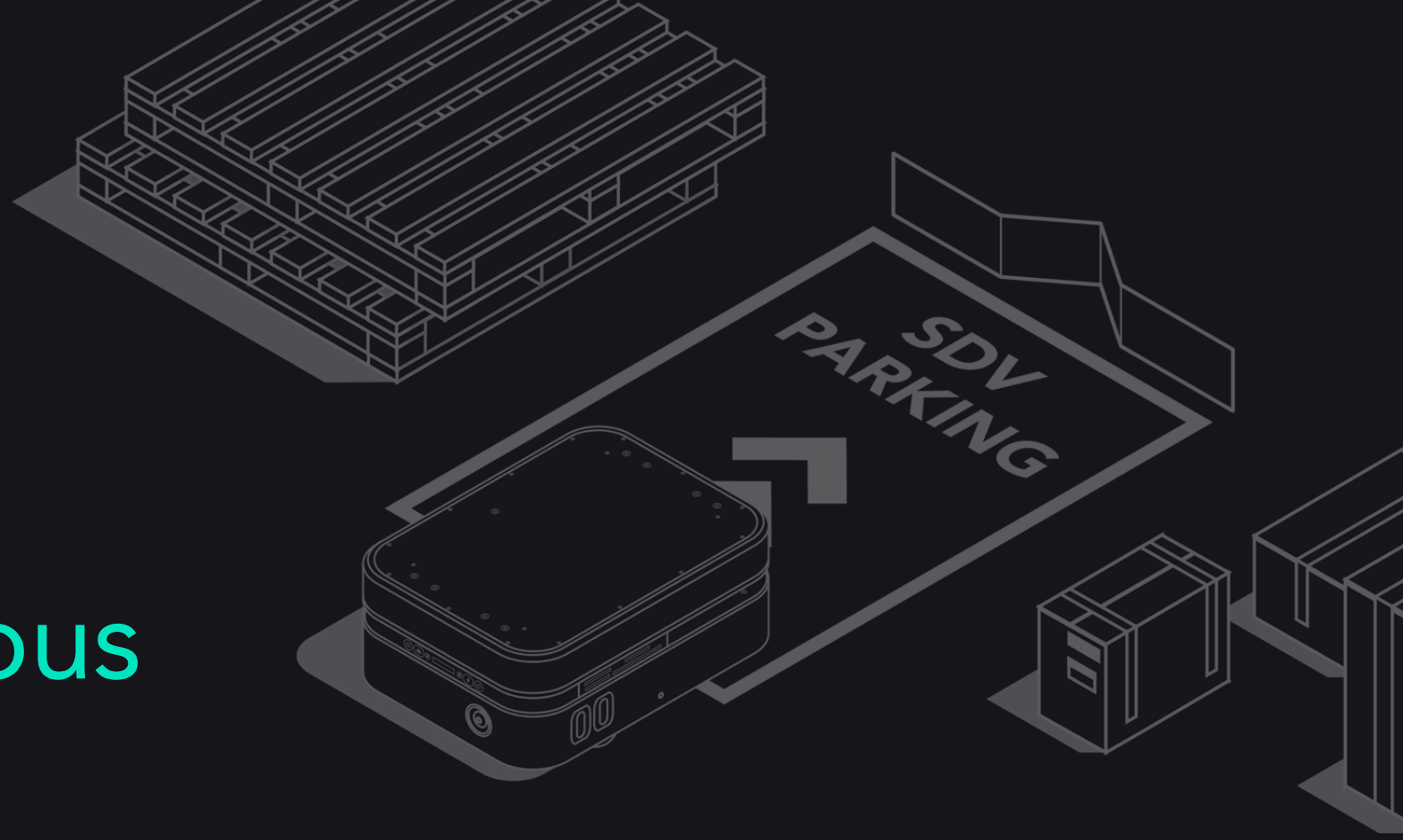
09.11.19 - ROSCon JP

Eight Steps to Safe Autonomous Robots



Ryan Gariepy, CTO Clearpath Robotics

OTTO MOTORS

My History

My History

2005 → 2007 → 2008 → 2009 →

Honda of Canada
(Intern)

Aeryon Labs
(Intern)

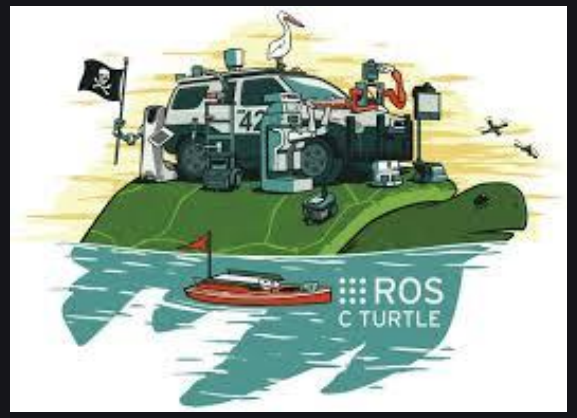
Kiva Systems
(Intern)

Clearpath Robotics
(Founder)

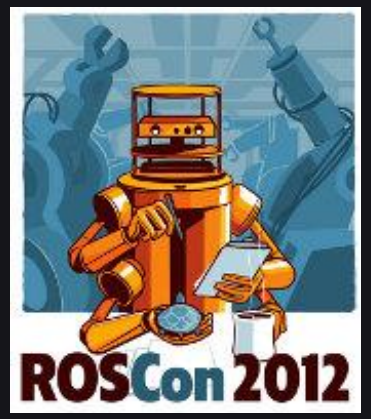
OTTO
MOTORS

My History (Continued)

2010 → 2012 → 2014 → 2019



First for-profit company to support ROS



First ROSCon, OSRF founded

OTTO Motors division started

OTTO International Expansion

OTTO
MOTORS

8 Steps to Safer Autonomous Vehicles

8 Steps

1. What Is Safety?
2. What Is The Environment?
3. Know The Rules & Regulations
4. Know Your Risks
5. Use Good Mitigations
6. Safety By Design
7. Safety Architecture & Use of Predictable Code
8. Use Statistics

OTTO MOTORS

What is Safety?

