How does POWERLINK Safety work?

openSAFETY: Stage 1
Christian Schlegel

Interview with Anton Meindl
EPSG Executive Officer
openSAFETY expands the open world of POWERLINK

With their open source release of the POWERLINK Safety stack, IXXAT adds a safety-oriented transfer protocol to the open source world of POWERLINK. A renowned service provider for data communication systems in the automation industry and a leading member of the Ethernet POWERLINK Standardization Group, IXXAT will make the stack available for download free of charge from their website on the occasion of the upcoming SPS/IPC/Drives exhibition. We take that cue to give you a POWERLINK FACTS issue that focuses exclusively on POWERLINK Safety. You will find a brief explanation of what POWERLINK Safety actually is, and how the software works. Christian Schlegel, IXXAT’s CEO, tells you in our interview why his company has decided to take this step. You also get the views of Anton Meindl, EPSG Executive Officer, as well as of Dr. Till Jaeger. A distinguished expert in the field of open source law, Jaeger discusses the specific liability issues anyone involved in the open source release and distribution of safety-oriented products should consider. The closing article provides information about the requirements for standard-compliant developments of safety software and hardware according to IEC 61508.

I hope you will find this an interesting read. Should you have any further questions about this subject, feel welcome to ask me in person at the EPSG stand at the upcoming SPS/IPC/Drives show.

Yours,
Rüdiger Eikmeier
EPSG General Manager

The purpose of safety systems

In order to prevent any damage to persons and machines, it is paramount that data in safety-sensitive areas of machines and plants are transmitted in time and in their entirety. Failures can occur for various reasons, e.g. if data packets are routed to the wrong recipient, or are delayed at a gateway due to traffic overload. Adverse conditions may also lead to erroneous transfer sequences for the packets, or cause incorrect data insertions. Lastly, electromagnetic interference also threatens the integrity of information transmissions. In bus-based safety systems, performance free from defects must be ensured by the protocol, which must enable cyclic checks of the network segments that are relevant for safety, and checks of the devices involved.

In case of an interruption in communication or an incomplete data transmission, it is to initiate a safe shutdown of the machine or plant.
Safety – what it is

Safety systems have long been implemented via dedicated external wiring. The introduction of new standards, such as the IEC 61508 in 1998, which defines the “Functional Safety of electrical/electronic/programmable electronic safety-related systems,” has cleared the way for bus-based safety systems featuring safety-oriented transfer protocols, which have allowed for shifting safety functions to control units, I/O modules, and drives. That has enabled safety measures with very little negative impact on production routines in risk scenarios.

■ Protocol-based solutions instead of extra wires

Safety systems have long been implemented via dedicated external wiring. The introduction of new standards, such as the IEC 61508 in 1998, which defines the “Functional Safety of electrical/electronic/programmable electronic safety-related systems,” has cleared the way for bus-based safety systems featuring safety-oriented transfer protocols, which have allowed for shifting safety functions to control units, I/O modules, and drives. That has enabled safety measures with very little negative impact on production routines in risk scenarios.

■ ■ ■■■

■ POWERLINK Safety

The safety-oriented protocol POWERLINK Safety is a real-time Ethernet-capable solution for machine and factory automation that is suitable for communication cycles in the microsecond range. As early as 2004, POWERLINK Safety was tested by TÜV RHEINLAND and approved for use in safety-sensitive applications as specified for IEC 61508 SIL 3 (see page 7), and for Category 4 of the EU standard 954-1. Hence, POWERLINK Safety is generally, and with no restrictions, suitable for applications of any safety level e.g. in power plants or traffic systems.

POWERLINK Safety allows for the transfer of both safety-oriented data and control data on one system, and via one line, irrespective of the bus that is used. Additional safe hardware modules, such as controllers and I/O modules, are indispensable to ensure compliance with safety requirements. However, they constitute components of one homogenous system. With this solution, parallel lines and installations of extra systems are no longer needed.

■ ■■■■

■ “Smart Safe Reactions” instead of machine stops

POWERLINK Safety enables flexible hazards management. “Smart Safe Reaction” denotes the safety system’s capability for flexible, measured responses to various situations. In order to protect people in hazardous areas, it is often entirely sufficient to slow down machine motions, or limit the torque to a safe level, instead of stopping altogether. This response maintains the synchronicity of the axes, and prevents offloading procedures, empty runs and restarts. In robot-supported factories, suitable programming allows for flexible changes to production routines as long as there are people within an unsafe area.

