Safety-related Functions and Interfaces - Introduction

UR robots are equipped with a range of built-in safety-related functions as well as safety-related electrical interfaces to connect to other machines and additional protective devices. Each safety function and interface is monitored according to EN ISO13849-1:2008

The robot has a number of safety-related functions that can be used to limit the movement of its joints and of the robot Tool Center Point (TCP). The TCP is the center point of the output flange with the addition of the TCP offset.

The limiting safety-related functions are:

Limiting Safety Function	Description
Joint position	Min. and max. angular joint position
Joint speed	Max. angular joint speed
TCP position	Planes in Cartesian space limiting robot TCP position
TCP speed	Max. speed of the robot TCP
TCP force	Max. pushing force of the robot TCP
Momentum	Max. momentum of the robot arm
Power	Max. applied robot arm power

Stopping times of the Safety System

The stopping time of the safety system is the time from a fault or violation of a safety-related function occurs to the robot is brought to a complete stop and the mechanical brakes are engaged.

The maximum stopping times in the table must be considered if the safety of the application relies upon the stopping time of the robot. E.g. if a fault in the robot results in a stop of a complete factory line, where certain actions must take place immediately after the stop, the maximum stopping times must be considered.

The measurements are conducted with the following configuration of the robot:

- Extension: 100% (the robot arm is fully extended horizontally).
- Speed: The TCP speed limit of the safety system is set to the described limit.

- Payload: maximum payload handled by the robot attached to the TCP (10 kg).

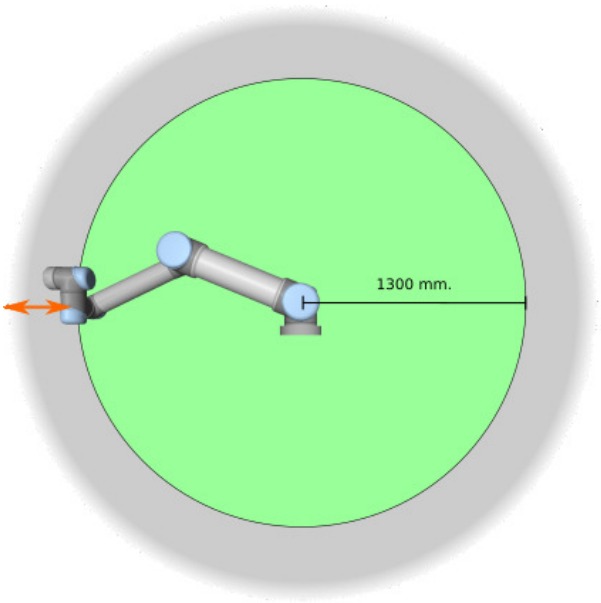
The worst case stopping time for Stop Category 0 in case of a violation of the safety limits or interfaces can be seen in the following table.

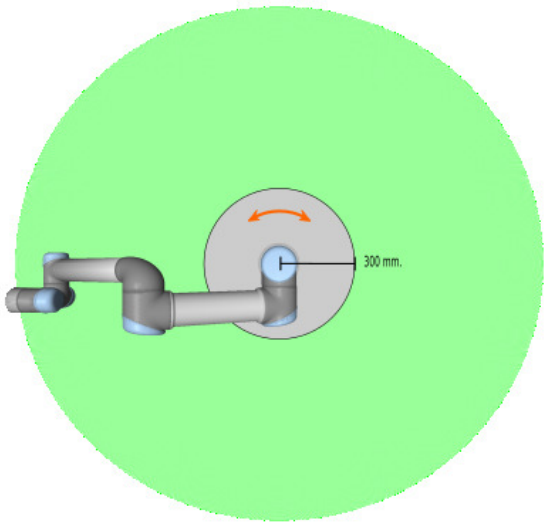
TCP Speed Limit	Maximum Stopping Time
1.0 m/s	450 ms
1.5 m/s	500 ms
2.0 m/s	550 ms
1.5 m/s	600 ms
3.0 m/s	650 ms

Limiting Safety - Related Functions

Advanced path control software decreases speed or issues a program execution stop if the robot arm approaches a safety-related limit. Violations of limits will hence only occur in exceptional cases. Nevertheless, if a limit is violated, the safety system issues a Stop Category 0.

