Table 1: Safety Function (SF) Descriptions

NOTE: all safety functions are individual safety functions

TUV NORD Certified SF	Internal?	Safety Function	Description	What is controlled?
SF0	Internal	**Emergency Stop** [1, 2, 3, 4] *There are two separate Emergency Stop safety functions*	Pressing the Estop PB on the pendant[1] or the External Estop (if using the Estop Safety Input configured for Estop) results in both a Cat 0 & a Cat 1 stop according to IEC 60204-1 (NFPA79) [3]. These are **SF0** and **SF1** respectively. **SF0**: 524ms timer setting in each safety controller's microprocessor. At the end of the 524ms, Cat 0 stop[3] (IEC 60204-1) is initiated by each microprocessor. **SF1**: Command[1] all joints to stop and upon all joints coming to a standstill state, power is removed. This is a Cat 1 stop[3] per IEC 60204-1. The stopping times[4] of the **SF0** and **SF1** Estop safety functions differ. • **SFO** has a functional safety rating of PLd Cat3 with the worst-case stopping time, as if all joint monitoring failed at the same time and after 524ms, then power is immediately removed while the robot is going the maximum speed. This could result in a worst case stopping time of 1250ms. • **SF1** has a functional safety rating of PLd Cat2 (see functional safety information, starting on page 6) with a reliable and realistic maximum stop time of approximately 300ms for UR3 and 400ms for UR5/UR10. See the User Manual for specific information. The application stop time can be reduced depending on the application's safety limits (SF3, 4, 6, 7, 8, 9) settings and the use of the stop time information provided in the manual.	**Robot Arm**
SF1				
SF2	Logic and outputs INTERNAL	**Safeguard stop (Protective Stop)**	This safety function is initiated by an external protective device using safety inputs which will initiate a Cat 2 stop[3] per IEC 60204-1. *For the functional safety rating of the complete integrated safety function, add the PFHd of the external protective device to the PFHd of SF2.* *If a PLd Cat3 stop is needed for protective devices, connect the protective device and configure the input as if it were an external Estop input (See SF0).*	**Robot Arm**

[1] **Communications between the Teach Pendant, controller & within the robot arm (between joints) are SIL 2** for safety data, according to IEC 61784-3. Any failure will be detected within 16ms.
See ***NOTES***

[2] **Estop validation**: the pendant Estop pushbutton is evaluated within the pendant, then communicated[1] to the safety controller by SIL2 communications. To validate the pendant Estop function, press the Pendant Estop pushbutton and verify that an Estop results. This validates that the Estop is connected within the pendant, functioning as intended, and the pendant is connected to the controller. See Estop Output for information about Estop I/O.

[3] **Stop Categories** according to IEC 60204-1 (NFPA79)

- **Category 0 and 1** result in the removal of drive power, with Cat 0 being IMMEDIATE and Cat 1 being a controlled stop (decelerate then removal of power).
  Estop is either Cat 0 or Cat 1. As an exception, the Estop can result in a Cat 2 stop.
- **Category 2** is a stop where drive power is NOT removed. For Category 2 stops, their specifications are defined in IEC 60204-1, while SS1 and SS2 are defined IEC 61800-5-2.

[4] **Emergency Stop response time**: From a user interface standpoint, selecting Estop results in having both the PLd Cat 2 and PLd Cat 3 Estop. It is an integration decision whether the PLd Cat2 or PLd Cat3 response time is used for the calculation of the stopping distance. Typically, the protective stop stopping time is used as this type of stop is intended for protective purposes.