Safety-oriented reactions therefore only apply to specific mechatronic units where a person is close by.

■ Total independence from the fieldbus
■ Safe reaction time down to 100 µs Only
■ Automatic safe parameterization
■ Ideal for safe modular machine concepts
■ Sole 100% open safety solution
■ True SIL3 Black Channel approach
The POWERLINK Safety protocol basically features three outstanding characteristics: its definition of data transfer, its upper-level configuration services, and, most notably, its encapsulation of data that is relevant to safety into an extremely flexible telegram format. In all applications, POWERLINK indeed uses a frame with a uniform format, no matter whether for payload data transfer, or for configuration or time synchronization purposes. As variable as it is economic, frame length is contingent on the amount of data to be transferred. The safety nodes on the network automatically recognize the content, i.e. frame types and lengths do not have to be configured. Since POWERLINK Safety only uses the application-oriented layers of the OSI model, it is independent from the bus protocol in use. While the open transfer protocol POWERLINK is an ideal basis due to its strictly deterministic timing, very short cycle times, and low jitter, it is not an outright prerequisite for using the Safety protocol. An autonomous, bus-independent protocol, POWERLINK Safety is categorically compatible to Ethernet-based and real-time capable fieldbuses. POWERLINK Safety uses checksum procedures to perpetually examine whether transferred data content is incomplete, and constantly monitors the data transfer rate. As POWERLINK features extremely short cycle times, failures are detected almost without any delay. Since all data traffic irregularities will thus be recognized, even unsafe networks do not compromise safety functionality. However, the highest degree of safety for an automation solution can be achieved by implementing a consistent safety-oriented architecture, which uses safe sensors, actuators, and controllers, i.e. devices that supply and process redundant data.

The following paragraphs provide a brief overview of the transmission errors that may occur in networks, and of the mechanisms POWERLINK Safety uses to recognize these faults.

**Causes of fault …**
- Data duplications can occur if a network is linked to other networks via two gateways, both of which transfer the same set of data.
- Data loss will happen when a gateway does not pass on data at all, or feeds it into the wrong network.
- Insertions can occur if data packets can only be transferred in a sequence of partial packages due to their length, and different transfer routes via various gateways result in a mix-up of specific packet segments.
- Gateways can delay data transfers due to high load.
- Electromagnetic interference can distort data, which may result in the destruction of single bits, or even entire information sections.
- And, lastly, in networks where standard data as well as safety data are transferred, so-called “masquerades” can occur, i.e. standard data is taken to be safety data due to mix-ups and insertions. This will result in serious malfunctions.

**... and how POWERLINK Safety deals with them**
One of POWERLINK Safety’s most crucial mechanisms, the time stamp prevents data duplications, mix-ups, and delays. Every data packet is stamped with the current time when it is sent. This stamp enables the receiver to avoid double read-outs, and to determine the time sequence of different packets as well as any delays. POWERLINK Safety does not depend on distributed clocks; a special procedure provides for reliable synchronization of all micro-controller clocks within the nodes.
ty – how it works

Time monitoring in order to prevent faults caused by data loss or excessive delays means that the nodes are continuously monitored for live operation and proper functioning. In addition, as they are prompted for reply, Consumers can tell that the data link remains established. POWERLINK Safety implements this mechanism, which is called “Watchdog,” as a software-based function.

POWERLINK Safety frames also feature a unique, 8-bit or 16-bit identification tag that encodes parts of the address field, the telegram type contained, and the frame type. This identifier precludes any mix-ups on the receiving end. The most reliable means to identify changes to the original content is the CRC procedure, which employs polynomial division to generate a checksum for each data set, and attaches that and the polynomial as a bit sequence to the data set. The checksum is a distinctive encoding of the data set itself. Using the bit sequence and the key, the receiver calculates the original data set, and checks the result against the unencoded data set received. If any deviations from the original data content are detected, the message will be ignored.

The most reliable means to identify changes to the original content is the CRC procedure, which employs polynomial division to generate a checksum for each data set, and attaches that and the polynomial as a bit sequence to the data set. The checksum is a distinctive encoding of the data set itself. Using the bit sequence and the key, the receiver calculates the original data set, and checks the result against the unencoded data set received. If any deviations from the original data content are detected, the message will be ignored.