The system is considered de-energized when the 48 V bus voltage reaches an electrical potential below 7.3 V. The de-energizing time is the time from a detection of an event until the system has been de-energized.





Safety Modes - Normal and Reduced mode

The safety system has two configurable safety modes: Normal and Reduced. Safety limits can be configured for each of these two modes. Reduced mode is active when the robot TCP is positioned beyond a Trigger Reduced mode plane or when triggered by a safety input. Reduced mode can be triggered either by using a plane or by using an input.

Using a plane to trigger Reduced mode: When the robot moves from the Reduced mode side of the trigger plane, back to the Normal mode side, there is a 20mm area around the trigger plane where both Normal and Reduced mode limits are allowed. It prevents the safety mode from flickering if the robot is right at the limit.

Using an input to trigger Reduced mode: When an input is used (to either start or stop Reduced mode), up to 500ms can elapse before the new mode limit values are applied. This could happen either when changing Reduced mode to Normal mode OR changing Normal mode to Reduced mode. It allows the robot to adapt e.g. the speed to the new safety limits.

Safety Modes - Recovery Mode

When a safety limit is violated, the safety system must be restarted. If the system is outside a safety limit at start-up (e.g. outside a joint position limit), the special Recovery mode is entered.

In Recovery mode it is not possible to run programs for the robot, but the robot arm can be manually moved back within limits either by using Freedrive mode or by using the Move tab in PolyScope. The safety limits of Recovery mode are:

Limiting Safety Function	Limit
Joint speed	30 °/s
TCP speed	250 mm/s
TCP force	100 N
Momentum	10 kg m/s
Power	80 W

The safety system issues a Stop Category 0 if a violation of these limits appears.

Safety-related Electrical Interfaces

The robot is equipped with several safety-related electrical inputs and outputs. All safety-related electrical inputs and outputs are dual channel. They are safe when low, e.g. the emergency stop is not active when the signals are high (+24V).

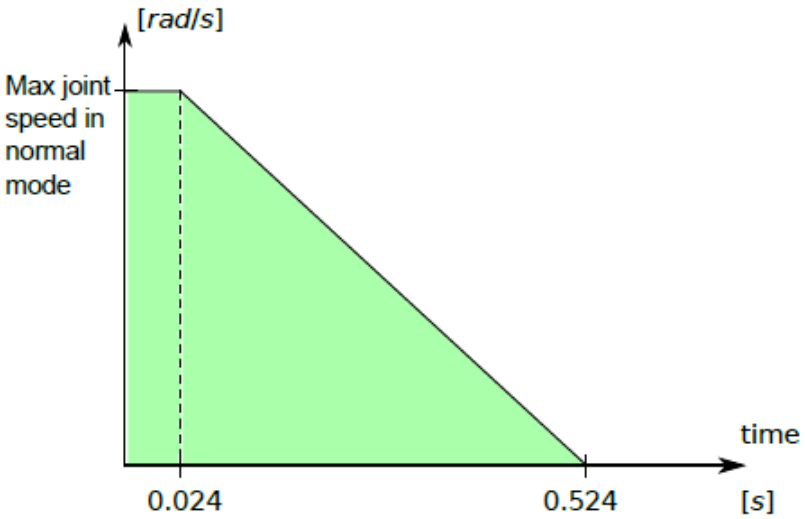
Safety-related Electrical Inputs

The table below gives an overview of the safety-related electrical inputs.

Safety Input	Description
Robot Emergency Stop	(Dedicated Input). Performs a Stop Category 1, which can be forwarded to other machines using the *System emergency stop* output when configured.
Emergency Stop Button	(Teach Pendant Button). Performs a Stop Category 1, which can be forwarded to other machines using the *System emergency stop* output when configured.
System Emergency Stop	(Configurable Input). Performs a Stop Category 1. To avoid deadlocks, this signal will not be forwarded to other machines through the *System emergency stop* output.
Safeguard Stop	(Dedicated Input). Performs a Stop Category 2.
Safeguard Reset	(Configurable Input). Resumes the robot from a *Safeguard stopped* state, when an edge on the Safeguard reset input occurs.
Reduced Mode	(Configurable Input). The safety system transitions to *Reduced* mode limits.
Three-Position Enabling Device	(Configurable Input). Functions as a safeguard stop input when the operational mode input is high.
Operational Mode	(Configurable Input). Operational mode to use when a Three-position enabling device is configured.