Safety does *not* mean ‘perfectly polite’ vehicles.

Zero risk is impossible.

What is Safety?

Safety is about keeping people free from harm.

FIRST-ORDER RISKS →

What is Safety?

Safety is about keeping people free from harm.

SECOND-ORDER RISKS →

What is Safety?

As safety increases, speeds decrease AND/OR space required increases

Robots must be safer than people performing the same task

OTTO MOTORS

No More Machine Operators

Machines have *operators*

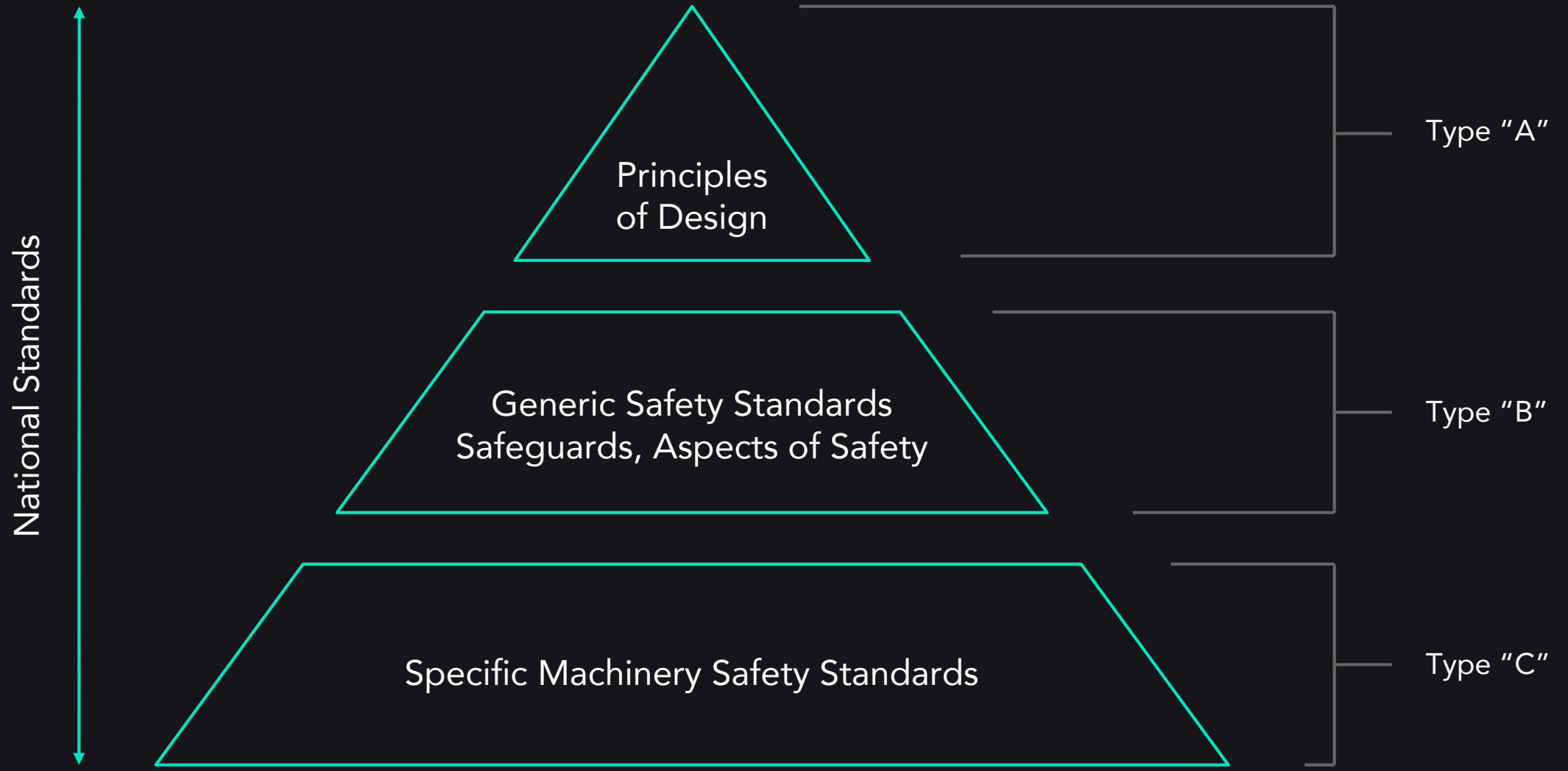
Robots have
bystanders

OTTO
MOTORS

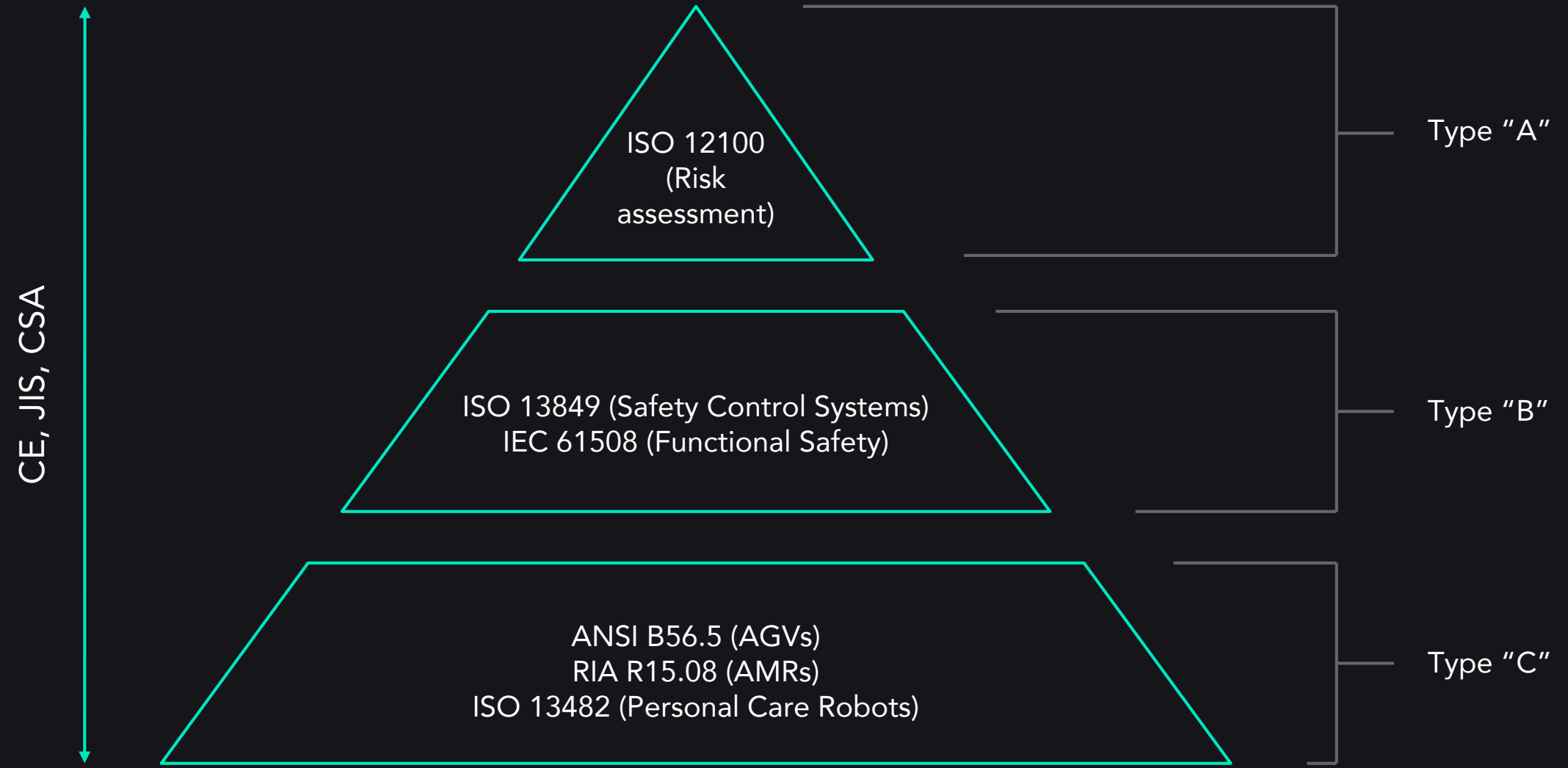
Environment/ Bystanders