TUV NORD Certified SF	Internal?	Safety Function	Description	What is controlled?
SF3	Internal	**Joint Position Limit (soft axis limiting)**	Exceeding the joint position limit results in a Cat 0 stop[5] (IEC 60204-1). Each joint can have its own limit. *Directly limits the set of allowed joint positions that the joints can move to. It is set directly in the safety setup part of the UI where you can enter values. It is a means of safety-rated soft axis limiting and space limiting, according to ISO 10218-1:2011, 5.12.3.*	**Joint (each)**
SF4	Internal	**Joint Speed Limit**	Exceeding a joint speed limit results in a Cat 0 stop[5] per IEC 60204-1. Each joint can have its own limit. *Directly limits the set of allowed joint speeds which the joints are allowed to perform. It is set directly in the safety setup part of the User Interface where you can enter values.* *It can be used to limit fast joint movements, for instance to limit risks related to singularities.*	**Joint (each)**
SF5	Internal	**Joint Torque Limit**	Exceeding the joint torque limit (each joint) results in a Cat 0 stop[5] (per IEC 60204-1). ***This is not accessible to the user as it is a factory setting, part of the force limiting safety function.***	**Joint (each)**
SF6	Internal	**TCP Pose Limit**	Monitors the **TCP** Pose (position and orientation), any violation of a safety plane or TCP Pose Limit will result in a Cat 0 stop[5] (IEC 60204-1). *This safety function consists of two parts. One is the safety planes for limiting the possible TCP positions. The second is the TCP orientation limit, which is entered as an allowed direction and a tolerance.* *This provides TCP inclusion/ exclusion zones due to the safety planes.* *When a limit (plane or TCP pose) is violated, a Cat 0 stop is initiated.*	**TCP**
SF7	Internal	**TCP Speed Limit**	Exceeding the **TCP** speed limit results in a Cat 0 stop[5] (IEC 60204-1).	**TCP**
SF8	Internal	**TCP Force Limit**	Exceeding the **TCP** force limit results in a Cat 0 stop[5] (IEC 60204-1). *Limits the external clamping force exerted by the robot. See also Joint Torque Limit (SF5).*	**TCP**
SF9	Internal	**Momentum Limit**	Exceeding the momentum limit results in a Cat 0 stop[5] (IEC 60204-1). *The momentum limit is very useful for limiting transient impacts.* *The Momentum Limit affects the entire robot arm.*	**Robot Arm**

[5] **Stop Categories** according to IEC 60204-1 (NFPA79)

- **Category 0 and 1** result in the removal of drive power, with Cat 0 being IMMEDIATE and Cat 1 being a controlled stop (decelerate then removal of power). Estop must be either Cat 0 or Cat 1.
- **Category 2** is a stop where drive power is NOT removed. For Category 2 stops, their specifications are defined in IEC 60204-1, while SS1 and SS2 are defined IEC 61800-5-2.

TUV NORD Certified SF	Internal?	Safety Function	Description	What is controlled?
SF10	Internal	**Power Limit**	Exceeding the power limit results in a Cat 0 stop[5] (IEC 60204-1). *This function monitors the mechanical work (sum of joint torques times joint angular speeds) performed by the robot, which also affects the current to the robot arm as well as the speed of the robot arm.* *This function dynamically limits the current/torque but maintain the speed.*	**Robot Arm**
SF11	Internal as a function with dual outputs	**UR Robot Estop Output**	When configured for Estop output and there is an Estop condition (see SF1), the dual outputs are LOW. If there is no Estop condition, dual outputs are high. Pulses are not used but they are tolerated. *For the integrated functional safety rating with an external Estop device, add the PFHd of the UR Estop function (SF0 or SF1) to the PFHd of the external logic (if any) and its components (e.g. Estop pushbutton).*[6]	**External connection to logic &/or equipment**
SF12	Internal as a function with dual outputs	**UR Robot Moving: Digital Output**	Whenever the robot is moving (motion underway), the dual digital outputs are LOW. Outputs are HIGH when no movement. *The functional safety rating is for what is within the UR robot. The integrated functional safety performance requires adding this PFHd to the PFHd of the external logic (if any) and its components.*	**External connection to logic &/or equipment**
SF13	Internal as a function with dual outputs	**UR Robot Not stopping: Digital Output**	Whenever the robot is STOPPING (in process of stopping or in a stand-still condition) the dual digital outputs are HIGH. When outputs are LOW, robot is NOT in the process or stopping and NOT in a stand-still condition. *The functional safety rating is for what is within the UR robot. The integrated functional safety performance requires adding this PFHd to the PFHd of the external logic (if any) and its components.*	**External connection to logic &/or equipment**

[6] **Estop validation**: the pendant Estop pushbutton is evaluated within the pendant, then communicated[1] to the safety controller by SIL2 communications.
See Communications and Safety Functions on page 10.
To validate the pendant Estop function, press the Pendant Estop pushbutton and verify that an Estop results. This validates that the Estop is connected within the pendant, functioning as intended, and the pendant is connected to the controller. See footnote 13. The connection from the pendant to the safety controller is by safety communications according to SIL 2 (See page 10).
See Estop Output for information about Estop I/O.