To the data set. The checksum is a distinctive encoding of the data set itself. Using the bit sequence and the key, the receiver calculates the original data set, and checks the result against the unencoded data set received. If any deviations from the original data content are detected, the message will be ignored.

As they are prompted for reply, Consumers can tell that the data link remains established. POWERLINK Safety implements this mechanism, which is called “Watchdog,” as a software-based function.

POWERLINK Safety duplicates the contents to be transferred and conjoins the two blocks of data into one POWERLINK Safety frame. Hence, the POWERLINK Safety frame consists of two subframes with identical content. Each subframe is provided with an individual checksum as a safeguard. The receiver compares the identical content of the two subframes. The probability that the same data is changed or destroyed in two such frames is extremely low, and even lower the more the frame length increases. That said, even in this extremely exceptional case, the checksums still serve as a corrective. The special format of the POWERLINK Safety frames, i.e. the two subframes with their own individual checksums, also makes “masquerades” extremely unlikely to occur, and precludes any erroneous processing of a masked standard message.

A POWERLINK Safety network may contain up to 1023 Safety domains, with up to 1023 nodes or devices permitted within each of these. Safety domains can extend over different and inhomogeneous networks, and can integrate the Safety nodes that are scattered throughout these into one domain. Safe and unsafe devices can be operated within one domain. Gateways allow for intercommunication between different Safety domains. POWERLINK Safety enables users to make hierarchical separations as well as to establish separate Safety zones on a network. Therefore, e.g. installations can be made in one zone, while production in other zones carries on unimpeded. In every domain, a Safety Configuration Manager (SCM) is responsible for continuous monitoring of all Safety nodes.

Illustration 2: The Safety frame is transported in the payload data area of a standard frame. It is comprised of two identical subframes, each of which carries an individual checksum to safeguard its integrity.
Mr Meindl, one and a half years ago, the EPSG has released openPOWERLINK, and it is now announcing an openSAFETY release for the upcoming SPS/IPC/Drives exhibition. What has been your experience with the open source release so far?

Meindl: We have had very good experiences with our open source policy. Since the day of the release of openPOWERLINK, we have seen a surge of downloads and have fielded many inquiries. Besides the German-speaking countries, our offer has been in great demand in Italy and France as well, and in Asia in particular, where openPOWERLINK has given rise to many new developments.

What, then, was the reason for the EPSG to release openSAFETY, i.e. a safety-oriented protocol, as open source?

Meindl: It is laid open because we intend to provide users in automation with an open source version of all crucial software needed to operate POWERLINK networks – in order to ensure top long-term viability for their investments. After SYSTEC electronic took the first step last year in April by releasing the open source version of the POWERLINK stacks for Masters and Slaves, the French service provider Kalycito followed suit one year later with a free configuration tool for POWERLINK networks, the openCONFIGURATOR. In the aftermath, many manufacturers have inquired whether there was also an open system for safety-oriented applications. Hence, we are glad that a respected specialist like IXXAT has taken up this issue and is now going to provide openSAFETY.

Are there any differences or restrictions compared to the existing POWERLINK Safety?

Meindl: No, the protocol is identical and provides the same scope of functions. With this open source release, manufacturers get a tried and tested system with no development risk, a system they can base their own product developments on.

You are not only the EPSG’s Executive Officer, but also a Business Manager at Bernecker+Rainer. What have been the reactions at B&R, where POWERLINK Safety is used as an integrated part of the safety systems?

Meindl: Well, comparable issues have come up with respect to POWERLINK before. Based on that previous experience, there is a very positive view at B&R as regards the opening of the safety protocol. We generally believe we need to distinguish ourselves based
on the devices. This is where we can create unique selling points. If you were to use a protocol as your USP, and this also goes for a safety-oriented protocol, that would even result in unfavorable views on the part of your customers. Openness tends to be more and more – and rightfully so – equated with long-term investment viability. What is true for standard network technologies will, in the future, increasingly be true for safety protocols as well.

