Risk based regulation and certification of autonomous transport systems

S.O. Johnsen, Å. Hoem, T. Stålhane /NTNU
G. Jenssen, T. Moen/ SINTEF

Purpose

Provide an overview of research in the field, discuss experiences of autonomous transport systems, and suggest a framework for risk based governance

AGENDA

- Introduction, scope, activities
- Main findings
- Conclusion, identified issues

Approach - autonomous transport systems in all modes

1) Review of experiences – incidents, recoveries and accidents

- Review of papers
- Gather user experiences
- Conduct expert workshops

2) Scope and regulatory framework

- Broad approach – whole eco-system
- Specific Case: Regulation of autonomous road transport in Norway

3) Risk reduction actions

- Case driven suggestions

Sea Air Rail/Metro Road

Autonomy and Levels of automation

Automated: Deterministic; does exactly what it is programmed to do

Autonomy: A non-deterministic system; freedom to make choices

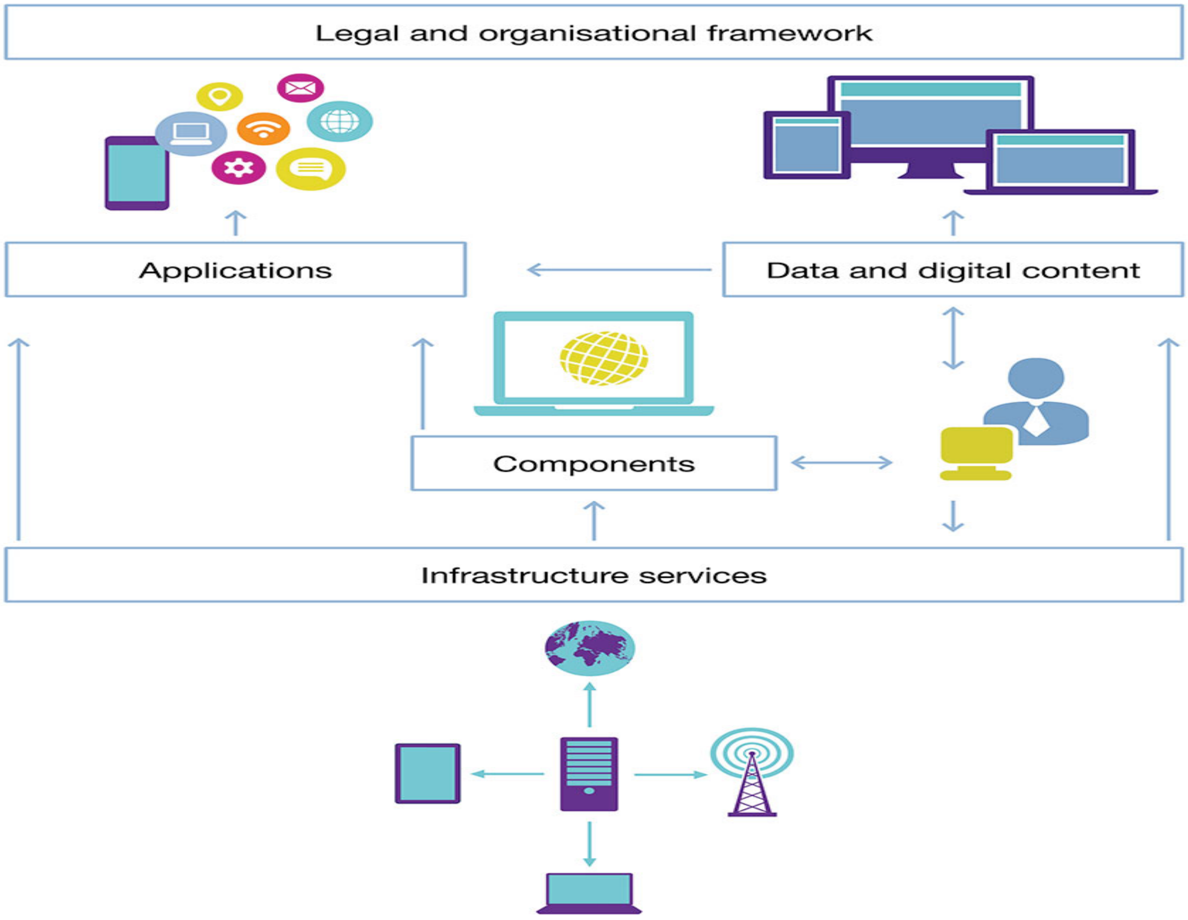
Levels of automation - Society of Automotive Engineers (SAE):