1. Who are your bystanders?
2. How big are they?
3. What clothing are they wearing?
4. How foolish are they?

Standards


National Standards
Principles of Design
Generic Safety Standards Safeguards, Aspects of Safety
Specific Machinery Safety Standards
Type “A”
Type “B”
Type “C”

Standards


CE, JIS, CSA
ISO 12100
(Risk
assessment)
Type “A”
ISO 13849 (Safety Control Systems)
IEC 61508 (Functional Safety)
Type “B”
ANSI B56.5 (AGVs)
RIA R15.08 (AMRs)
ISO 13482 (Personal Care Robots)
Type “C”

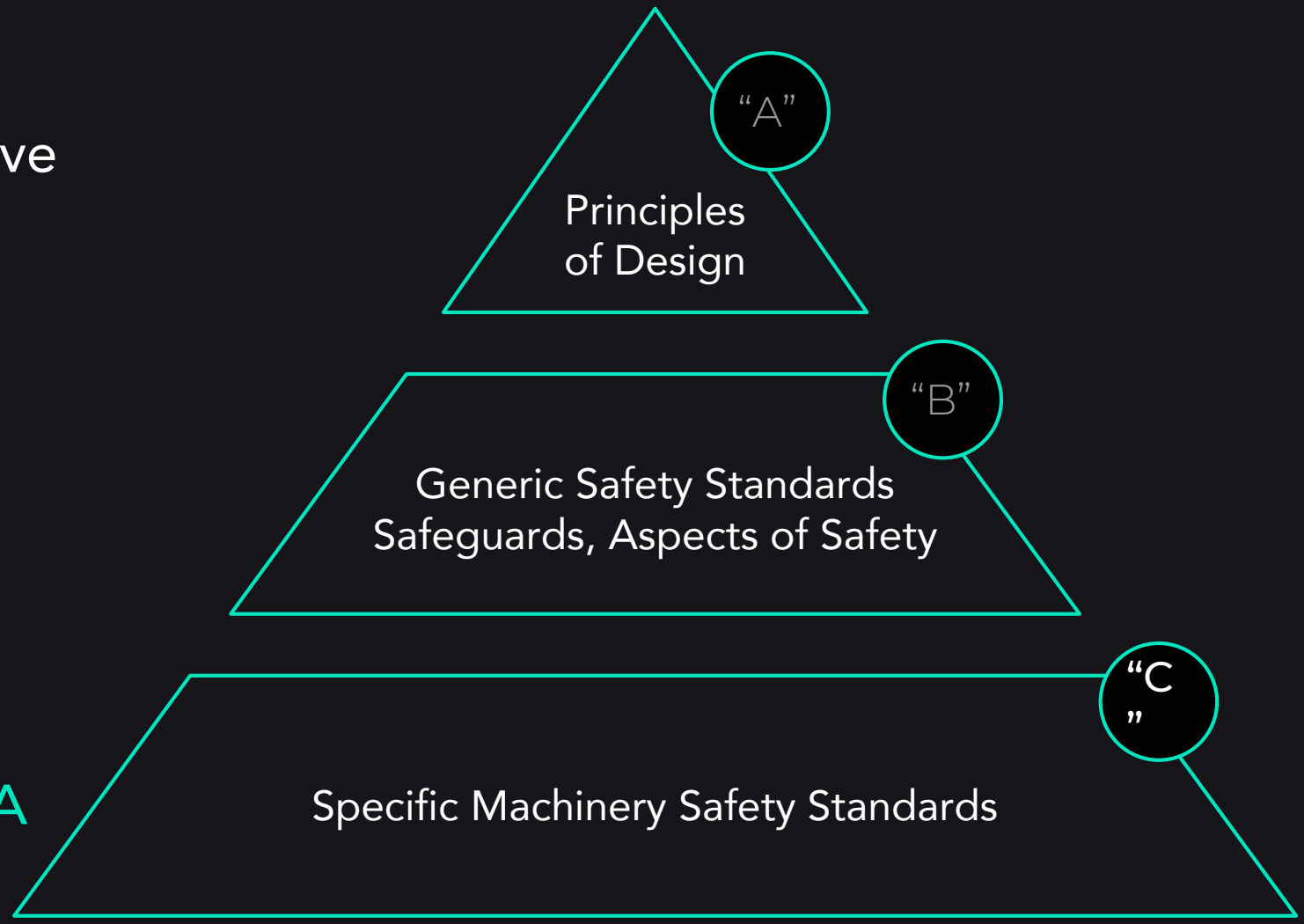
New Industry - Type C Standards Still In Progress!