**What does SIL mean?**

POWERLINK Safety has been approved by TÜV Rheinland for SIL 3 systems. What does that mean? SIL means Safety Integrity Level and constitutes a rating of the failure probability of a system based on IEC/EN 61508. The categories run from SIL level 1 to 4, with the probability of failure decreasing as the level rating increases. SIL 3 corresponds to a probability of failure of $10^{-7}$ to $10^{-8}$ failures per hour. The responsible IEC commission once established the general rule that the bus of a safety system must not be involved with more than one percent of all failures. In practice, that means that POWERLINK Safety may cause no more than $10^{-9}$ errors per hour – in other words, no more than one fault about every 115,000 years.

**What does that mean?**

**Meindl:** That means that, while openSAFETY is released under the BSD license, it can only be downloaded via IXXAT’s website, and only following a registration.

**Why is that so?**

**Meindl:** For reasons to do with the special considerations regarding safety-sensitive products. This is the only way to enable IXXAT to provide those who have downloaded openSAFETY with important information about the software, or notify them about updates or revisions.

**Do you generally assume that the "downloaders" have the necessary know-how for safe adaptations of the software to their devices?**

**Meindl:** That totally depends on the specific case. We do give all users a chance, though, to review the source code. If and how they use the software depends on the experience and capacities of the development departments that use the code. If users have only little or no expertise for IEC standard-compliant technology development, we recommend that they seek adequate support from experts, anyway. When in doubt, this will save manufacturers a great deal of time, money, and nerves, since the IEC 61508 standard imposes demanding requirements on them. These include experience with the interpretation of the standards, the strict documentation rules, and the special project management skills needed for the creation of functionally safe products. Those who have the expert knowledge as well as the necessary experience, and who can do without external services, do get a free software basis in openSAFETY, and do not have to pay any license fees.
Mr Schlegel, what has moved you and your company to make the stack for POWERLINK Safety openly available to the public at this time?

Schlegel:
We are doing this in support of the EPSG policy of creating an open POWERLINK world. With the POWERLINK user organization releasing an open source POWERLINK version last year, and the openCONFIGURATOR following suit this year, we believe this is a logical next step. Even though laying open POWERLINK Safety is a fundamentally different matter than the open release of the regular POWERLINK stack.

What are the differences?

Schlegel:
The differences lie in liability issues. In this regard, safety-oriented products are a very sensitive area. Only in its present form is the POWERLINK Safety stack TÜV-certified for Safety Integrity Level 3. This is a sample certification, so to speak, which is obviously only valid for the unmodified stack, and for POWERLINK Safety’s basic safety mechanisms.

But if users cannot adapt the stack, what good is the open source release?

Schlegel:
It is not so that users cannot modify the stack. Functional changes or optimizations are, of course, possible. However, if a modified stack is to be used in an actual application, it will have to undergo a reexamination and a new certification. As a rule, though, this will be necessary anyway, since manufacturers will have to create new or modified code in any case in order to adapt the stack to their hardware, and a certificate can basically only be issued for a specific product. Hence, our release is supposed to initially provide users and other interested parties with two things: firstly, we support manufacturers who are developing safety products, or plan such developments, by making code openly available to them that they can familiarize themselves with, and base developments of their own solutions on, even for their own communication protocols. Secondly, the open source release relieves users of license fees that would otherwise be due. Of course, we offer our services to manufacturers as well.

What kind of services do you actually offer in this regard?

Schlegel:
Generally speaking, in order to comply with the standard, any development of safety-oriented hardware and software must observe the applicable IEC 61508 requirements, which makes the matter somewhat complex. It is guided by the systematics of the V model. One might say that the V model can, as a rule, be used as a blueprint for approaching the entire safety development process; it applies a structure of recurring cycles of analysis, development, validation, and extensive documentation. Besides these procedures, a Functional Safety Management System (FSM) must also be established. For SIL3, the Functional Safety assessment including the development process and FSM should be conducted by an independent organization (e.g., TÜV). Hence, manufacturers seeking to implement a product in compliance with the IEC 61508 standard on Functional Safety need a great deal of methodological skills as well as adequate qualifications. In order to facilitate that and to speed it up, we offer our range of services, including a hands-on introduction to POWERLINK Safety and the implementation of the openSAFETY stack, and services for the creation of systems and deployment concepts, and development and certification services for customized, IEC 61508 compliant hardware and software, and additional support and maintenance services.

If I am interested in your POWERLINK Safety stack, where do I get it? Will IXXAT make it available on Sourceforge.net?

