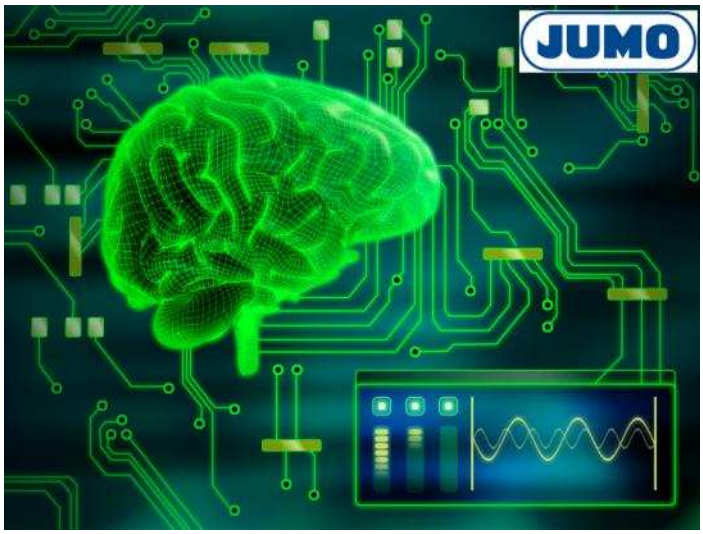
# Recertification of SIL Devices: Challenges and Opportunities




JUMO, named after the first two initials of its founder (**JU**chheim **MO**ritz), is a family-run medium-sized company based in Fulda, Germany that manufactures products and provides services in the field of industrial measurement, control, and automation technology. A look at the product portfolio quickly reveals that knowledge of sensor and control technology is a fundamental element of the company.

Early on JUMO already had a special focus on high and increased safety for sensors and thermostats. Thermostats, temperature monitors, temperature limiters, safety temperature limiters – all these devices reliably monitor the measured temperatures and, if necessary, safely disconnect the corresponding elements.
JUMO safety sensor technology has been given an additional boost through the JUMO dTRANS p20 pressure transmitter family with HART® protocol. This device is intrinsically safe or encapsulated in a pressure resistant manner for absolute/relative or differential pressure measurements. The device series has now been recertified by TÜV Nord according to the latest standard DIN EN 61508/-1/-2: 2011 path 2H. (IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems part 1 and 2). It is now classified as a SIL-capable device for safety equipment which has been proven in use.

But what exactly does "recertified" mean? Is this even "real" SIL? Does a standard SIL device not need to be developed from the start based on IEC 61508?
On the contrary, the consensus leans more toward the following: a recertification is an extremely time-consuming endeavor in which all relevant components and parts are subjected to extensive testing and supporting documentation is required. In concrete terms, a recertification according to DIN EN 61508/-1/-2: 2011 path 2H means the following for the manufacturer:


**Specifications and architecture:**
An error analysis must be created according to DIN EN 61508-2 table A1 with a corresponding diagnostic coverage for SIL 2 (type B). Corresponding IEC standards and manufacturer-specific information must be used to precisely identify the error distributions and error rates. Moreover, an FMEDA (Failure Mode Effect Diagnostic Analysis) must be conducted, calculated, and evaluated up to the component level. The final step is to evaluate and assess the electronics, software, and mechanics of the entire pressure transmitter architecture. Data that has been collected and evaluated is included in the overall analysis.

**Returns statistics:**

In addition, corresponding error analyses based on the quantities sold and repairs must also be performed. All possible errors identified in these analyses need to be categorized. Additionally, each individual status requires corresponding suggestions for improvement and adequate implementation of improvements. This means that an analysis must always be performed to ensure functional safety as well as the classification into systematic and random errors. The implementation of the stipulated improvements must be verified. Corresponding failure statistics and failure rates must be compiled from the categorized errors. These errors need to be given corresponding matrix classifications of dangerous, safe, detectable, and non-detectable. The data that has been collected and evaluated here is also included in the overall analysis.

**Validation of production:**
All work instructions for production must be indicated with corresponding specifications of the manufacturing process. For the series release, the individual process steps within the production must also be accurately defined in additional, specific documents. Management documents for the commencement of production must also be conveyed. These are, for example, basic documents for the series release including all relevant drawings, test instructions, and adjustments to the configuration plan and the alignment plan.

**Systematic suitability of production**:
The production must also be audited for functional safety on top of the already-existing monitoring facilities/audits such as for ATEX, ISO 9001 quality management, maritime approvals, and Eurasian approvals.

**TÜV Nord as the arbitrator:**
At this point it is important to be aware that even though the above steps need to be performed on-site, they need to be monitored, verified, and ultimately validated by a neutral body. It is certainly conceivable that such thorough monitoring of internal processes and procedures by an external individual may have a significant organizational impact. Additional costs also factor into the equation. However, the overhead really does make sense as all processes are ruthlessly exposed. Potential weaknesses or vulnerabilities are therefore clearly indicated and the opportunity of implementing change is provided.

**Safety was already included**
JUMO already focused on safety and reliability during the development stage of the JUMO dTRANS p20 series. The process transmitters had therefore implemented internal diagnostic algorithms from the start to verify the accuracy and validity of all process variables as well as the proper functioning of the memory. The output stages of the pressure gauges were and are also checked for possible irregularities by reading back the analog output signal and continuously reading the voltage supply.

**Verification with the calibration certificate**
Every JUMO dTRANS p20 and every JUMO dTRANS p20 Delta device receives a calibration certificate after a successful manufacturing and calibration process. This certificate confirms the analog current output related to a stipulated pressure signal. The adjustment and testing is performed using testing equipment that meets German standards (DAkkS - German Accreditation Body).


**Safety function and safety manual**

The objective with the JUMO dTRANS p20 and JUMO dTRANS p20 Delta versions was 1oo1 architecture (one-out-of-one). The hardware fault tolerance for this architecture is exactly zero (HFT = 0). Accordingly, this provides the architectural path 2H of DIN EN 61508/-1/-2: 2011 with low demand requirements: the pressure transmitters can be used with single-channel up to SIL 2 (HFT = 0). The safety function relates exclusively to measuring pressures and is described in detail in the attached safety manual. The JUMO dTRANS p20 generate a process-related measured value that is transmitted to the automa-

tion system as a 4 to 20 mA output signal. This means that the current output is the only safety-related signal of the transmitter. The available HART® signal, which is available at the same time, serves exclusively as a means of communication or configuration signal. The safety function is specified according to NAMUR NE 43, which means that the valid output signal is between 3.8 and 20.5 mA (measurement information). The output signal (failure information) in the event of a malfunction can be set to ≤ 3.6 mA or ≥ 21.0 mA.

**Recertification according to DIN EN 61508/-1/-2: 2011, path 2H:**
Even in this brief description it should be clear that recertification according to DIN EN 61508/-1/-2: 2011 actually guarantees a reliable device – for rigorous use in safety-critical systems. And to answer the question posed at the beginning:
"Yes, a recertified device is 'real' SIL!"

The recertification of an established and proven device is in no way inferior to a new device that has been developed according to SIL requirements. On the contrary – the "field experience" of these devices can be incorporated in the certification to improve safety. However, there is one bit of bad news from the manufacturer's perspective: enhancing or supplementing a recertified device to include additional features, measuring ranges, or process connections involves a great deal of overhead. The reason here is that the device is certified for a specific execution state (firmware, hardware, specific versions) and bears the amendment "SIL classification on grounds of proven in use".