INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

TC65: Industrial-process measurement, control and automation

Automation Forum

Dalian, China 29 October 2015

Bridging safety and security

Koji Demachi – TC65/AHG1 Convenor

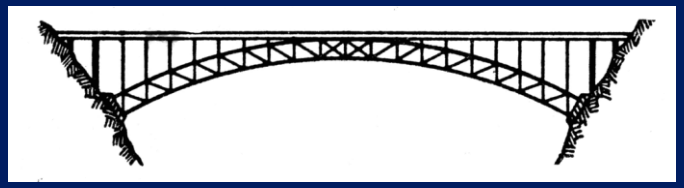
Bridging safety and security

Outline

- Introduction
- Gaps and Challenges
- Benefit and Opportunities
- Examples
- Proposal

Introduction

- **Safety and Security are big concerns for industry**
  - **Large hazards: High-energy, Harmful substance**
  - **Serious consequence: High-criticality**
- **Many Safety and Security standards exist today,**
  having commonalities but differences too
- **Differences raise challenges**
- **Commonalities raise opportunities for efficiency**
- **Solutions are needed**



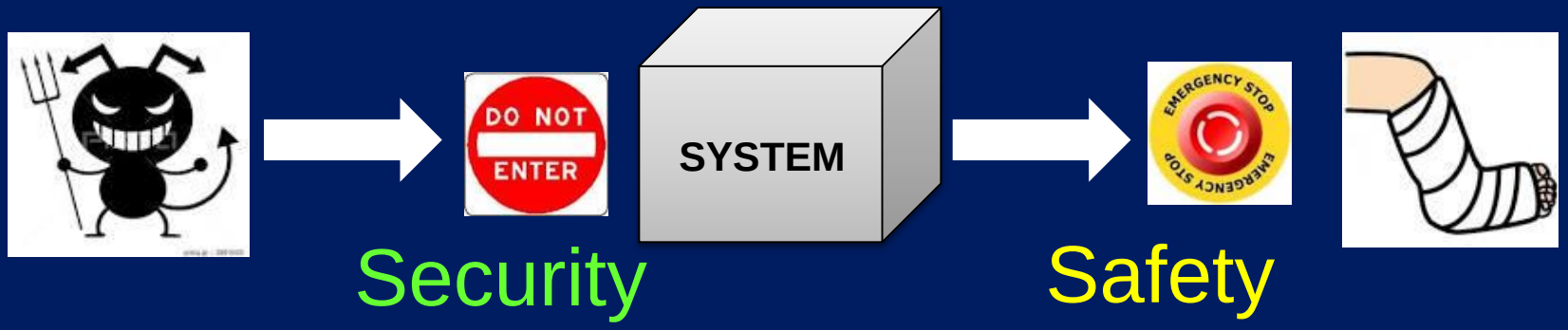
➢ **BRIDGE these standards**

- **to create a path of understanding**
- **to allow effective collaboration between them**

Differences (security/safety)

- **Both have the same final objective**
  - **to reduce risk to acceptable level**

- **Each has different approach**
  - **Safety: to protect Human, Environment and manufacturing systems**
  - **Security: to protect the system from outside attacks**



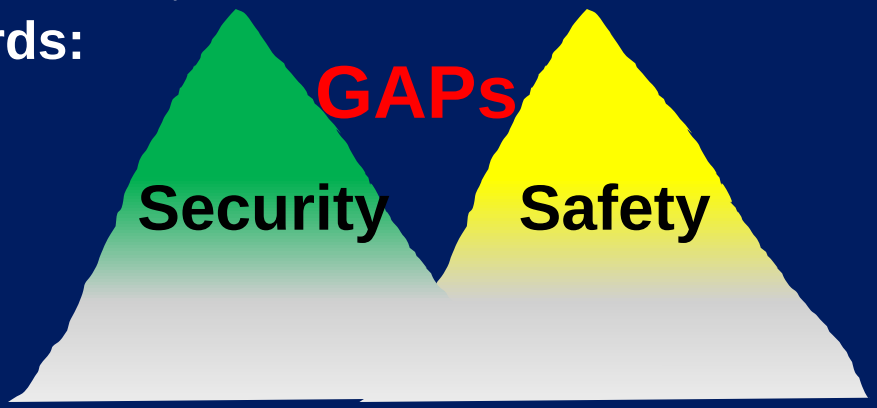
Commonalities & Differences

Differences:

- Focusing on: Outside / Inside
- Focusing on: Data / Physical asset
- Only systematic failure / Including random failure
- Malicious users / Trusted users
- Variable volatile risks / Stable risks
- Effectiveness / Correctness
- Non-quantitative / Quantitative
- SL, EAL / SIL

Security standards:

ACSEC
ISO/IEC 27000
IEC 62443
IEC 62351
IEC 62859
ISO/IEC 15408
ISO/IEC 18045
DO 326A
DO 355



Commonalities:

- Reducing risk to acceptable level
- Risk assessment, Audit
- Lifecycle management
- Boundaries, perimeters

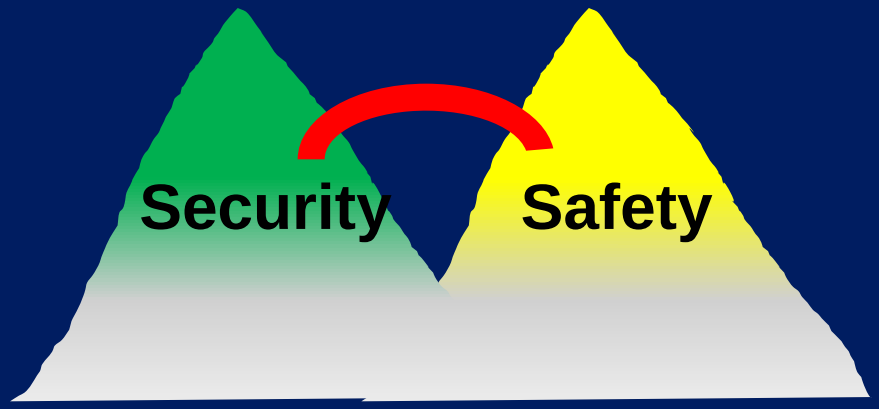
Safety standards:

ISO/IEC Guide 51
IEC 61508
IEC 61511
IEC 61513
IEC 62061
ISO 13849
IEC 60601
ISO 26262
EN 50126/7/8
DO-254
ARP4754
ARP4761

Benefits & Opportunities

- **Bridging differences could minimize conflict**
- **Bridging commonalities could avoid duplication**

- **The bridging will facilitate:**
  more safe, secure and effective
  implementation, deployment and management
  of industrial systems.



Examples of BRIDGING

Showing some examples, using the following template

- **Viewpoint**
  <The aspect for the following topics>
- **Commonalities**
  <The commonalities of safety and security in terms of the aspect>
- **Differences**
  <The differences between safety and security in terms of the aspect>
- **Challenges**
  <The issues caused by the differences>
- **Potential Bridging**
  <A potential solution solving the issues and its benefit>

Example-1

- **Viewpoint:** Risk
- **Commonalities**
  - Objective is to reduce the risk to the acceptable level
- **Differences**

  Safety: Stable risks, Quantitative scale, Trusted personnel
  need to minimize changes

  Security: Variable volatile risks, Non-quantitative, Malicious personnel
  need for rapid change
- **Challenges**
  - To have a common scale of risk
  - To have a common risk management
- **Potential Bridging**
  - Mechanism to convert and to integrate the two types of risk
  - Synchronizing safety and security lifecycle management

Risk

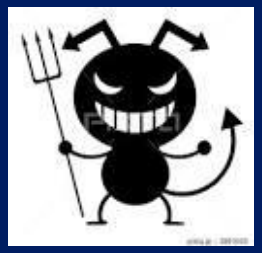
Vulnerability inside

Slow
Stable

Hazard inside

Threat outside

Quick
Volatile



Malicious personnel

SL

Security

SYSTEM

SIL

Safety

Trusted personnel

Example-2

- **Viewpoint:** Requirements
- **Commonalities**
  - Both need to address both devices and system
- **Differences**