Type C standards should have specific advice on:

- Moving object detection
- 3D object detection
- Vehicle dynamic testing and restrictions
- Proper use of machine learning

But they usually don't!

Must use Type B or Type A



Risk Assessment Formats

Life Cycle Phases & Tasks as per EN ISO 12100:2010 Table B.3	Hazards Details as per EN ISO 12100:2010 Tables B.1 through B.4		Probability	Exposure	Severity	Avoidance	Evaluation	Evaluation Category	Planned Risk Control Measures (Design, Safeguarding, Complementary proptective measure, Awareness means, Information for use)	EN ISO 13849 for SRP/CS Only - Risk Reduction Required to be Contributed by Safety Function						Implemented Risk Control Measures (Design, Safeguarding, Complementary,	Probability	Exposure	Severity	Avoidance	Evaluation	Evaluation Category
										SF ID	Risk Parameters prior to			Per for ma	Per for ma						
											S	F	P								
			POHE	DEHS	LDHS	PHLA	R_v										POHE'	DEHS'	LDHS'	PHLA'	R_v'	
Transportation: Unloading; Lifting; Loading; Packing; Unpacking Assembly, Installation and Commisioning: Running the machine without load; Testing; Demonstration Setting, teaching, programming & process change-over: Mapping. Operation: Control & inspection; driving the machine; Manual loading/unloading of material; Minor interventions during operation; Operating manual controls; Restarting the machine after stopping/interruption; Charging; Docking or undocking; Lifting or lowering payload; Pallet engagement	Description: Sharp Edges Hazard: Sharp edges Hazardous Situation: Person makes contact with static robot Hazard Zone: Reach distance of the robot Hazardous Event: Contact between robot and person	Start	5	5	2	2	100	High	D—Round corners and smooth surfaces to preclude puncturing and stabbing.							D—Round corners and smooth surfaces to preclude puncturing and stabbing.	1	1	1	1	1	Negligible
Assembly, Installation and Commisioning: - Running the machine without load; Testing; Demonstration Setting, teaching, programming & process change-over: Mapping. Operation: Control & inspection; driving the machine; Manual loading/unloading of material; Minor interventions during operation; Operating manual controls; Restarting the machine after stopping/interruption; Charging; Docking or undocking; Lifting or lowering payload; Pallet engagement	Description: Collision with lowered robot tines in free space, speeds up to 1.0 m/s Hazard: Acceleration, deceleration., Kinetic Energy, Machinery Mobility Hazardous Situation: Person near robot/payload gets struck Hazard Zone: Envelope that leading faces (not flanks) of robot/payload could pass through within 1 second + reach distance. Hazardous Event: Contact between robot/payload and person	Start from item #1	15	5	10	8	6000	Extreme	D— Onboard obstacle avoidance navigation system		2	2	2	PLe	PLa	D - PLa compliant obstacle avoidance system;	5	2.5	10	8	1000	Extreme
		Continue from above	5	2.5	10	8	1000	Extreme	S—Separation control by means of ISO 13849-compliant control system triggering IEC 60204-1 Category 0 stop when an object is detected in AOPD protective field. AOPD protective field		2	2	1	PLd	PLd	S -LIDAR protective stop safety function with field set switching via safety	1	0.5	10	2	10	Low
		Cont. from above	1	0.5	10	2	10	Low	C—Emergency stop function compliant with ISO EN 13850 triggering IEC 60204-1 Category 0 stop. Actuator located at side of vehicle					n/a		E-stop pushbuttons	1	0.5	10	1	5	Low
		Continue from above	1	0.5	10	1	5	Low	A—High-visibility lighting providing intuitive indication of planned vehicle motion ("forward" direction of travel, directional signaling before turns, brake lights).					n/a		Awareness Means; Information for use	0.033	0.5	10	1	0.165	Negligible

