Stakeholder views on the future role of standardization, testing and certification

Notified Body

Eric FAE – INERIS (France)

Eric.fae@ineris.fr

1) **Responsibility for a product that is part of a digitalized process including artificial intelligence**.

2) **Are NB competent for innovative products (in case no standards are available)?**

3) **Improvement of Coordination of NB is needed?**

4) **Importance of Testing & Certification is increasing in the future considering that standardization is often too slow to keep pace with technological development?**

5) **Notification authorities in Europe give NB's enough flexibility to act on innovations?**

Before to answer the question : what is the actual mandatory situation and state of art in machinery sector

- <u>Standardization vs certification</u>
- Standards gives the state of the art and the harmonized standards can be used to give presumption of conformity
- 2 kind of standards :
  - Standards for **machine manufacturers**
    - type B standards e.g. ISO 13849-1 / IEC 62061 how to integrate safety device to build a safety function
    - Type C standards
  - Standards for **safety devices manufacturers** how to build the safety devices in terms of architecture and fault reaction (IEC 61508 and ISO 13849-1).
- These functional safety standards (IEC 61508 and ISO 13849-1) are the one used today to certify the smart devices used for **digitalized systems (hardware + software)**

EUROSHNET Dresden 2019

1) Responsibility for a product that is part of a digitalized process including artificial intelligence

- Safety of process vs safety of persons
- **Process** = voluntary certification (IEC 61508 / IEC 61511)
- **Machinery** : self certification when all EHSR **E**ssential **H**ealth and **S**afety **R**equirements are covered by one or more harmonized standards;
- Today for these new smart devices, we are in the **same configuration** as in the end of 1990 when new electronic safety devices (new technology not only based on electromechanical devices).
- For this purpose, a European project was raised STSARCES - Standards for Safety Related Complex Electronic Systems that deal with certification procedures for safety devices that is always applicable.

1) Responsibility for a product that is part of a digitalized process including artificial intelligence

- Before this period (end of 1995) for the application of the machinery directive for safety components, electronic devices were used not for safety but for product management and if they fails, the consequence was not impacted the safety of workers.

- Today the situation is :
  - You have machine manufacturer that build machines according to the requirements of Annex I of machinery directive
  - They use monitoring devices (standard PLC, …)
  - They use safety components (safety barriers -SICK for example, safety PLC, …).

1) Responsibility for a product that is part of a digitalized process including artificial intelligence

- c) 'safety component' means a component:
- — which serves to **fulfil a safety function**,
- — which **is independently placed on the market**,
- — the failure and/or malfunction of which endangers the safety of persons, and
- — which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function.
- An indicative list of safety components is set out in Annex V, which may be updated in accordance with Article 8(1)(a);
- These safety components are in most cases logic units that are defined in annex IV of the machinery directive 21. Logic units to ensure safety functions.
- An indicative list of logic unit was presented inside a RfU by VG 11 under the reference CNB/M/11.045/R/E Rev 06

EUROSHNET Dresden 2019

1) Responsibility for a product that is part of a digitalized process including artificial intelligence

- Theses logic unit are assessed / certified according safety standards : IEC 62061 based on IEC 61508 or ISO 13849-1/2
- First thing as it was said during the past 2 days in the conference : regulation and standardization is not simple.
- When these logic unit / safety components are certified they are put on the market by the manufacturer of the device under its responsibility
- **So the answer for the first question :**
- Responsibility for a product that is part of a digitalized process including artificial intelligence.

1) Responsibility for a product that is part of a digitalized process including artificial intelligence

1. Does the product that is part of a digitalized process including artificial intelligence **assume its own safety function** ?

- If **yes** then the situation is similar to the actual one.

- At INERIS we are in the process :
  – to certify a device with Bluetooth communication (connected object)
  – to certify an AI safety system based on image recognition for a typical application (external environment well defined)
  – To certify a safety system that also embedded NON safety functions based on IA (image recognition, LINUX, …) **and we are on the core of the EUROSHNET conference**

- If **NO** then my answer is different :

1) Responsibility for a product that is part of a digitalized process including artificial intelligence

- **DR. STEIGER :**
- *Safety of machine is based on stable situations (…) IT security is based on the fact that the situations are not stage and are moving*

- **O. GORNEMANN**
- *you will not certify product but process – need to change the regulation*

EUROSHNET Dresden 2019

1) Responsibility for a product that is part of a digitalized process including artificial intelligence

- **My questions and perhaps a preliminary conclusion**
  - When the certification is based on the **process**, if the process changes where are the limits of what is checked/assessed/certified ??
  - We saw with AI, that if the model / algorithm is not good, the hazard is always present (remember the car on the presentation "**The influence of artificial intelligence on standardization and OSH")**.
- So if we do not certify products, we will have to certify perhaps **not a product (or logic unit of safety component)t but perhaps a process but in this case in a defined external environment and in a defined collaborative environment**.
  - HOW ??
  - Who will take the responsibility ??
  - Who will eat the oranges ??

2) Are NB competent for innovative products (in case no standards are available)?

- Machinery directive is not a stop for technology innovation.

  New changes, new skills, change comes from discomfort and there is a resistance to human being

New technologies today based on software with different kind of software with different layers (from WEB to machine language)

- The stop is given by the persons who do not want to change their habits face to the non-presence of the harmonized standards and the lot of different knowledge that is necessary to assess and certify these new devices.

- For machinery and "*cybersecurity aspects but not only*" : IEC TS 63074 that is based on IEC 62443 series for machinery sector and other publications at ISO levels

EUROSHNET Dresden 2019

3) Improvement of Coordination of NB is needed?

- The rules exists and are in place
- **As in the past for complex electronic devices** when harmonized standards were not present the notified bodies apply prEN ….., and other document that were **the state of art,** example for safety systems :
  - the German draft DIN V VDE 0801 based on DIN V 19250 which builds up a hierarchical system of eight risk reduction levels AK)
  - **IEC 1508 parent of IEC 61508**

    Preliminary answers were given by the RfU

4) Importance of Testing & Certification is increasing in the future considering that standardization is often too

slow to keep pace with technological development?
5) Notification authorities in Europe give NB's enough flexibility to act on innovations?

- YES for 4 & 5
- **All the information presented in the present presentation is not the position of the notified bodies in Europe, but the position of the speaker**

Thank you

Eric FAÉ - INERIS