

CECIP

European Association
of Weighing Instruments
Manufacturers

**CECIP webinar - Data security
3 December 2020**

Welcome





Data the new oil/gold



Data creation in different sectors



| WELMEC | EU | OIML | Standards | Others |
|-----------|---------------------------|-----------------|-----------|---------------------------|
| Guide 7.2 | Radio Equipment Directive | D31 on software | IEC62443 | General fraud legislation |
| Etc. | Cybersecurity act | R76 | | |
| | GDPR | R51 | | |
| | NAWID | Etc. | | |
| | MID | | | |

- Presentations

- Bobjoseph Mathew, Vice Director METAS & Vice President OIML
- Paul Turner, Head of Legal Metrology NSAI
- Ulrich Rauchschalbe, Head of Controller Development Schenck Process & CECIP LMG member

- Panel debate

- Questions & Answers audience

Bobjoseph Mathew (METAS & OIML)



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Institut für Metrologie METAS



Data Security

Bob Joseph Mathew, Vice Director METAS, Head of Legal Metrology

Focus of the presentation

- **Importance of Data Security assessment**
- **Device Security and Process Security**
- **Example for an approach for the assessment**

Casino Leak



Source: Bitdefender Box

- A casino had customer data stolen from them via the aquarium
- The aquarium used an IoT temperature sensors connected to the WiFi
- Using a trivial vulnerability in the smart thermometer, hackers gained access to the network, retrieved data about high-paying customers

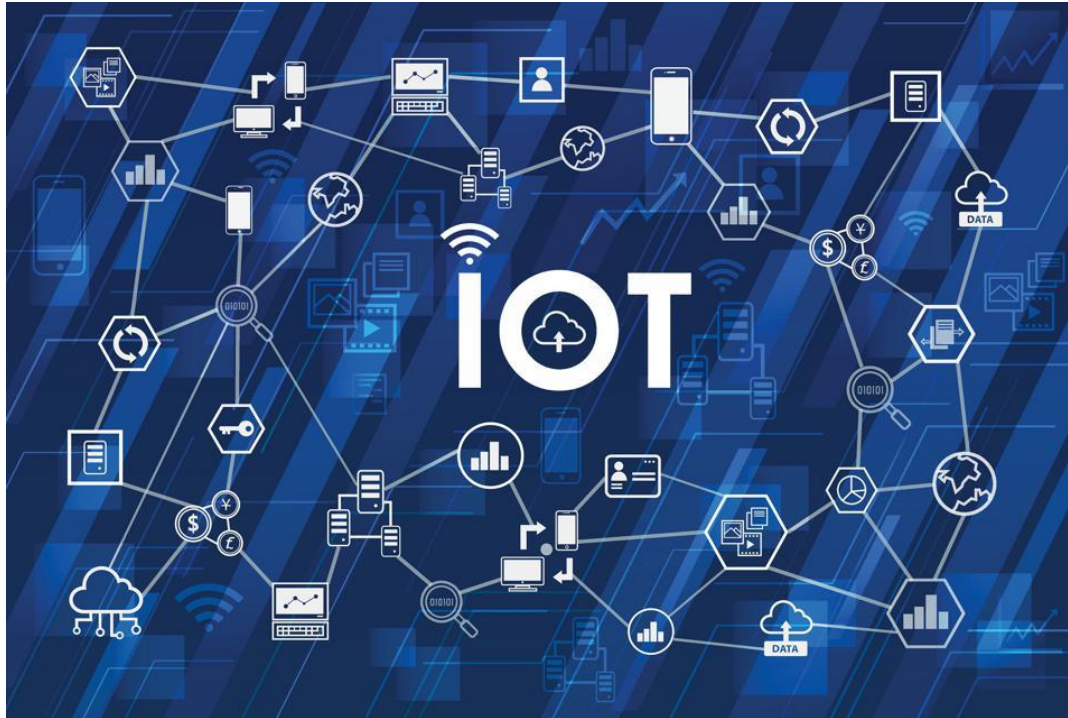
Scale of the challenge



Source: Specialist Hub

- **Security breaches** have increased by 11% since 2018 and 67% since 2014 (Accenture)
- The average time to **identify a breach** in 2019 was 206 days (IBM)
- In the **GDPR's** first year, there were 144,000 complaints filed with various GDPR enforcement agencies and 89,000 data breaches recorded (EDPB)
- **Financial and Manufacturing services** have the highest percent of exposed sensitive files at 21% (Varonis)
- **Supply chain attacks** are up 78% in 2019 (Symantec)
- **IoT devices** experience an average of 5,200 attacks per month. (Symantec)