ISO 12100 Format

OTTO MOTORS

Risk Assessment Formats

Life Cycle Phases & Tasks as per EN ISO 12100:2010 Table B.3	Hazards Details as per EN ISO 12100:2010 Tables B.1 through B.4		Probability	Exposure	Severity	Avoidance	Evaluation	Evaluation Category	Planned Risk Control Measures (Design, Safeguarding, Complementary proptective measure, Awareness means, Information for use)	EN ISO 13849 for SRP/CS Only - Risk Reduction Required to be Contributed by Safety Function						Implemented Risk Control Measures (Design, Safeguarding, Complementary,	Probability	Exposure	Severity	Avoidance	Evaluation	Evaluation Category
										SF ID	Risk Parameters prior to			Per for ma	Per for ma						
			POHE	DEHS	LDHS	PHLA	R_r				S	F	P	PL_r	PL_a		POHE'	DEHS'	LDHS'	PHLA'	R_r'	
Transportation: Unloading; Lifting; Loading; Packing; Unpacking Assembly, Installation and Commisioning: Running the machine without load; Testing; Demonstration Setting, teaching, programming & process change-over: Mapping. Operation: Control & inspection; driving the machine; Manual loading/unloading of material; Minor interventions during operation; Operating manual controls; Restarting the machine after stopping/interruption; Charging; Docking or undocking; Lifting or lowering payload; Pallet engagement	Description: Sharp Edges Hazard: Sharp edges Hazardous Situation: Person makes contact with static robot Hazard Zone: Reach distance of the robot Hazardous Event: Contact between robot and person	Start	5	5	3	3	100		D—Round corners and smooth surfaces to preclude puncturing and stabbing.							D—Round corners and smooth surfaces to preclude puncturing and stabbing.	1	1	1	1	1	Negligible
Assembly, Installation and Commisioning: - Running the machine without load; Testing; Demonstration Setting, teaching, programming & process change-over: Mapping. Operation: Control & inspection; driving the machine; Manual loading/unloading of material; Minor interventions during operation; Operating manual controls; Restarting the machine after stopping/interruption; Charging; Docking or undocking; Lifting or lowering payload; Pallet engagement	Description: Collision with lowered robot tines in free space, speeds up to 1.0 m/s Hazard: Acceleration, deceleration., Kinetic Energy, Machinery Mobility Hazardous Situation: Person near robot/payload gets struck Hazard Zone: Envelope that loading fr... (not flanks) of robot/payload could pass through within 1 second + reach distance. Hazardous Event: Contact between robot/payload and person	Start from Step #1	15	5	10	8	6000		D— Onboard obstacle avoidance navigation system		2	2	2	PLe	PLa	D - PLa compliant obstacle avoidance system;	5	2.5	10	8	1000	Extreme
		Continue from above	5	2.5	10	8	1000		D— Safeguarding control by means of ISO 13849-compliant control system triggering IEC 60204-1 Category 0 stop when an object is detected in AOPD protective field. AOPD protective field		2	2	1	PLd	PLd	S -LiDAR protective stop safety function	1	0.5	10	8	10	Low
		Continue from above	1	0.5	10	2	10		D— Emergency stop function compliant with ISO EN 13850 triggering IEC 60204-1 Category 0 stop. Actuator located at side of vehicle					n/a		E-stop pushbuttons	1	0.5	10	1	5	Low
		Continue from above	1	0.5	10	1	5		D— Visually lighting providing intuitive indication of planned vehicle motion ("forward" direction of travel, directional signaling before turns, brake lights).					n/a		Awareness Means; Information for use	0.033	0.5	10	1	0.165	Negligible

ISO 12100 Format

OTTO MOTORS

Types of Risk

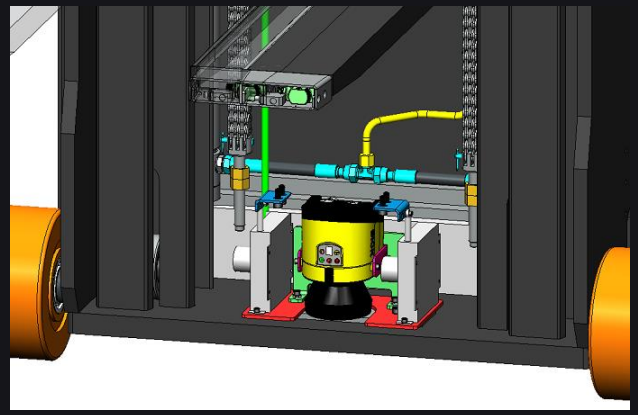
	Low Probability ↘	High Probability ↗
Low Impact	Result: Improvement opportunity, not safety issue Prioritized: Via kaizen initiatives after release	Result: Product quality issue, not safety issue Prioritized: Via customer feedback before release
High Impact	Result: Major safety risk, difficult to know Prioritized: Needs active investigation	Result: Major safety risk Prioritized: Via safety culture in development team

Types of Risk

	Low Probability ↘	High Probability ↗
Low Impact	Result: Improvement opportunity, not safety issue Prioritized: Via kaizen initiatives after release	Result: Product quality issue, not safety issue Prioritized: Via customer feedback before release
High Impact	Result: Major safety risk, difficult to know Prioritized: Needs active investigation	Result: Major safety risk Prioritized: Via safety culture in development team

Mitigations

Intrinsic Safety:
Best



Functional Safety:
Standard

Training & Awareness:
Sometimes OK

Protective Equipment
Undesired

OTTO
MOTORS

Intrinsic Safety

Remember the bystanders?

Intrinsic Safety

"Can the bystanders beat the robot in a fight?"

