Performance Level of Plasmasystem PB3/PS2000

Safety considerations according to EN ISO 13849

The risk of a high voltage powered plasma-processing unit is assessed. If system boundaries are clearly defined, the risks are identified and intercepted with adequate technical measures it is straight forward to design safe equipment. Integrating a PS2000 and a high power plasmajet of relyon in a "state of the art" processing unit can easily reach a performance level (PL) D.

Safety systems are active or passive components that make production equipment safer for the operator and the environment.

Machines and process equipment can be dangerous if operated inadequately or if faulty, subsystems lead to malfunction. In some cases, the damage can propagate and induce secondary failures if the equipment is not stopped immediately. However the best safety system will not avoid that the operating personnel is aware of the potential hazards. Typically production processes are controlled via software (PLC or computer) and embedded into an electrical and mechanical safety concept. First the potential hazards have to be listed and the risk has to be assessed. This safety concept has then to intercept these critical situations with a given reliability. Particularly electrical installations powered with dangerous voltages have to be shut down quickly.

The following risk assessment will be carried out using an inductive approach that analyzes the system reaction to a given fault scenario and the probability to detect and the ability to reduce the effect to an acceptable level. That means that statistical tests have to be performed using induced faults and the propagation trough the safety system.

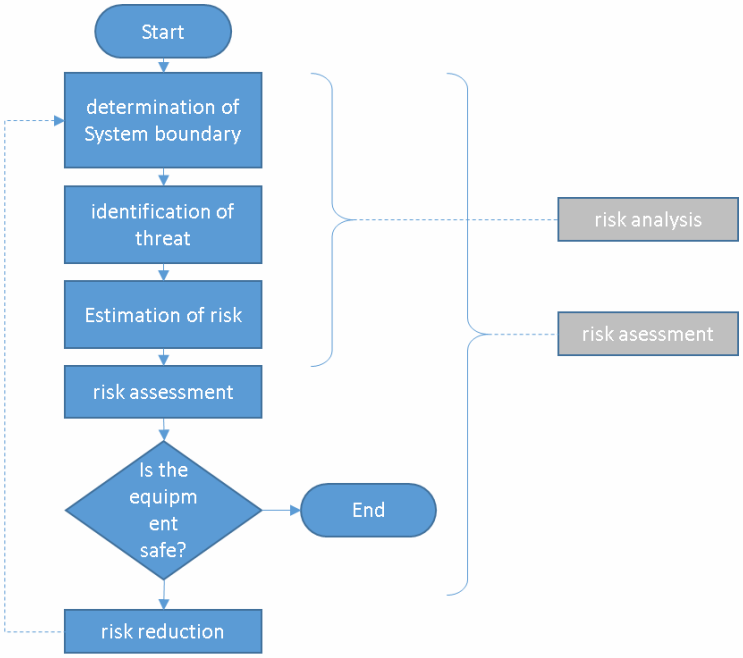

Diagram 1 Flow chart of risk assessment

System definition and boundaries

Diagram 2 Plasmasystem composed of a 19Inch Rack mountable high voltage power supply (PS2000) a high voltage connector and cable assembly and the plasma generator (PB3) with nozzle..

The power supply PS2000 is the central part of an atmospheric plasma system used to treat technical surfaces and materials. Typical application are surface activation prior to molding, coating casting, printing etc. The power supply is designed to be rack mounted (19inch standard) and to drive the PB3 atmospheric plasma generator of relyon. Therefore, the subsystem consisting of the power supply, the connecting cable and the plasma generator will be considered here.

The PS2000 is equipped with an emergency stop circuit that has to be included into the safety assessment.

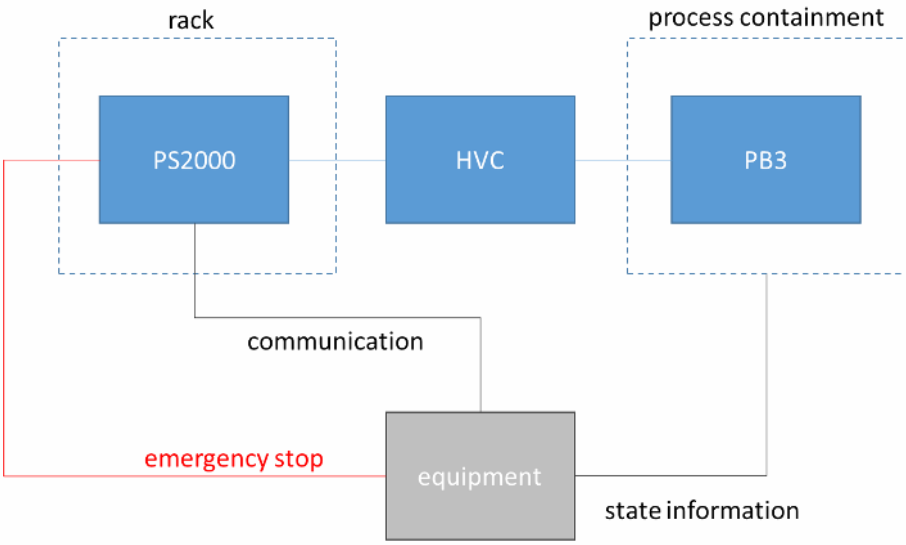

Diagram 3 Rack mounted Power supply (PS2000) connected via high voltage cable (HVC) to the plasma generator (PB3). The dotted line depicts the enclosure of the process equipment with safety means to avoid accidental contact with operating personnel (light barrier or door). The complete state information is transferred to the process controller. The emergency stop is wired separately.

