Safety for Autonomous Ships

Lessons learned from other domains

Autonomous Ship Technology, Amsterdam, June 25-27, 2019

Stig Petersen, SINTEF Digital
stig.petersen@sintef.no

Safety can be defined as freedom from unacceptable risk of harm to humans, property or the environment.

Safety can be achieved by using barriers:

Physical barriers, work processes, training and education, control systems, emergency response, …

Autonomy is traditionally defined related to the technical capabilities of a system.

SAE[1] Levels of Autonomy

Level 0 No Automation	**Level 1** Driver Assistance	**Level 2** Partial Automation	**Level 3** Conditional Automation	**Level 4** High Automation	**Level 5** Full Automation
	Some driver assist features may be present.	The vehicle has combined automated functions.	The driver is necessary but does not need to monitor the environment.	The vehicle performs all driving functions under certain conditions.	The vehicle can perform all driving functions under all conditions.
The driver performs all tasks.	The vehicle is controlled by the driver.	The driver must be engaged and monitor the environment at all times.	The driver must be ready to take control at all times with notice.	The driver may have the option to control the vehicle.	The driver may have the option to control the vehicle.

[1] Society of Automotive Engineers

SINTEF

Autonomous cars are currently in testing on public roads.

On 18 March 2018, a pedestrian was killed by an Uber car testing self-driving technology in Tempe, Arizona.

The car made no attempt to brake prior to the accident.

The accident report concluded that emergency braking was not enabled while the vehicle was under computer control.

The driver was relied on to take action, but the system was not designed to alert the driver when intervention was needed.

Uber avoided a potential lawsuit from the family of the deceased by settling shortly after the accident.

In March 2019, Yavapai county attorneys concluded that the Uber corporation is not criminally liable for the accident

The driver of the vehicle may still face criminal prosecution.

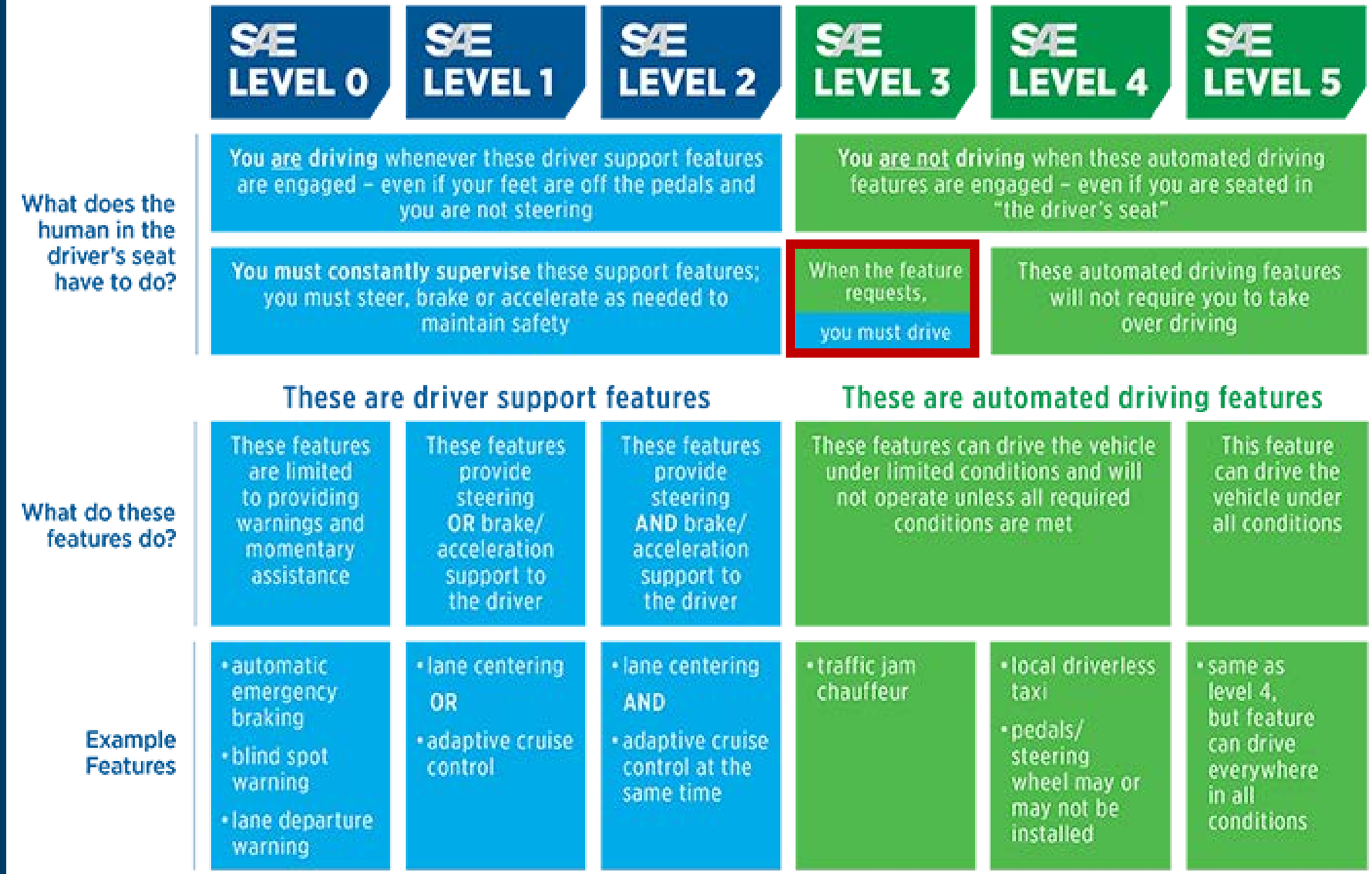
SAE[1] Levels of Autonomy

Level 0 No Automation	**Level 1** Driver Assistance	**Level 2** Partial Automation	**Level 3** Conditional Automation	**Level 4** High Automation	**Level 5** Full Automation
	Some driver assist features may be present.	The vehicle has combined automated functions.	The driver is necessary but does not need to monitor the environment.	The vehicle performs all driving functions under certain conditions.	The vehicle can perform all driving functions under all conditions.
The driver performs all tasks.	The vehicle is controlled by the driver.	The driver must be engaged and monitor the environment at all times.	The driver must be ready to take control at all times with notice.	The driver may have the option to control the vehicle.	The driver may have the option to control the vehicle.

[1] Society of Automotive Engineers

SINTEF

SAE J3016™ LEVELS OF DRIVING AUTOMATION



With the introduction automated and self-driving technologies, electronic systems are gradually replacing human operators.

Autonomy definition revisited:

A system is considered autonomous if it can legally accept accountability for an operation.

NFAS Levels of Autonomy

Level 1 Decision Support	**Level 2** Automatic	**Level 3** Constrained Autonomous	**Level 4** Fully Autonomous
	The operation follows a pre-programmed sequence.	The ship can operate fully automatic in most situations.	The ship handles all situations by itself.
The crew is in command of ship operation and supervises all operations.	Humans must intervene from bridge or shore control center (SCC) upon request.	SCC or bridge personnel must take immediate control when requested by the system.	SCC or bridge personnel is not required.

SINTEF

Summary

Defining autonomy as a technical capability introduces uncertainties regarding division of responsibilities between humans and machines.

A general definition of autonomy should be based on legal accountability – not technical function.

Unresolved challenges

The practical and formal implications of transferring accountability between humans and computer systems.

The shape and form of the safety regimes necessary for handling approval and certification of autonomous systems.

The spilt of accountability between system designers, operators, authorities and certification agencies.

Technology for a better society