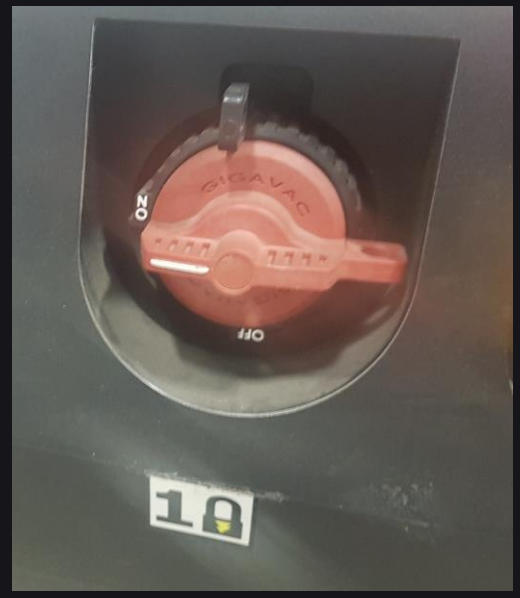
Speed <0.3 m/s or total mass <100 kg?

OTTO
MOTORS

Other Safety Basics

Safety Lasers

Emergency Stops

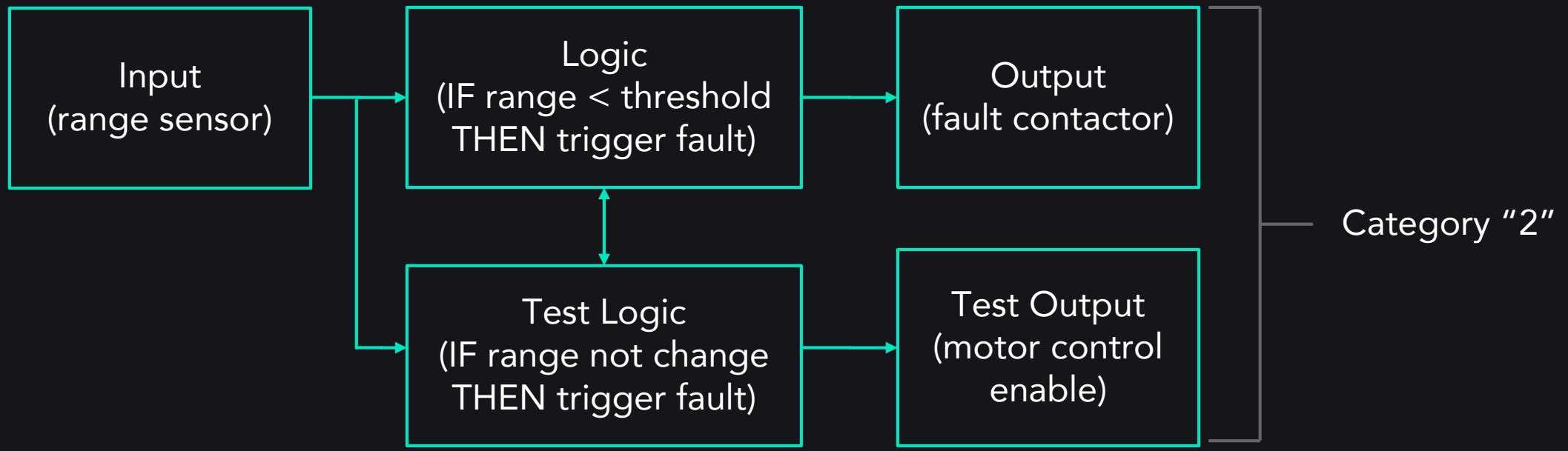


Lockouts

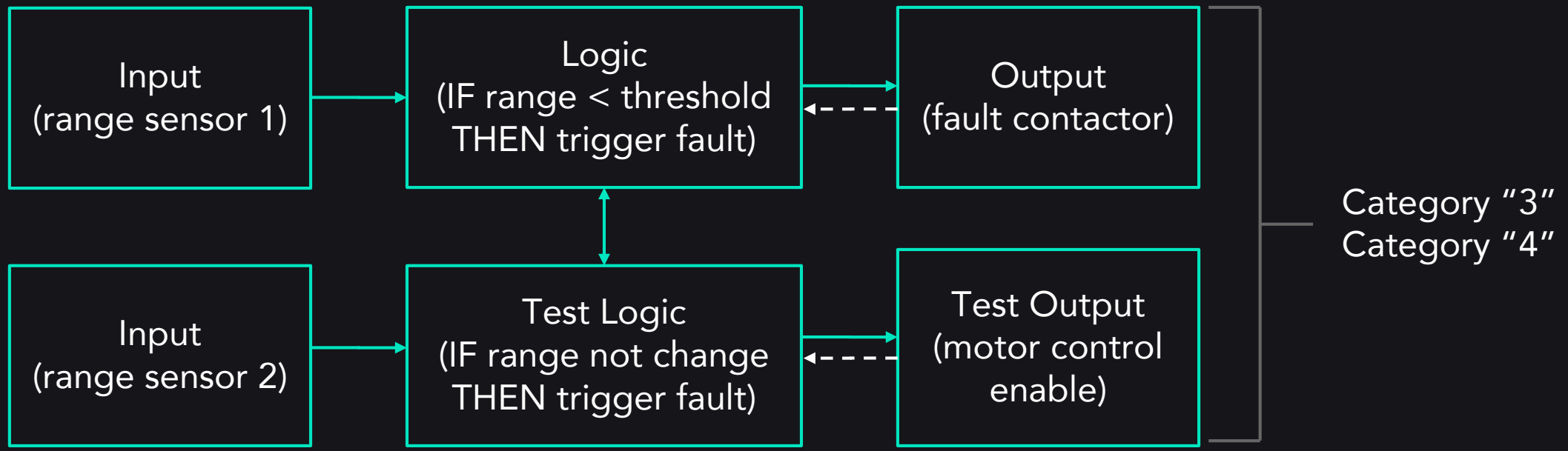
Wireless Emergency Stops

Architecture: ISO13849 Levels

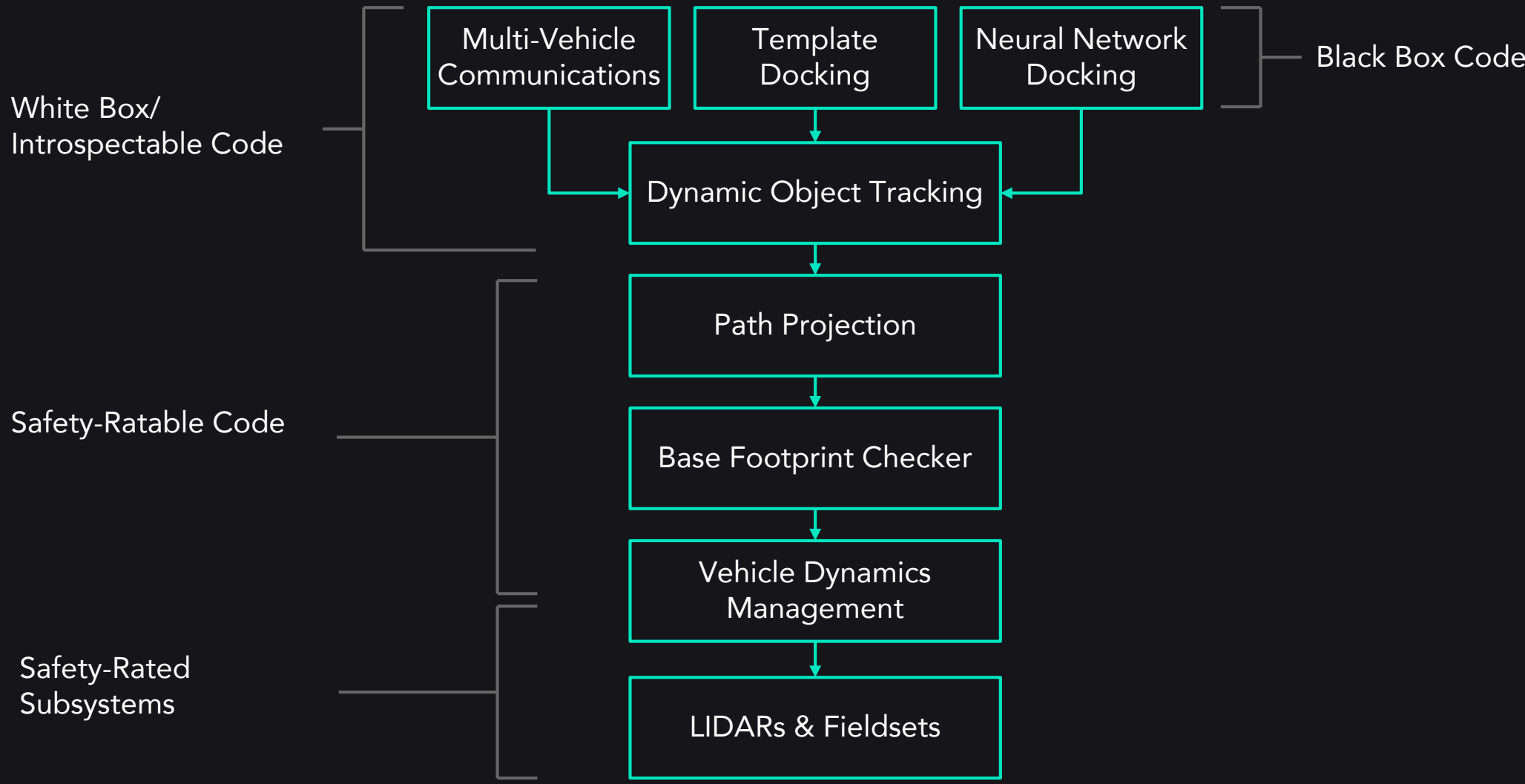