  Safety: Focus on mainly inside of the system and its boundary

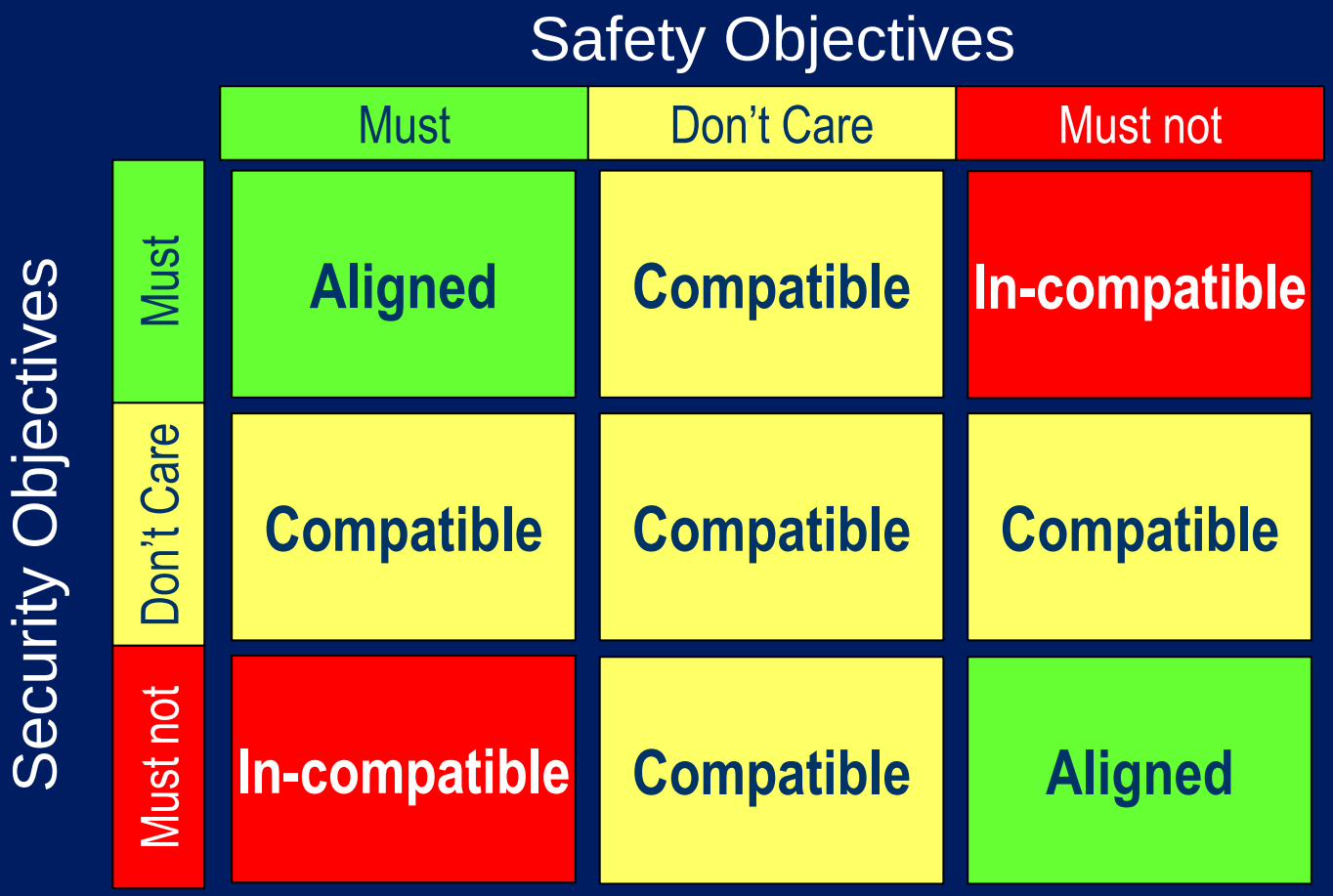
  Some safety requirements conflict with security requirements

  Security: Focus on mainly outside of the system and its boundary*

  Some security requirements conflict with safety requirements
- **Challenges**
  - To solve the conflicts with minimum impact to each
  - To avoid the duplications
- **Potential Bridging**
  - Defining interface between safety function and security function
  - Coordinating priorities of safety and security requirements

*except insider threat

Requirements



Example-3

- **Viewpoint:** Origin of standards
- **Commonalities**
  - Objective is to reduce the risk to the acceptable level
- **Differences**

  Safety: Focusing on Physical assets, Including random failure, Originated from Automation and Control Technology

  Security: Focus on data, Only systematic failure, Originated from Information and Communications Technology

  Each has different terminology
- **Challenges**
  - To share and understand ideas of each other
  - To collaborate with each other
- **Potential Bridging**
  - Mechanism to translate languages bi-directionally

Origin of the standard

English	Safety	Security
French	**Sécurité**	**Sécurité**
German	**Sicherheit**	**Sicherheit**
Italian	**Sicurezza**	**Sicurezza**
Spanish	**Seguridad**	**Seguridad**
Chinese	安全 (ANCHUANG)	安全 (ANCHUANG)
Japanese	安全 (ANZEN)	セキュリティ (SEKYURITHI)
Korean	안전 (ANJONG)	보안 (POAN)

Proposal (Next Step)

- **TC65/AHG1 is preparing a new work item proposal for developing a Technical Specification**
  - To facilitate the application of safety and cyber security standards by bridging the relevant technical areas
  - The scope includes, but is not limited to, aspects of the cyber security of safety-related systems.
- **This TS is the 1st step.**
- **The project does NOT intend to integrate existing standards into one standard**
  - To promote a more widespread, cost effective and consistent application of the relevant applicable standards.

Invitation

- NP is expected to be circulated shortly
- **Your participation is really appreciated!!**
- The output of AHG1 (65/xxx/INF) will be reported during TC65 plenary meeting on October 30th

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

THANK YOU!