0-No automation;

1- Driver assistance; 2-Partial automation; 3-Conditional automation;

4-High automation; 5-Full automation

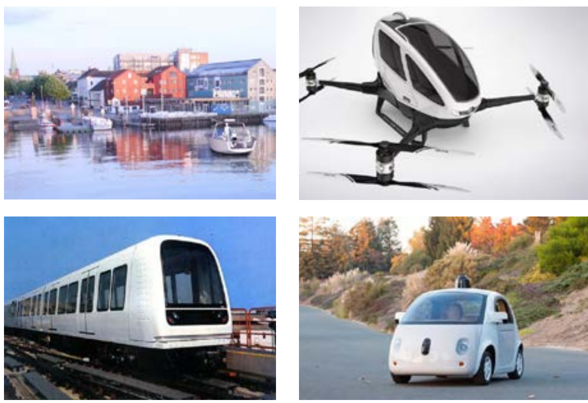
Using concept: ’Software ecosystems' a metaphor inspired by natural ecosystems to describe a distributed, adaptive, and open socio-technical system



Scope of autonomous transport system

System (LoA/Internal control)

External control



Interaction/ Communication with others (actors/ systems)

Literature review - key findings

- **Missing systematic data reporting of incidents and accidents**
  - Different taxonomies, systematic data is missing (ex: autonomous rail)

- **Key (security) vulnerabilities exists in autonomous cars**
  - Easy to attack, can control steering, brakes. Can erase evidence
  - Policy of responsible disclosure of vulnerabilities is needed
  - Need for CERTS – Computer emergency response teams that can handle vulnerabilities in transport infrastructure

- **Framework conditions such as regulation must improve**
  - Automation in control - i.e. software is in control/responsible, vendors liability not clear (Volvo, Mercedes Benz.. accept responsibility)
  - Operator (OEM) must have responsibility of totality ("påse ansvar")
  - Security of critical software must improve, need for regulation and incentives, minimum security standards, IEC61508; IEC62443; IACS Cybersecurity Certification Framework

Manned and Unmanned Aircraft Systems (UAS)

Manned

- Ultra-safe transportation – IATA no fatal accidents in 2012, 2017
- Increasingly automated, but “Human In the Loop” challenges
- Human Factors in design and analysis (Airbus hiring HF)
- Focus on accident investigation and improvements – (MTO accident investigation – HFACS)- need broader accident data

Unmanned Aircraft Systems (UAS)

- DoD UAS mishap rates: ca. 50-100 mishaps occur every 100,000 flight hours vs DoD human-operated aircraft one mishap per 100,000 flight hours
- Issue: Poor Human factors engineering continue to proliferate and cause UAS mishaps – need for improved design guidelines

Rail/metro automation from 1980 – no accidents
Isolated and Task oriented automation

Grade of Automation	Type of train operation	Setting train in motion	Stopping train	Door closure	Operation in event of Disruption
GoA 1	ATP with driver	Driver	Driver	Driver	Driver
GoA 2	ATP and ATO with driver	Automatic	Automatic	Driver	Driver
GoA 3	Driverless	Automatic	Automatic	Train attendant	Train attendant
GoA 4	UTO	Automatic	Automatic	Automatic	Automatic

ATP - Automatic Train Protection

ATO - Automatic Train Operation

Automation in (Road) transportation

Hospital: Automated Guided Vehicles (10 years experience)

- Low energy – few incidents – but need central control facility
- Type of collisions/ learning – observe hindrances?
- Communication to humans; doors; elevators is challenging

Road transport (Google Cars and automated buses)