Schlegel:
No, at least not with the first step we take. Again, this is due to legal issues and user safety issues. We will provide the stack on the IXXAT website for download free of charge, but tied to a registration, so we can notify users of any changes as they happen via
What does the free availability of the stack mean for manufacturers and for IXXAT?

Schlegel:
For manufacturers, openSAFETY is a basis for implementing safety systems and components that is delivered free to their doorstep. However, every manufacturer of safety technology will have to make some adaptations so the software fits their hardware. For these necessary adaptations, manufacturers may choose to take these on themselves, or to make use of services offered by IXXAT. Besides that, we are, of course, not only a software provider; our range of services includes customized hardware developments as well as the supply and maintenance of customer-specific series products. Manufacturers without intimate experience regarding safety matters may find it much more economical to commission an external service provider like IXXAT for complex developments. The Safety open source release simply gives manufacturers in the industry more room to maneuver.

And you benefit from that?

Schlegel:
The bottom line is that we will, of course, also benefit from the increasing proliferation, and will gain more exposure as a competent partner for technology relevant to safety. For quite some time, we have already been having a similar experience with CANopen. Obviously, we have grown up in the CAN world, and our experience in this field has been that an open standard is a boon to all, and enables market growth. While we do not want to be dogmatic about it – we also provide a wide range of other industrial Ethernet-based communication systems –, we do consider POWERLINK and its potential for high availability networks and safety applications to be an ideal complement to CANopen. Moreover, POWERLINK Safety also works in CAN networks.
Liability for safety open source?

As in other areas, the use of open source software has become an everyday practice in the automation industry. For all the benefits comprehensive licensing may have for users, it does, on the other hand, leave software manufacturers faced with the question of the extent of their liability whenever they provide developments under an open source license, such as the GNU General Public License (GPL). Do any additional liabilities arise for implementations that make a claim to provide special safety standards, e.g. because they are supplied with suitable safety certificates?

In order to understand legal liability as it pertains to the use of open source software, one must be aware that the scope of liability is not tied to the nature of the licensing model, but rather to the actual distribution model. As a rule, liability for software therefore applies regardless of whether conventionally licensed, so-called proprietary software or an open source program is used. Anyone selling products that operate with the help of open source software is liable to buyers of these to the same extent as to users of proprietary software; since the customer pays for a product as a whole, he may expect a working system irrespective of whether contractual or non-contractual software defect reports and establish a means to contact the acquirers to pass any relevant notifications on to them. However, a general obligation to remit, but should also enable software distributors to monitor their products. This includes information requirements as regards defects of the software that become known as well as an obligation to take measures that depend on the scale and scope of the danger and on other individual circumstances, e.g. the safety relevance and the price of the software, as well as on knowledge about technical workings. The information requirements pertain to the collection and examination of customer complaints – software manufacturers may therefore not close their eyes to problems. Hence, a download service should not only provide the open source software itself, but should also enable defect reports and establish a means to contact the authors faced with the question of the extent of the user rights for a product as a whole, he may expect a working system irrespective of whether conventional or non-conventional software licenses are liable to any lesser extent than distributors who include such programs in products for commercial distribution. This also applies to open source software on which users bestow particular trust due to a safety certificate. Safety certificates do not lead to an expansion of the grounds of liability – i.e. whether liability must be assumed for negligent acts or only for intentional misrepresentations –, but solely have an impact on what can be considered a software defect. If a software buyer can expect particular safety features due to public statements of the seller about the software at hand or designated certificates for it, the presence of a software defect can be assumed if the software does not meet the expectations regarding safety. In this case, the seller must provide compensation for any damage that results from intentional or negligent conduct causing a failure to meet the safety level, while the grantor of a license for a gratuitous offer is only liable for immediate damage caused by intentional misrepresentations, and for so-called consequential damage to other legally protected interests if such damage is caused by gross negligence.

Dr. Till Jaeger is a partner at JBB Rechtsanwälte in Berlin, a law firm specializing in intellectual property protection issues and focusing on counseling corporate clients from the IT industry. In 2000, he co-founded the Institute for Legal Issues of Free and Open Source Software (iF+OSS), which provides an academic perspective on legal issues concerning open source software and intellectual property legislation. Till Jaeger is an accredited IP law and media law specialist and co-author of the standard work, “Open Source Software – Rechtsfragen der Freien Software” (Open Source Software – Legal Issues in Free Software).
What do manufacturers of Safety devices need to consider?

