The Need of Improved Methods to Handle Functional Safety and Cybersecurity in Critical Industrial Infrastructures

Mary Ann Lundteigen[1] and Bjørn Axel Gran[2]

[1]Professor, NTNU (mary.a.lundteigen@ntnu.no)
[2]Halden Project & Adjunct Professor NTNU (bjorn.axel.gran@ife.no)

Norwegian University of Science and Technology

NTNU

The starting point

- **Industrial control and safety** (ICS) systems represent an important critical infrastructure.
- **Functional safety** is the safety achieved by industrial control and safety (ICS) system(s)
- Traditionally, this has been ensured by the ICS system **responding adequately** to **physical hazards and events** arising in a system under protection.
- The specification, design and operation/maintenance of ICS systems involve many **"traditional" ("non-IT")** engineering disciplines and skilled workers
- **Standards** developed for functional safety are mainly developed by these disciplines.

Example: Oil and gas

NORSOK S-001, P-002	ISO 10418 ISO 13702
Norwegian Oil and Gas GL 070	IEC 61508 IEC 61511

The current situation

- An ICS is **no longer isolated** from the worldwide web
- ICS systems are **desired targets** to outside hackers
- Cybersecurity attacks *can* result in **major accidents**

Thus:

- It is recognized that functional safety **cannot be ensured** without also considering cybersecurity

ICS and cybersecurity events

- Maroochy water breach (2000)
- Stuxnet worm (2007)
- Pipeline system Sabotage, Turkey (2008)
- Maersk attack by ransomware (2017)
- TRITON attack (2017)
- **Hydro attack (2019)**
  - affected the ability to operate the plants ICS's
  - No safety incidents were reported
  - Manual measures was necessary to stop the plant in case of unsafe events.
  - Cost estimated now to about 400-450 MNOK

Source: https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

Gaps – as observed for the industry

- **Standards** on functional safety of ICS systems are **not aligned** with standards on cybersecurity
- Traditional disciplines involved in ICS specification, design, installation, operation and maintenance have **insufficient knowledge** about how they may impact or introduce cybersecurity vulnerabilities
- Many ICS systems include **older technologies**
- Methods used to define safety requirements, realize safety functions, and assess their performance **do not address** the impact of cybersecurity

Scope of the paper

- Identify **element**s of the «state of the art» on standards, industry guidelines, research on cybersecurity for functional safety
- Identify **position** of government/rule makers

- **Suggest directions** for a research project to close knowledge gaps for ensuring functional safety – considering the impact of cybersecurity threats.
- **Focus: Safety part** of ICS systems in the **Oil and gas** industry

Some results: Regulatory perspective

- Petroleum Safety Authority has carried out a mapping of **“Trends, knowledge, and proposals for new measures**” in relation to digitalization (report by IRIS).

- Cybersecurity addressed as part of this mapping:
  - **Cybersecurity** seems to be the most important contributor to the added risk from digitalization
  - **Need to balance** the ability to allow information sharing between different actors with the capability to manage cybersecurity
  - “**Everybody” have a role** in ensuring cybersecurity. More competence in ICT security is needed for most disciplines, also the traditional engineering disciplines like process, mechanical engineering,….

- A need for regulator body to consider how security risks can be reflected in targets, for monitoring,…

Some results: Standards' perspective

Functional safety

Cybersecurity

IEC 61508	IEC 61511	IEC 62443 series
• Focus is on safety part of ICS system • Function oriented • Life cycle oriented • Cybersecurity seems to be treated separately from functional safety		• Focus on control and safety system as a whole • Not relating any concepts or methods to functional safety • Not so well aligned with functional safety lifecycle phases • Few references to IEC 61508 (mostly on terminology) • Topology/system oriented
• Only mentioned in relation to hazards and risk analysis • Even considered as potentially *not* needed… • Ongoing discussions in the committee about the way forward	• Recognizes that security threats *shall* be identified • Recognizing (by more requirements addressing needs to consider security threats) for more phases	
Reference to IEC 62443	Reference to IEC 62443, ISA TR84.00.09, ISO/IEC 27001	*Almost no references to IEC 61508*

Some results: Suggestions of industry practiss

- **SaSe method** on *remote access* to SIS (safety part of ICS)

  Developed as part of research project with PDS forum participants (www.sintef.no/pds) (**2007**)

- **NOG 104:** Security requirements for ICS systems (**2016 -2nd ed.**)

  Developed by the Norwegian Oil and Gas Association

- **DNV-GL RP G108:** On the application of IEC 62443 for O&G sector

  Developed as part of a Joint industry research project. (**2017**)