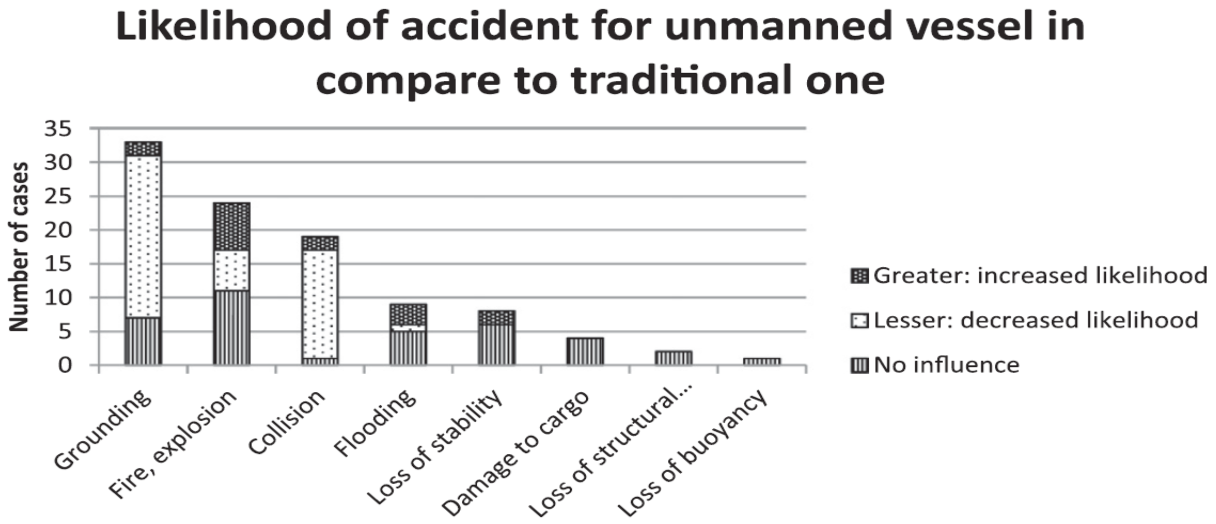
- Few incidents (3 in 2009- 2015) while driving 2,208,199 km (accident rate 1,36 incidents pr. million km; 1/3 of human-driven vehicles under similar conditions) – "Risk based" training needed
- Risks: Other accidents such as rear end collisions, nicknamed: "rage against the machine", expect 50% reduction of accidents
- Takeover time for human driver varies from 2 to 26 seconds (i.e. design challenge)
- Buses – less experiences but few accidents in operations

Sea, few experiences - pilot projects

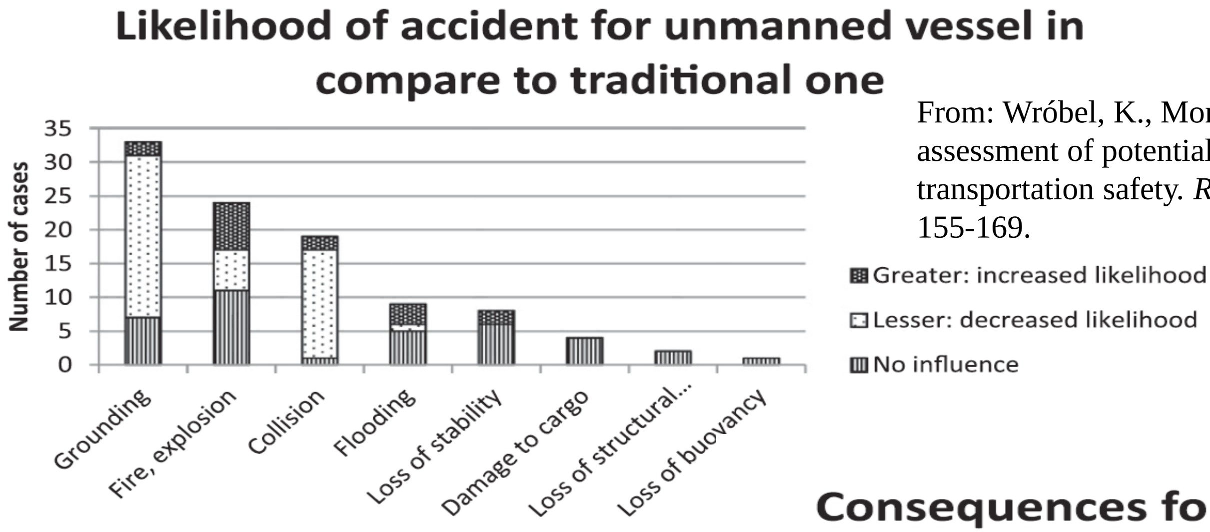
At present three test areas for autonomous shipping in Norway