Internet of Things



Source: Adobe Stocks

- Network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet (Wikipedia)
- Increasing connectivity and interdependencies
- Measuring instruments are part of IoT

Measuring Instruments are exposed to risks



For example

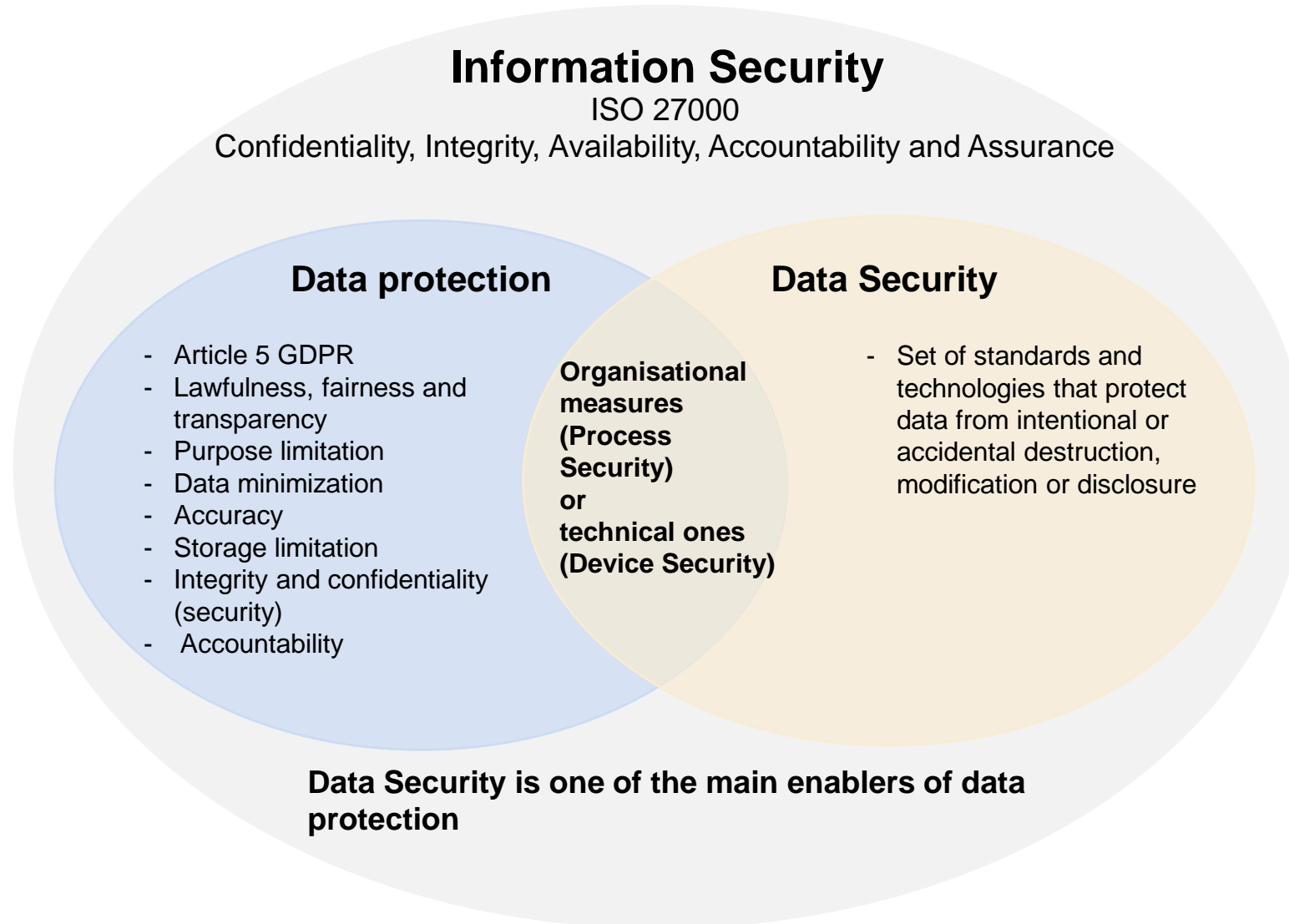
- Interruption of production and availability of services
- Violation of data privacy
- Manipulated measurements or calculations