TUV NORD Certified SF	Internal?	Safety Function	Description	What is controlled?
SF14	Internal as a function with dual outputs	**UR Robot Reduced Mode: Digital Output**	Whenever the robot **is in reduced mode,** the dual digital outputs are LOW. *See Robot Reduced Mode below.* *The functional safety rating is for what is within the UR robot. The integrated functional safety performance requires adding this PFHd to the PFHd of the external logic (if any) and its components.*	**External connection to logic &/or equipment**
SF15	Internal as a function with dual outputs	**UR Robot Not Reduced Mode: Digital Output**	Whenever the robot is NOT in reduced mode, the dual digital outputs are LOW. *The functional safety rating is for what is within the UR robot. The integrated functional safety performance requires adding this PFHd to the PFHd of the external logic (if any) and its components.*	**External connection to logic &/or equipment**
Robot Reduced Mode	Internal Logic and Outputs, with Dual Inputs (1 through 4)	**Reduced Mode Input**	Reduced Mode can be initiated by a safety plane/ boundary (starts when at 2cm of the plane and reduced mode settings are achieved within 2cm of the plane) or by use of an input to initiate (will achieve reduced settings within 500ms). When the external connections are Low, Reduced Mode is initiated. Reduced Mode means that ALL reduced mode limits are ACTIVE *Reduced mode is not a safety function, rather it is a state affecting the settings of the following safety function limits: SF3 joint position, SF4 joint speed, SF6 TCP pose limit, SF7 TCP speed, SF8 TCP force, SF9 momentum, and SF10 power.*	**Robot Arm**
Safeguard Reset	Internal Logic and Outputs, with Dual Inputs (1 through 4)	**Safeguard Reset Input**	When configured for Safeguard Reset and the external connections transition from low to high, the safeguard stop RESETS Safety input to initiate a reset of safeguard stop safety function SF2.	**Robot**

TUV NORD Certified SF	**Internal?**	**Safety Function**	**Description**	**What is controlled?**
Enabling Device	External Enabling Device as input to UR Robot logic	**3 Position Enabling Device INPUT**	When the external Enabling Device connections are Low, a Safeguard Stop (SF2) is initiated. ***Recommendation****: Use with a mode switch as a safety input.* *If a mode switch is not used and connected to the safety inputs, then the robot mode will be determined by the User Interface. If the User Interface is in* • *"run mode", the enabling device will not be active.* • *"programming mode", the enabling device will be active. It is possible to use password protection for changing the mode by the User Interface.*	**Robot**
Mode Selection	External Mode Switch using dual Inputs (1 through 4) and internal logic	**Mode switch INPUT**	When the external connections are Low, Operation Mode (running) is in effect. When High, the mode is programming or teach. ***Must be used with an Enabling Device as a safety input****.* *When in Teach/Program (Mode switch inputs high), enabling device is required for operation. When in teach/program, initially the TCP speed will be limited to 250mm/s.* *The speed can manually be increased by using the pendant user interface "speed-slider", but upon activation of the enabling device, the speed limitation will reset to 250mm/s.*	**Robot**

Table 2: Compliance and ISO 13849-1 Functional Safety Information [7, 8]

TUV NORD Certified SF	Safety Function	Limits or USER configuration or Factory Setting	Stop Category per IEC 60204-1[9]	IEC 61800-5-2 Stop: power to final switching devices retained *for Category 2 stop*	PL	Cat	PFHd UR 3/5/10
SF0	**Emergency Stop** 8, 9, 10, 11, 12, 13, 14 *There are two separate Emergency Stop safety functions: SF0 and SF1*	No	**Cat 1 Stop** *524ms time-delay before Cat 0 stop is initiated*	*NA*	**d**	**3**	**4.38E-8** See [10]
SF1	**Emergency Stop** 11, 13, 14 *There are two separate safety functions: SF0 & SF1*	No	**Cat 1 Stop** *when at SS1 standstill, Cat 0 stop initiated*	**SS1** [15] *when at SS1 standstill, Cat 0 stop initiated*	**d**	**2**	**3.16E-07** See [10]

[7] All safety functions are individual safety functions.