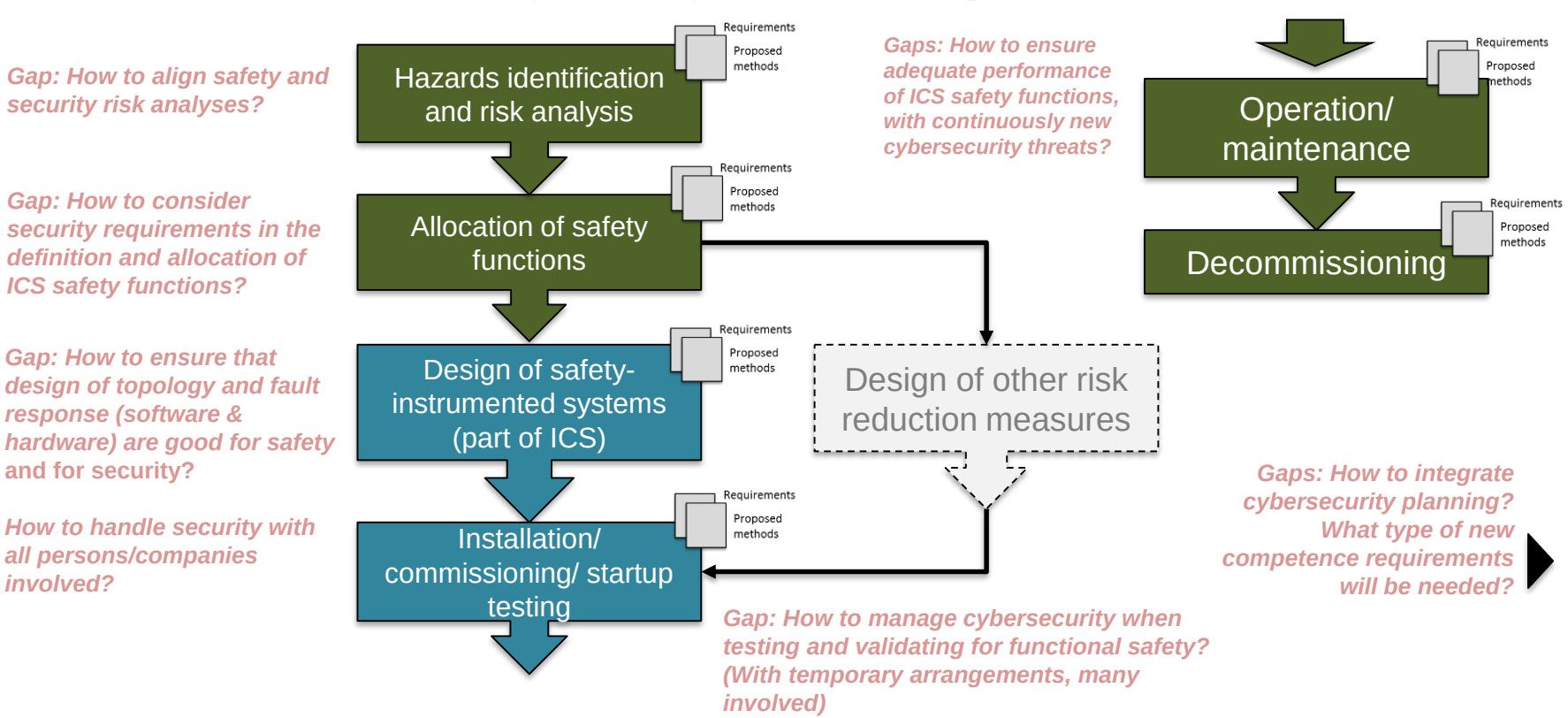
Some results: Research status

- Detailed and *extensive* literature review by the ITEA **MerGE project.** 2012-2016. ICS systems one of the use cases.

- Overall – **many** initiatives and proposals on safety and security co-engineering:
  - Graphical vs non-graphical
  - **Unified vs separation**
  - **Whole lifecycle or just parts**
  - **Qualitative vs quantitative**

- Some issues pointed at:
  - What should be the **desired coupling level** (low for safety vs high for security)
  - **Unified** approach possible in practice? **Separation** may result in conflicting goals
  - Possible to **learn** from “both sides”: Improve methods by learning from the other?
  - **Probabilistic** approaches possible or suitable for cybersecurity?

Our position: Cybersecurity needs to be addressed in the functional safety lifecycle. The question is how?



Suggested direction of new research project

Focus suggested on:

- How to **formulate requirements** for functional safety while ensuring cybersecurity. Development of suitable methods
- How to **follow-up/monitor** the performance of requirements. Management of change.
- How to **express** requirements to in a way that is comprehensible for people involved in all phases of SIS lifecycle

NTNU has initiated a new PhD project starting September 1st .

Collaboration with:

- IFE Cybersecurity Centre
- BRU21 project www.ntnu.edu/bru21

Two application areas:

- NPP
- Oil & Gas

Questions?

Mary Ann Lundteigen
Professor

Department of Mechanical and Industrial Engineering*
(*Department of Engineering Cybernetics from 1.6.2019)
Norwegian University of Science and Technology (NTNU)
7491 Trondheim, Norway
Tel: +47 930 59 365
mailto:mary.a.lundteigen@ntnu.no
http://www.ntnu.edu/employees/mary.a.lundteigen

Bjørn Axel Gran

Department Head

Risk, Safety and Security

Professor II, Department of Mechanical and Industrial Engineering, NTNU

+47 909 55 295
bjorn.axel.gran@ife.no

Clarification of terms used

ICS system: Industrial control and safety systems

- Field instruments including communication
- Logic controllers
- Networks
- HMI and connection to remote locations/outer world

Safety-instrumented systems (SIS):

- Understood as the parts of the ICS dedicated to safety.

Safety-instrumented function (SIF):

- Carried out by a SIS.

Cyber-physical system:

- Integrations of computation, networking, and physical processes.
- Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa (source: https://ptolemy.berkeley.edu/projects/cps/)

Functional safety:

- Safety achieved by the use of SIS, in combination with other risk reducing measures (see IEC 61511)
- Freedom from unacceptable risk (see ISO/IEC Guide 51, “Physical” risks”)

Cybersecurity (ICT security):

- Measures taken to protect a computer or computer system against unauthorized access or attack (IEC 62443-3-2)
- Freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others (in the context of hostile forces) (wiki)