Questions arise

- Software update
- Data transfer, Measurement results

Leads to potential threats concerning information security, data security and data protection

Information security/ Data protection/ Data security



Data Security: Vulnerabilities

| | | | |
|----|---|---|---|
| 1 | Weak, Guessable, or Hardcoded Passwords | ★ | △ |
| 2 | Insecure Network Services | | △ |
| 3 | Insecure Ecosystem Interfaces | | △ |
| 4 | Lack of Secure Update Mechanism | ★ | △ |
| 5 | Use of Insecure or Outdated Components | ★ | |
| 6 | Insufficient Privacy Protection | ★ | △ |
| 7 | Insecure Data Transfer and Storage | ★ | △ |
| 8 | Lack of Device Management | ★ | |
| 9 | Insecure Default Settings | ★ | |
| 10 | Lack of Physical Hardening | ★ | △ |

OWASP (Open Web Application Security Project) IoT Top 10, which represents the top ten things to avoid when building, deploying, or managing IoT systems (Vulnerabilities)

OWASP

★ Process Security

△ Device Security

Data Security comprises

Device Security



- Functionalities
- Interfaces
- Cryptography
- Data transmission
- Operations
- RAMS (Reliability, Availability, Maintainability, Safety)

- Preservation of
- Confidentiality
 - Availability
 - Authenticity
 - Integrity

Process Security



- Operations
- ISMS (Information Security Management System ISO 27000)
- Training
- Infrastructure
- Data
- User / Clients / Roles
- Data Protection (GDPR)

- Preservation of
- Confidentiality
 - Availability
 - Authenticity
 - Integrity



Source: Allianz Risk Barometer 2020

Example for an approach for Data security assessment



«Protection Requirement Analysis Smart Metering in Switzerland»

| Threats | B1: Unberechtigte Modifikation Daten lokal | B2: Unberechtigte Modifikation Daten remote | B3: Unberechtigte Modifikation Zeiten | B4: Unberechtigter Datenzugriff lokal | B5: Unberechtigter Datenzugriff remote | B6: Unberechtigter Datenzugriff auf im Gerät gespeicherte, nicht mehr bearbeitete Daten | B7: Unberechtigtes Schalten des Breakers | B8: Unberechtigtes Schalten der Relais im Smart Meter | B9: Sicheres Aufstarten | B10: Einschränkung der Verfügbarkeit der Daten |
|---|--|---|---------------------------------------|---------------------------------------|--|---|--|---|-------------------------------------|--|
| Protected objects | | | | | | | | | | |
| O1: Messdatenverarbeitungssystem | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| O2: Visualisierungsplattform | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| O3: KS0 Lokale Schnittstelle Administration | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| O4: KS3 Schnittstelle WAN | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| O5: KS2 Schnittstelle HAN | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| O6: KS1 Schnittstelle LMN | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| O7: Kryptoschlüssel | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| O8: Firmware Update | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| O9: Firmware | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| O10: Zählerkonfigurationsdaten | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| O11: Zeiten (System, RTC) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| O12: Netzrelevante Daten | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| O13: Lastgang, Registerdaten | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| O14: Alle Daten aus dem Smart Meter | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Directive for Data Security of Intelligent Measuring Systems (Device/Process)

Testing methodology

Key success factors

- Without data security no data protection
- Legal requirements need to cover process and device security
 - A core baseline of IoT device security capabilities for manufacturers
 - Risks are context-dependent and situational
 - Customised, risk-adapted approach
 - Secure, flexible and allowing innovation
 - Requirements for secure operation (ISMS)
- Security experts wanted
- Fast technical evolution – can regulation keep up?





Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Institut für Metrologie METAS



Thank you very much for your attention

Paul Turner (NSAI)

CECIP Webinar

Data Security

Paul Turner
Head of Legal Metrology

3rd December 2020



Legal Metrology

- Inspection of Instruments in use
- Verification of Instruments in use - outsourced
- Pre-Packaged Goods
- Market Surveillance
- Notified Body – Module D & F
- National & International Representation for Ireland

Our Legislation

- Metrology Act, 1996
- Unlike most European countries, NO statutory verification interval
- Instruments must be verified at all times
 - Conformity assessment
 - Sealed
 - Within legal tolerances
- NAWI Inspections – EN45501



Approach to Inspection & Challenges

| Approach | Challenges |
|-----------------------------------|--|
| Type Approval & Test Certificates | Not possible to tell when physical seals broken |
| Markings | Not possible to tell when new hardware installed |
| Correct installation & setup | Not possible to tell when cabling replaced |
| Metrological Test | Difficult to access and trace cabling |
| Data security & integrity | Difficult to identify cabling |

45 tonne Weighbridge Example



Weighbridge Access to Junction Box



Ideal Junction Box



Reality



The Future ???

- Ongoing recruitment of electrical/electronic and IT specialists for Legal Metrology
- Digital pairing using over air signalling
- No cabling
- Secure pairing of load cells and display
- Any changes will be captured by event counter, logging time and date of change
- Automatic Notification sent to authorities when event counter changes
- WELMEC 7.2 – Software Guide for Measuring Instruments Directive 2014/32EU
– “Transmission of measurement data (T)”



Milk Meter Example

Piper Systems PD688 Display and digital pairing of peripheral devices:

The PD688 Display module is connected via a secured interface to the flow transmitter (the PD340 Magnetic Flow Meter)

The Flow Meter is digitally paired with the Display module using the Flow Meter's unique serial number, which is a protected value embedded within the flow meter's software.

This serial number can be displayed on the display/controller and validated

If the flow meter is replaced, the replacement meter then needs to be digitally paired with the display unit and a change to the meter and serial number is recorded within the system software.

Provides better traceability for regulators and confidence for consumers

Thank you.

WWW.NSAI.IE

paul.turner@nsai.ie



Search "NSAI"



Ulrich Rauchschalbe (Schenck Process)

Data Security

A large graphic with a dark blue background. In the center is a glowing padlock icon surrounded by a circular ring of light. Radiating from this center are numerous thin, light blue lines that resemble a complex network or circuit board, extending towards the edges of the frame.

CECIP Webinar 2020-12-03

1. Why data security?
2. Internal Data Security
3. Data transmission
4. Technology helps
5. Room for innovations



1. Why data security?

2. Internal Data Security

3. Data transmission

4. Technology helps

5. Room for innovations



THE WORLD IS CHANGING

- **Structure of plants and applications change**
 - De-localized
 - Cloud storage
 - Remote Service
 - ...
- **Customer (and notified bodies) sensitivity increases**
 - Real security breaches, e.g.
 - US election 2016
 - Ebay
 - Facebook
 - ...
 - Media hype
- **Threats increase**
 - More hackers out there
 - Even on government level
 - Better tools available



ORIGIN FOR REQUIREMENTS

- **Some requirements are LFT ones**
- **Others – the majority – are driven by other legislation OR by customers**



DIFFERENT REGIMES FOR DATA SECURITY

- Often: Data security ⇔ Data transmission
- 1. Internal data security
- 2. ‚External‘ Data Security, i.e. Data Transmission



1. Why data security?
2. Internal Data Security
3. Data transmission
4. Technology helps
5. Room for innovations



→ Typical approach: Risk assessment

1. ASSETS TO PROTECT

- Process availability
- Protection customer data
- **Protection of customer infrastructure**
- **Correct Weight !**
- (Safety of people)
- (Protection of the environment)



2. RISK POTENTIAL – OF A SCALE

- It is not about environmental hazards or disasters (SIL)
- It is not a matter of danger to life and limb (EN 13849)
- A **legal-for-trade** scale is 'only' about money



- **But** financial damage must of course also be averted.