Stop Category 1 and a Stop Category 2 decelerates the robot with drive power on, which enables the robot to stop without deviating from its current path.

Monitoring of safety inputs



The green area below the ramp is the allowed speeds for a joint during braking. At time 0 an event (emergency stop or safeguard stop) is detected at the safety processor. Deceleration begins after 24 ms.

Stop Category 1 and Stop Category 2 are monitored by the safety system in the following way:

1. The safety system monitors that the braking initiates within 24 ms, see Figure 4.2.
2. If a joint is moving, its speed is monitored to never be higher than the speed obtained by constantly decelerating from the maximum joint speed limit for Normal mode to 0 rad/s in 500 ms.
3. If a joint is at rest (joint speed is less than 0.2 rad/s), it is monitored that it does not move more than 0.05 rad from the position it had when the speed was measured below 0.2 rad/s.

Additionally, for a Stop Category 1, the safety system monitors that after the robot arm is at rest, the powering off is finalized within 600 ms. Furthermore, after a Safeguard Stop input, the robot arm is only allowed to start moving again after a positive edge on the safeguard reset input occurs. If any of the above properties are not satisfied, the safety system issues a Stop Category 0.

A transition to Reduced mode triggered by the reduced mode input is monitored as follows:

1. The safety system accepts both Normal and Reduced mode limit sets for 500 ms after the reduced mode input is triggered.
2. After 500 ms, only the Reduced mode limits are in effect.

If any of the above properties are not satisfied, the safety system issues a Stop Category 0. A Stop Category 0 is performed by the safety system with the performance described in the following table. The worst-case reaction time is the time to stop and to de-energize (discharge to an electrical potential below 7.3 V) a robot running at full speed and payload.

Safety Input Function	Detection Time	De-energizing Time	Reaction Time
Robot Emergency Stop	250 ms	1000 ms	1250 ms
Emergency Stop Button	250 ms	1000 ms	1250 ms
System Emergency Stop	250 ms	1000 ms	1250 ms
Safeguard Stop	250 ms	1000 ms	1250 ms

Safety-related Electrical Outputs

The table below gives an overview of the safety-related electrical outputs:

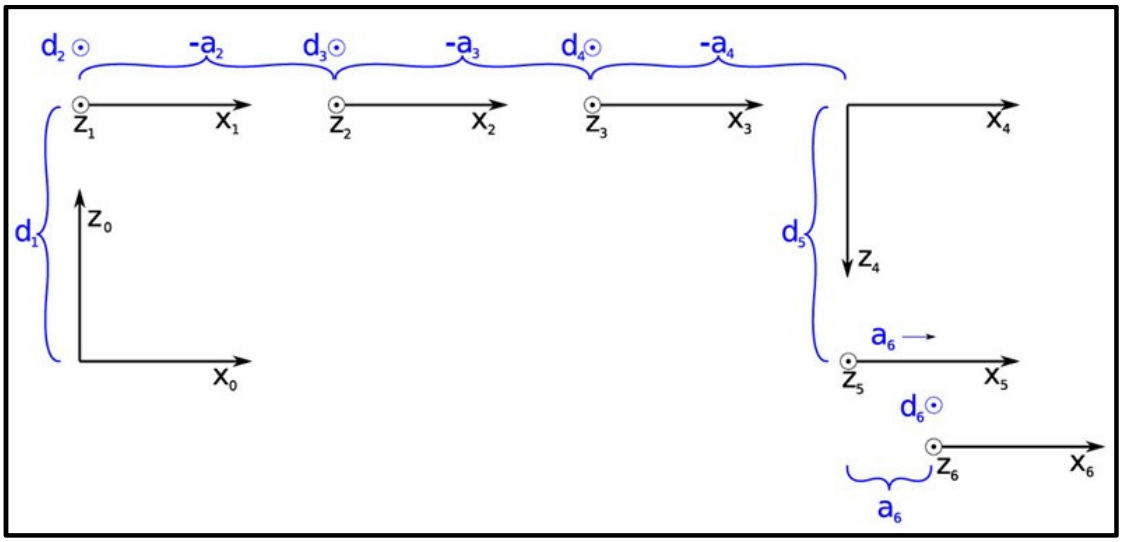
Safety Output	Description
System Emergency Stop	Logic low when the *Robot emergency stop* input is logic low or the Emergency stop button is pressed.
Robot Moving	While this signal is logic high, no single joint of the robot arm moves more than 0.1 rad.
Robot Not Stopping	Logic high when the robot is stopped or in the process of stopping due to an emergency stop or safeguard stop. Otherwise it will be logic low.
Reduced Mode	Logic low when the safety system is in *Reduced* mode.
Not Reduced Mode	The *Reduced mode* output negated.