Architecture: ISO13849 Levels



Architecture: ISO13849 Levels



Architecture: Navigational Safety Layering



Statistics

MTTFd: Mean Time to Dangerous Failure.

MTTF, except only for failures which create hazards

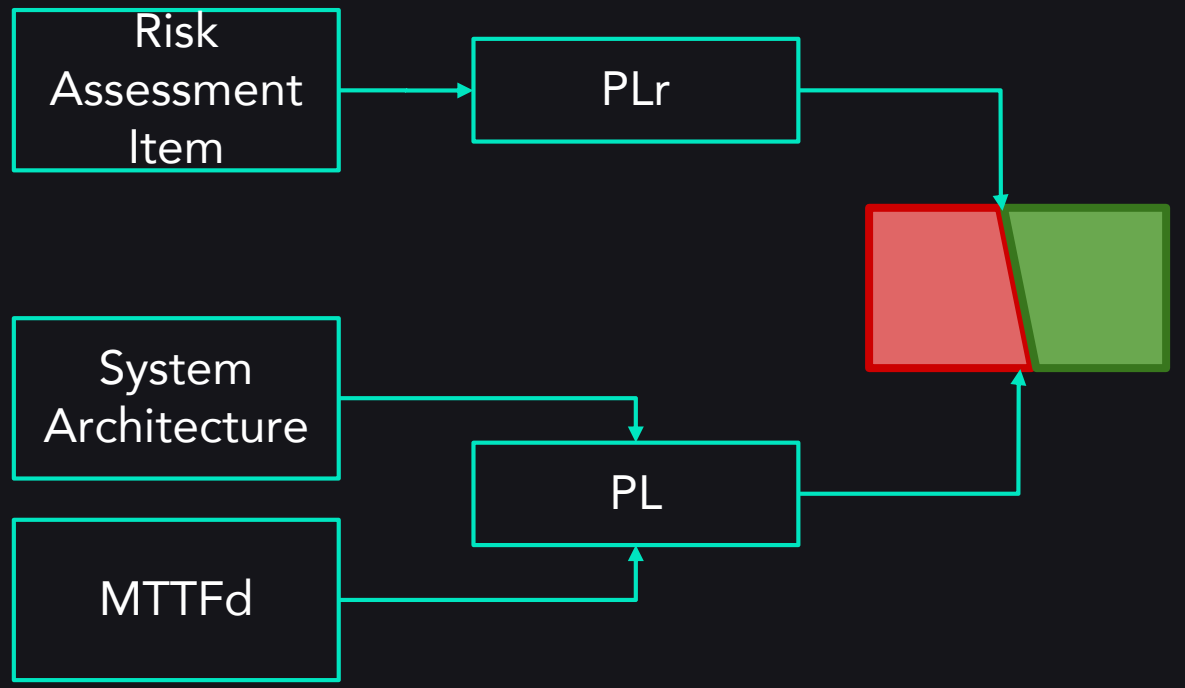
PL: Performance level of safety system/subsystem