3. WHO IS THE POTENTIAL FRAUDSTER

- „Russian hackers“ - i.e. third party, high capability ??
 - Will rather hack
 - Internet Banking
 - Ebay or
 - The German government
 - ...
- The operator - i.e. an involved party ??
 - Does not usually have the capabilities
 - Often has much simpler methods – weigh more than shipped
- The manufacturer ??
 - Motivation ?
 - Usually easy to do !
 - Trust must be there !



1. Why data security?
2. Internal Data Security
3. Data transmission
4. Technology helps
5. Room for innovations



VERY DIFFERENT USE CASES

1. ‚Local‘ installations

- Scale to POS
 - Scale to ERP / PLC / SCADA system –
 - Scale to Data Storage
- ➔ ‚Conventional‘ solutions are appropriate



.....

N. WLAN / Internet / Cloud solutions

- Truck scale to company HQ
 - Cloud storage for LFT data
 - Metrology Cloud
 -
- ➔ High security solutions are required



VERY DIFFERENT USE CASES

X. Data transmissions without data

- Internet connection to equipment
- The real threat
- See ‚Internal Data Security‘



1. Why data security?
2. Internal Data Security
3. Data transmission
4. Technology helps
5. Room for innovations



TECHNOLOGY HELPS

- Biggest challenges are the WLAN / Internet connections
 - Technology is readily available to solve these challenges !
 - E.g. HTTPS
 - PKI
 - **End-to-end Encryption**
 -
 - State-of-the-art Hardware supports all this

- Restrictions due to
 - Export restrictions
 - Older Hardware
- Requires a technology cycle

- Perform a risk assessment



1. Why data security?
2. Internal Data Security
3. Data transmission
4. Technology helps
5. Room for innovations



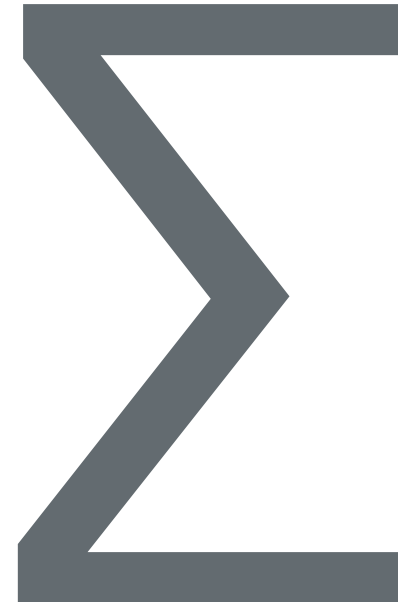
LEAVE ROOM FOR INNOVATIONS

- Regulations are necessary !
 - Define the Assets
 - Formulate essential requirements
 - Appropriate for the applications
- Leave room for Innovations
 - Technology cycle is 2-3 years
 - Good ideas happen every time !
 - Security standards follow this cycle
- Revision cycle of OIML Rs is 10 years
- Revision of R76 will take \approx 5 years
- R76 \rightarrow EN 45501 took 10 years
- WELMEC is not really faster



SUMMARY

- Security is an issue
- There is more to protect than weights
- Risk assessment is the tool to use
- E.g. based on accepted Security Standards
- We (manufacturers) see Challenges
- AND Chances !



schenck process



Panel discussion

- Follow CECIP on LinkedIn
- Register for the CECIP newsletter

Follow US

Sign up to stay up to date with the latest news from CECIP

Subscribe



European Weighing Industry

Thank you

For more information,
please **contact:**

Tim Hamers

CECIP's Secretary General:

tim.hamers@cecip.eu

+32 2 706 82 15

www.cecip.eu

CECIP offices:

Bluepoint Building
Boulevard Auguste Reyers 80
B-1030 Brussels