In the following consideration only the functional reliability and safety of the plasma-sub-system is considered. This perspective has to assume that the plasma system is embedded into a well-designed and functional environment and that the safety means (light barriers etc.) are working correctly. Also it is assumed that the plasma system is integrated in compliance with the manual and oeration instruction from relyon plasma. The overall function of the complete process equipment cannot be assessed here. Particularly it is assumed that if an external failure occurs the emergency stop is triggered reliably.

Possible hazards (Identification)

1. Contact with unmounted PB3 plasma generator, enclosure opened
2. Contact with plasma beam during process operation
3. Damage of the high voltage cable
4. Unplugging the HVC from the PB3 during operation
5. Unplugging the HVC from the PS2000 during operation

Hazard frequency (risk estimation)

All failures involving high potentials are considered as severe hazards with potentially lethal consequences and therefore the safety concept has to be reliable.

Hazard 1 and 2 can occur daily (manual service, exchange of nozzle etc.) and would be critical if the high voltage is not switched off.

Hazard 1 and 2 are intercepted if the emergency circuit of the PS2000 is correctly embedded into the safety concept of the process equipment

Hazard 3 will only occur quite rarely. Identical equipment has been working for a cumulated 10^5 hours or more and similar defects have only been observed less than 10 times if. In most situations, the cable was damaged mechanically due to violent interaction. In all reported cases the PS2000 has switched off triggered by a detection of a low HV status. If the equipment is started, again the same failure will shut down the high voltage again and trigger the emergency stop.

The cable is made of flame retardant and self-extinguishing material. However, we decided to simulate this scenario (cable damage) practically, to document the effect, and to log the system reaction.

Hazard 4 will only occur if during service activities the high voltage cable is disconnected without stopping the process or if the process is started while the cables are still disconnected. The frequency of this operating error is estimated to be 1 per annum. All connectors are designed and certified to be protected against direct contact with the high voltage side (male/female concept) and isolated against voltage surge. Additionally the power supply will detect the load less situation and switch off after about 1 second. Communication will still be running.

Hazard 5 can only occur if the HV cable is unplugged and can be considered similarly to failure 4.

Hazard 1-2 have to be intercepted via emergency stop actions. Hazard 3-5 are detected by the PS2000 internally and will also trigger the emergency stop.

Performance Level of the internal emergency circuit

The only critical interface carrying hazardous voltages is the high voltage line. The high voltage is generated using an active switching unit and transformer (switching power supply) If the beat of the switching unit misses the potential disappears. No direct galvanic connection to the grid power is present at this interface. Hence shutting down of the high voltage can be reached using two totally independent channels: (A) disconnecting the PFC voltage from the power stage using the implemented relay, or stopping the beat of the chopping final stage. The communication (CAN bus) is running on a separate microcontroller and will not be affected by either of both.

Notaus (Geräterückseite PS2000)

The PS2000 power supply is delivered with a connector to plug in an external emergency stop circuit (normally open function).

Triggering this emergency circuit, will (a) disconnect the high power stage and PFC from the grid by opening a relay and stop the heartbeat for the generation of the swiched high voltage.

The internal relay has a MTTF of $3*10^4$ cycles. If the relay would lock, the power stage would still get the power from the PFC. In this case additional safety reserve is gained through stopping the heartbeat needed for the active high voltage generation. To check the reliability of this process we induced the emergency 10^4 times with two PS2000 with clamped disconnecting relays (induced damage). In no case of this hardware in the loop test, a dangerous voltage was found even though the relay was clamped on intentionally.

Given the logged data of the tests, the failure probability can be calculated:

$P_{Rel} < 1/24*1/30.000 = 1.38 \times 10^{-6}$

$P_{Soft} < 10^{-4}$

$\underline{P_{Notaus} < 1.38e^{-6}*10^{-4} = 1.38*10^{-10}}$

Risk assessment of HV cable damage

We simulated practically the damage of the HV cable by different mechanical means (cutting, squeezing, crushing) and burning.

During the 200 documented induced failures, the power supply (PS2000) always detected an error and triggered the emergency stop. Communication a failure reporting continued to be active over the CAN interface. With these experimental findings, the failure probability can be calculated:

$P_{Kabelschaden} < 10/300/4000 = 8.33*10^{-6}$

$P_{Nichterkennung} < 1/200 = 10^{-2}$

200 induced cable damages.

$\underline{P_{HV} < 4.16*10^{-8}}$

Risk assessment of incorrect disconnection of the high voltage cable (failure 4-5)

Assuming that once a year the connection is opened under load, the probability of the failure can be calculated:

$P_{Trennung} < 2/365*24 = 2.28*10^{-4}$

$P_{Nichterkennung} < 1/10.000$

$P_{HVC}<2.3*10^{-8}$

Tested by checking 10.000 times the shut-down of the HV at missing load..

Risk summary

The different hazard risks weighted with the probability to avoid the hazard by the related safety means yields that the probability of a dangerous failure is **$<10^{-7}$ per hour**.

Using the table below a plasma system build of the described components can reach **performance level D**.

Performance Level (PL) according EN ISO 13849-1	Probability of fatal error per hour	Safety integrity level (SIL) according to IEC 61508
A	$10^{-4} – 10^{-5}$	-
B	$10^{-5} – 3\ 10^{-}6$	1
C	$3\ 10^{-6} – 10^{-7}$	1
D	**$10^{-7} – 10^{-8}$**	**2**
E	$10^{-7} – 10^{-8}$	3

Table 1 Overview of PL classification.