PLr: Required performance level given risks

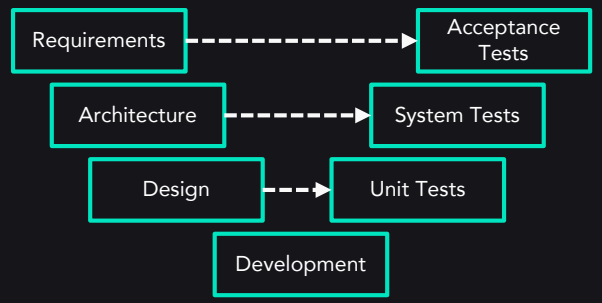
Table 1 – Relationship between PLs and SILs based on the average probability of dangerous failure per hour

Performance level (PL)	Average probability of a dangerous failure per hour (1/h)	Safety integrity level (SIL)
a	$\geq 10^{-5}$ to $< 10^{-4}$	No special safety requirements
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

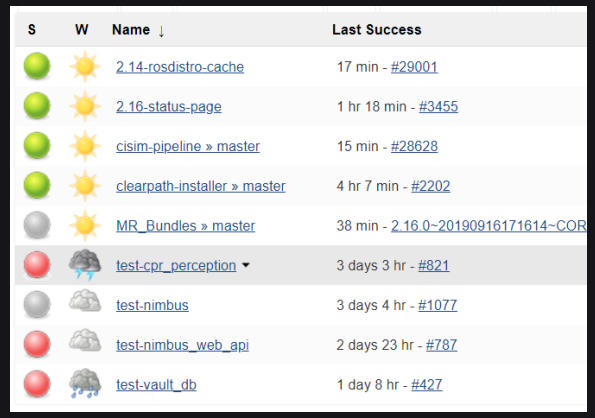
ISO 13849 IEC 62061



Software Testing

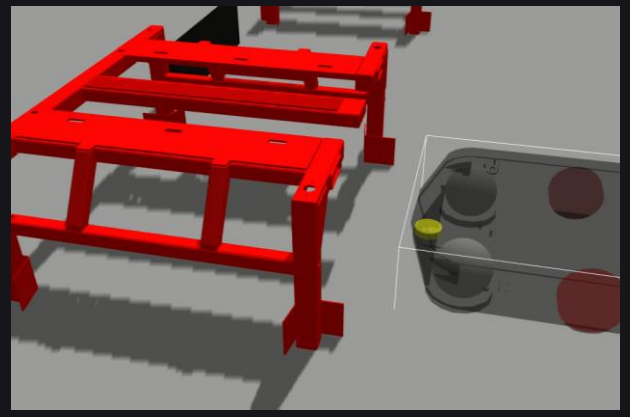


V-Model Development

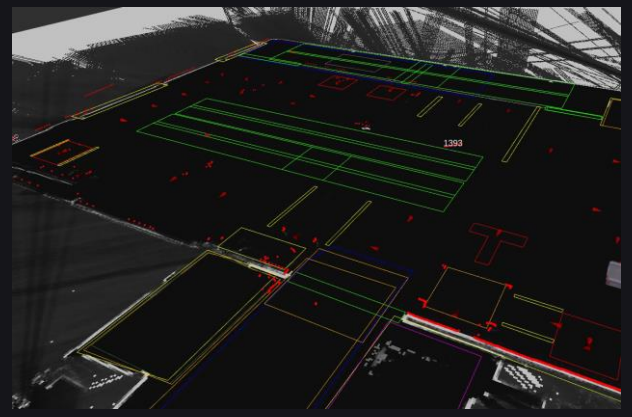


S	W	Name ↓	Last Success
		2.14-rosdistro-cache	17 min - #29001
		2.16-status-page	1 hr 18 min - #3455
		cisim-pipeline » master	15 min - #28628
		clearpath-installer » master	4 hr 7 min - #2202
		MR_Bundles » master	38 min - 2.16.0~20190916171614~COR
		test-cpr_perception	3 days 3 hr - #821
		test-nimbus	3 days 4 hr - #1077
		test-nimbus_web_api	2 days 23 hr - #787
		test-vault_db	1 day 8 hr - #427

Unit Testing



Simulations



Real World Testing

OTTO MOTORS

Conclusions

Conclusions

1. What Is Safety?	*More cautious than people, but not 'perfectly polite'*
2. What Is The Environment?	*How foolish are your bystanders?*
3. Know The Rules & Regulations	*You will probably need first principles*
4. Know Your Risks	*Look for low-likelihood/high-impact*
5. Use Good Mitigations	*Intrinsic safety best, functional safety OK*
6. Safety By Design	*Keep it slow and light, have stopping methods*
7. Safety Architecture	*Build for redundancy and determinism*
8. Use Statistics	*Don't trust your eyes, trust the statistics*

OTTO
MOTORS

Questions

Together, We Can Start a Self-Driving Revolution.

Join us on our mission to change the way materials move in factories worldwide.

Ryan Gariepy
CTO, Clearpath

ryan@clearpath.ai