- Yara Birkeland from 2020: 75 meters; 150- containers (removing ~ 40.000 trailers/ year) - Phased implementation LOA from low to high
- Pilots: “Plaske”/AutoFerry/MilliAmper - Unmanned ferry in Trondheim ; safety&security analysis performed using STAMP
- Experiences from “self- service ferries”: accidents and fatalities due to overload and capsize; however expects safer shipping with automation

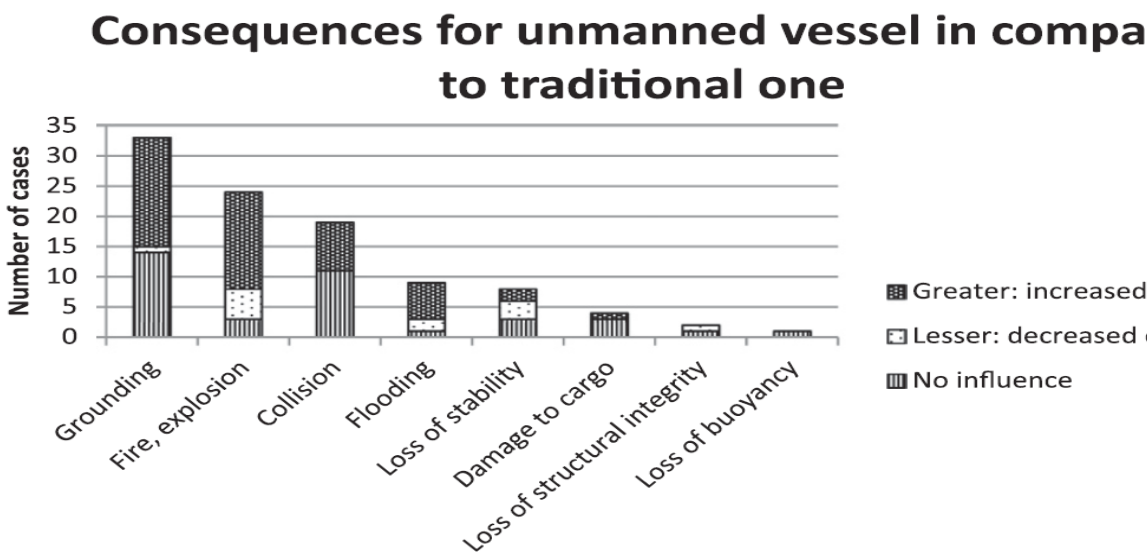
Unmanned vessels and transportation risks



Unmanned vessels and transportation risks



From: Wróbel, K., Montewka, J., & Kujala, P. (2017). Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. *Reliability Engineering & System Safety*, *165*, 155-169.



Summary of Risk and mitigation

Different levels of maturity – lessons to be learned across industry

(Manned aviation with selected automation – ultra safe)

- **Reporting and understanding of incidents (accidents and success stories) of automated systems should be improved – impacting regulation**
  - New risks (i.e. “Rage against the machine”); Models (HFACS); Richer set of data; Need Taxonomies; Organizational issues (CERTS); and improved accident investigations; Defined Hazards (DFU) – such as: sensor failures/poor quality of sensor data

- **Functional based regulation in the age of eco-systems - impacting design**
  - Require improved safety by automation; Road transport (50% reduction of accidents?)
  - Responsibility (in Automated cars – the system); In general “Påse ansvar” one resp.
  - Complex interaction needs safety case testing/certification including security focus

- **Requirements and design of interaction between humans and automation**
  - Automation fails- Training & Design of take-over (i.e. Human in the loop; 2-26 second)
  - Safety Critical Task analysis; New models needed to explore risks; such as STAMP-Engineered for humans
  - Experiences cross areas - Such as Design guidelines from the area of UAS

Further research needs

- **Establish taxonomies and gather systematic operational data** from operations of autonomous systems based on ecosystem approach (ex: Rail, autonomous robot trolleys, autonomous ships, ..)

- **Improve methods to analyse risks/hazards** of autonomous systems/ and AI systems based on ecosystem approach

- **Improve design methods and training** to support "human in the loop" i.e. interventions and interactions to support sensemaking

- **How to regulate** when automation replaces powerful stakeholders i.e. pilots or three-party collaboration now (robots n the future) ?
  - How to establish proactive and agile regulation (i.e. best of breed) in an ecosystem cross countries

Questions

Provide an overview of research in the field, explore experiences of autonomous transport systems, and suggest a framework for risk based governance

Sea Air Rail/Metro Road