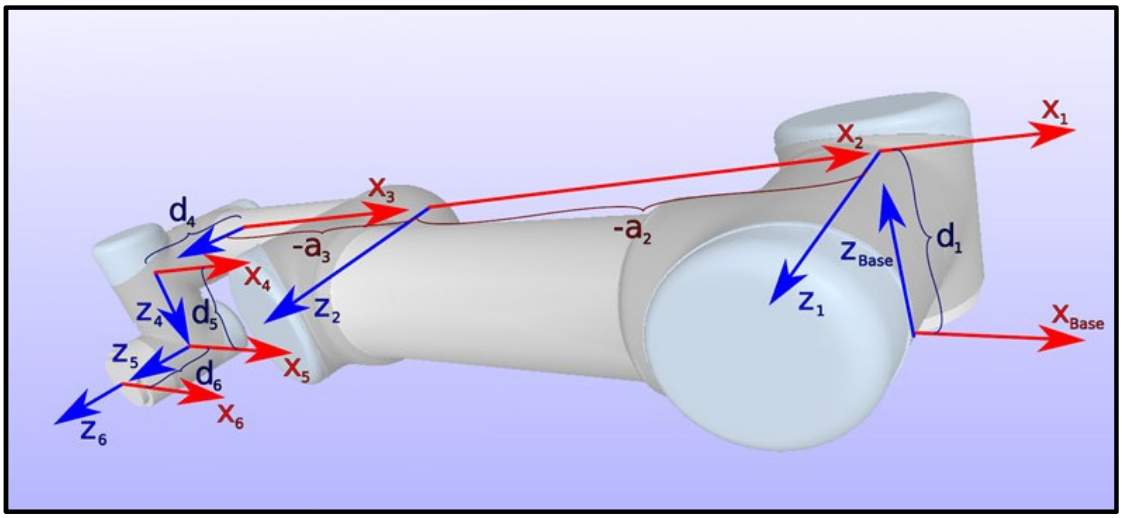
If a safety output is not set properly, the safety system issues a Stop Category 0, with the following worst-case reaction times:

Safety Output	Worst Case Reaction Time
System Emergency Stop	1100 ms
Robot Moving	1100 ms
Robot Not Stopping	1100 ms
Reduced Mode	1100 ms
Not Reduced Mode	1100 ms

Kinematics

The Denavit–Hartenberg parameters in UR10 robot are described as the below diagrams:





The Denavit–Hartenberg parameters of UR robots are shown as below.

UR10							
Kinematics	Theta [rad]	a [m]	d [m]	Alpha [rad]	Dynamics	Mass [kg]	Center of Mass [m]
Joint 1	0	0	0.1273	π/2	Link 1	7.1	[0.021, 0.000, 0.027]
Joint 2	0	-0.612	0	0	Link 2	12.7	[0.38, 0.000, 0.158]
Joint 3	0	-0.5723	0	0	Link 3	4.27	[0.24, 0.000, 0.068]
Joint 4	0	0	0.163941	π/2	Link 4	2	[0.000, 0.007, 0.018]
Joint 5	0	0	0.1157	-π/2	Link 5	2	[0.000, 0.007, 0.018]
Joint 6	0	0	0.0922	0	Link 6	0.365	[0, 0, -0.026]