[8] **MTTFd is limited to 100 years by ISO 13849-1.** The actual MTTFd values are greater than 100 years. **For all safety functions, the DCavg is 90%.**

[9] **Stop Categories according to IEC 60204-1 (NFPA79).**

- **Category 0 and 1** result in the removal of drive power, with Cat 0 being IMMEDIATE and Cat 1 being a controlled stop before removal of power. Estop is either Cat 0 or Cat 1.
- **Category 2** is a stop where drive power is NOT removed. For Category 2 stops, their specifications are defined in IEC 60204-1, while SS1 and SS2 are defined IEC 61800-5-2.

[10] **Emergency stop safety functions**: MTTFd, DCavg and PFHd uses fault exclusion in accordance with ISO 13849-1 due to use of direct acting contacts.
If fault exclusion were **not** used, then the PFHd values would be: **SF0**: 1.60E-07; **SF1**: 4.27E-07; **SF11**: 1.56E-07.

[11] **Emergency stop components and safety function** complies with IEC 60204-1, IEC 60947-5-1 (direct acting contacts), ISO 13850 and ISO 13849-1.

[12] **Communications between the Teach Pendant and the controller, as well as within the robot arm & between joints are SIL 2** for safety data, according to IEC 61784-3. Any failure will be detected within 16ms. See Communications and Safety Functions on page 10.

[13] **Estop validation**: the pendant Estop pushbutton is evaluated within the pendant, then communicated[1] to the safety controller by SIL2 communications. To validate the pendant Estop function, press the pendant Estop pushbutton and verify that an Estop results. This validates that the Estop is connected within the pendant, functioning as intended, and the pendant is connected to the controller. See Estop Output for information about Estop I/O.

[14] **Emergency Stop response time**: From a user interface standpoint, selecting Estop results in having both the PLd Cat 2 and PLd Cat 3 Estop. It is an integration decision whether the PLd Cat2 or PLd Cat3 response time is to be used for the calculation of the stopping distance.

[15] **SS1 (Safe Stop 1)** according to IEC 615800-5-2

a) initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit; or
b) initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit; or
c) initiates the motor deceleration and initiates the STO function after an application specific time delay.

NOTE This safety function corresponds to a controlled stop in accordance with stop category 1 of IEC 60204-1.

TUV NORD Certified SF	Safety Function	Limits or USER configuration or Factory Setting	Stop Category per IEC 60204-1[9]	**IEC 61800-5-2 Stop:** power to final switching devices retained *for Category 2 stop*	PL	Cat	PFHd UR 3/5/10
SF2	**Safeguard stop (Protective Stop)**	No	**Cat 2**	**SS2** [16]	**d**	**2**	**3.15E-07**
SF3	**Joint Position Limit (soft axis limiting)**	Limits[17]	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF4	**Joint Speed Limit**	Limits[17]	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF5	**Joint Torque Limit** *internal factory setting*	factory setting	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF6	**TCP Pose Limit**	Limits[17]	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF7	**TCP Speed Limit**	Limits[17]	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF8	**TCP Force Limit**	Limits[17]	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF9	**Momentum Limit**	Limits[17]	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF10	**Power Limit**	Limits[17]	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**

[16] **SS2 (Safe Stop 2) according to IEC 615800-5-2**

a) initiates and controls the motor deceleration rate within set limits to stop the motor AND initiates the safe operating stop function when the motor speed is below a specified limit; OR

b) initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function when the motor speed is below a specified limit; OR

c) initiates the motor deceleration and initiates the safe operating stop (SOS) function after an application specific time delay.

NOTE This safety function corresponds to a controlled stop in accordance with stop category 2 of IEC 60204-1.

[17] UR robots are controlled so that the use of our robots will NOT exceed or reach a limit. This is internally accomplished by limiting speeds, momentum, and other attributes. Therefore, validation of a safety limiting function can only be done by trying to move the robot with the intent of reaching a limit. Being unable to reach the limit is the validation. Extremely low operating speeds can happen because UR robots adjust operational settings to ensure not exceeding any limits.

