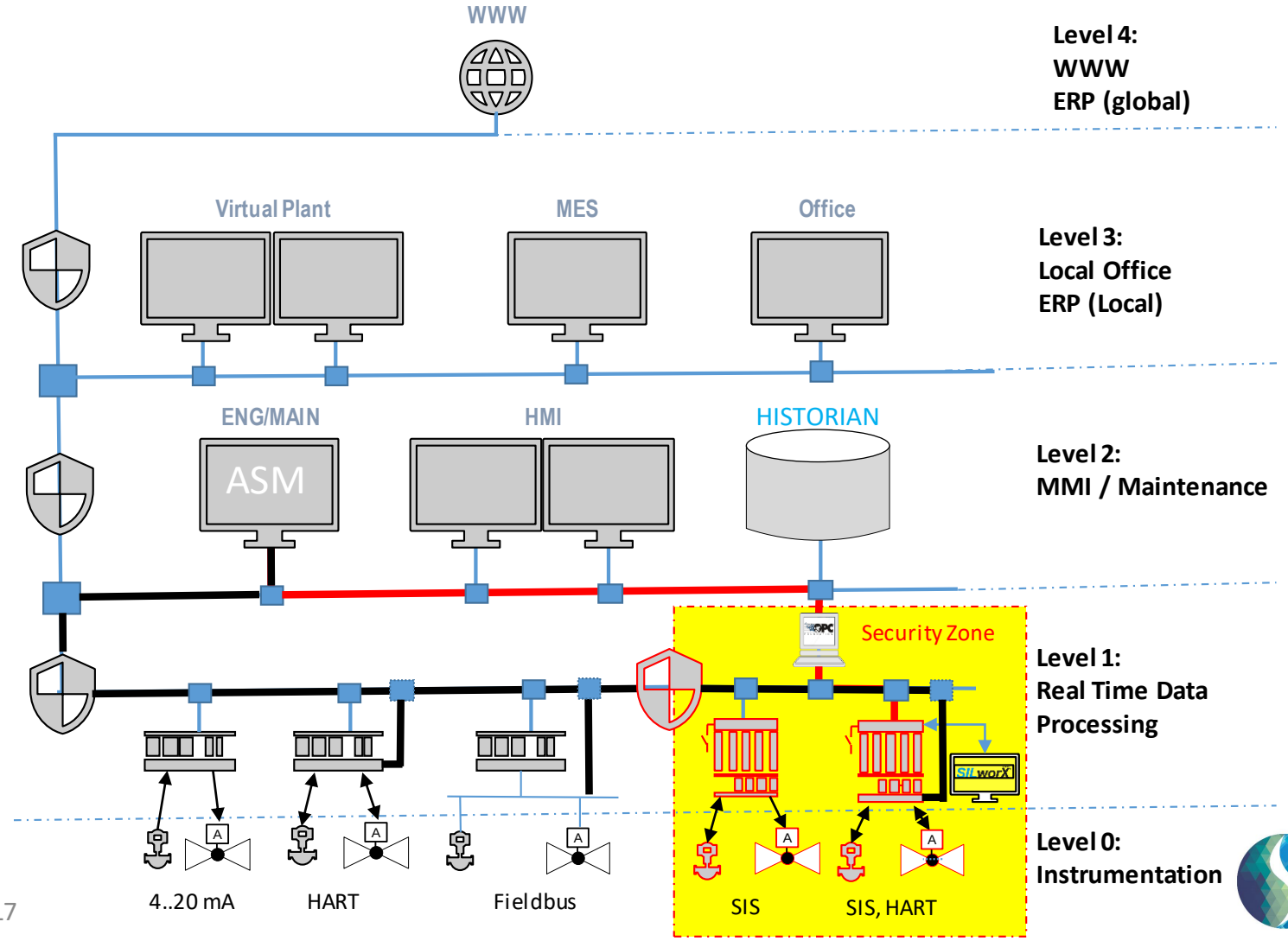
Use Case: Unification of engineering Stations



Use Case: Data to DCS



Use Case: HART for SIS Field Devices



Closing Thoughts

> The world is a dangerous place to live; not because of the people who are evil, but because of the people who don't do anything about it."
>
> **Albert Einstein**

So, let's go and do something!

Thank You.

Peter Sieber,
Vice President Region China
Vice President Norms & Standards

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 6202 709-0
Fax: +49 6202 709-107

E-mail: info@hima.com
Internet: www.hima.com

Safety Case Symposium 2018
Singapore
www.SafetyCaseSymposium.com