TUV NORD Certified SF	Safety Function	Limits or USER configuration or Factory Setting	Stop Category per IEC 60204-1[9]	IEC 61800-5-2 Stop: power to final switching devices retained *for Category 2 stop*	PL	Cat	PFHd UR 3/5/10
SF11	**UR Robot Estop Output**	Output & I/O Configuration	**See Estop SF1**	*See Estop SF1*	**d**	**2**	**4.41E-08** See [10, 11]
SF12	**UR Robot Moving: Digital Output**	Output & I/O Configuration	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF13	**UR Robot Not stopping: Digital Output**	Output & I/O Configuration	**Cat 0**	*NA*	**d**	**2**	**3.15E-07**
SF14	**UR Robot Reduced Mode: Digital Output**	Output & I/O Configuration	**Cat 0** if fault detected	*NA*	**d**	**2**	**3.15E-07**
SF15	**UR Robot Not Reduced Mode: Digital Output**	Output & I/O Configuration	**Cat 0** (immediate stop)	*NA*	**d**	**2**	**3.15E-07**
Robot Reduced Mode	**Reduced Mode INPUT**	Input & I/O Configuration	**Cat 2**	**SS2** [18]	**d**	**2**	**3.15E-07**
Safeguard Reset	**Safeguard Reset INPUT**	Input & I/O Configuration	**Cat 2**	**SS2** [18]	**d**	**2**	**3.15E-07**
Enabling Device	**3 Position Enabling Device INPUT**	Input & I/O Configuration	**Cat 2**	**SS2** [18]	**d**	**2**	**3.15E-07**
Mode Selection	**Mode switch INPUT**	Input & I/O Configuration	**Cat 2**	**SS2** [18]	**d**	**2**	**3.15E-07**

[18] **SS2 (Safe Stop 2) according to IEC 615800-5-2**

a) initiates and controls the motor deceleration rate within set limits to stop the motor AND initiates the safe operating stop function when the motor speed is below a specified limit; OR

b) initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function when the motor speed is below a specified limit; OR

c) initiates the motor deceleration and initiates the safe operating stop (SOS) function after an application specific time delay.

NOTE This safety function corresponds to a controlled stop in accordance with stop category 2 of IEC 60204-1.

NOTES

All safety functions are individual safety functions.

The UR safety controller has two microprocessors for monitoring incoming inputs, logic, and communications (see page 9)**.**

Stopping times of the SF0 and SF1 Emergency Stop safety functions:

SFO has a functional safety rating of PLd Cat3 with the absolutely-worse case stopping time, as if all joint safety monitoring failed at the same time, at full speed, and then after 524ms, the power is immediately removed. This results in a worst case stopping time of 1250ms

SF1 has a functional safety rating of PLd Cat2 with a reliable (see functional safety information, starting on page 6) and realistic maximum stop time of approximately 300ms for UR3 and 400ms for UR5/UR10. See the User Manual for specific information. The application stop time can be reduced depending on the application's safety limits (SF3, 4, 6, 7, 8, 9, 10) settings and the use of the stop time information provided in the manual. *From a user interface standpoint, selecting Estop results in having both a PLd Cat 2 and PLd Cat 3 Estop.*

SF2 has a functional safety rating of PLd Cat2 with a reliable (see functional safety information) and realistic maximum stop time of approximately 300ms for UR3 and 400ms for UR5/UR10. See the User Manual for specific information. The application stop time can be reduced depending on the application's safety limits (SF3, 4, 6, 7, 8, 9, 10) settings and the use of the stop time information provided in the manual.

It is an integration decision whether the Protective Stop (PLd Cat2) or the Emergency Stop (PLd Cat3) response time is to be used for the calculation of the stopping distance. Since the Emergency Stop is not considered a safeguard, it is typically recommended to use the Safeguard Stop (Protective Stop) stopping time.

Communications and Safety Functions:

Communications between the Teach Pendant and the controller, as well as within the robot arm & between joints are SIL 2 for safety data, according to IEC 61784-3. Any failure will be detected within 16ms.

Some diagnostics require filtering of data to avoid false positives. In these cases, the detection of a fault can range from 8 to 25ms.

Depending on the safety function and its diagnostics, fault detection is between 16ms and 33ms.
<u>It is recommended to use 33ms</u>, due to the detection variability.