Manufacturers seeking to develop products that comply with the IEC 61508 standard on Functional Safety in electronics face much more demanding requirements than those for technical expertise alone. The development of safe devices is a management task that calls for highly qualified staff with a range of advanced methodological skills.

Given its extensive obligations regarding documentation as well as proof of extensive analyses and validations, IEC 61508 constitutes a management challenge with repercussions throughout the company. The Safety Integrity Level (SIL) is often mistaken for a plain device predicate. However, the IEC 61508 standard applies to the entire safety lifecycle of a product – from its conceptual design, to planning and development, to implementation, software and hardware testing phases, and the validation of the system as a whole, with a view to their timing and level of detail, which yields a diagram featuring a V-format for the sequence of discrete steps. The particular methods and tools employed depend on the SIL level to be achieved, which calls for highly qualified developers with a range of advanced methodological skills.

One mistaken often made is e.g. the separate development of safety-related and not safety-related parts of a system, when it is indeed imperative to define the safety requirements for every single component at the outset. Much in the same vein, the overall effort must be monitored continually, and there must be running assessments at all times as the project proceeds, lest expenses for incidental remediation become unnecessarily high. Inexperienced developers often expect auditors to provide precise instructions for remediation – but to no avail, for an auditor will only check whether a system complies with the standard or not. The only means to come to grips with any faults is a design-oriented management scheme that systematically defines measures in every phase of development, and considers the entire safety lifecycle.

In order to identify any faults as quickly as possible, and to comply with the standard at all times in the course of a project, the entire development sequence should adhere to the V model. This project management method aligns all project stages, such as analyses of requirements, the design, implementation, software and hardware testing phases, and the validation of the system as a whole, with a view to their timing and level of detail, which yields a diagram featuring a V-format for the sequence of discrete steps. The particular methods and tools employed depend on the SIL level to be achieved, which calls for highly qualified developers with a range of advanced methodological skills. It has become clear that Functional Safety developments impose demanding requirements on management as a whole. Manufacturers lacking extensive experience in these matters are well advised to turn to specialized service providers. The additional expenses can be compensated to some degree by using the free and openly available protocols openSAFETY and openPOWERLINK, which relieve manufacturers of a great portion of the development effort for data communication solutions.

■ Functional Safety Management

A “proven-in-use” approval is not possible for new developments. The procedural steps mandated by the IEC 61508 standard must therefore be defined and established as binding by a development department. At first, the existing hardware and software of the devices must be analyzed with respect to the planned safety function. Small changes to the hardware will usually suffice, and sometimes some existing software portions can be kept as well. A lack of experience regarding the interpretation of the complex standard, as well as pertaining to audit and certification procedures, often make it hard to achieve the goal. Insufficient systematics of the working process and an insufficient definition of procedural steps also add to these complications.

■ Avoid systematic faults, keep accidental faults in check

The extensive documentation that accompanies the project is not the only cause for considerable effort. Contributing factors also include risk analyses, analyses of the implications of changes, and validations that conclude every development step in order to rule out any systematic faults. However, accidental faults cannot be eliminated in this way, but do instead require an analysis of the probability of failure as well as a deployment of tools for system diagnostics. A dedicated Safety Manager must assume responsibility for monitoring all activities based on a safety plan.

■ Structuring software development: the V model

In order to identify any faults as quickly as possible, and to comply with the standard at all times in the course of a project, the entire development sequence should adhere to the V model. This project management method aligns all project stages, such as analyses of requirements, the design, implementation, software and hardware testing phases, and the validation of the system as a whole, with a view to their timing and level of detail, which yields a diagram featuring a V-format for the sequence of discrete steps. The particular methods and tools employed depend on the SIL level to be achieved, which calls for highly qualified developers with a range of advanced methodological skills. It has become clear that Functional Safety developments impose demanding requirements on management as a whole. Manufacturers lacking extensive experience in these matters are well advised to turn to specialized service providers. The additional expenses can be compensated to some degree by using the free and openly available protocols openSAFETY and openPOWERLINK, which relieve manufacturers of a great portion of the development effort for data communication solutions.
FACT 6: 300 PERCENT APPROVED

100 % safe with POWERLINK Safety
100 % secure due to separate domains
100 % reliable due to High Availability services

POWERLINK safety implements integrated TÜV-certified safety up to SIL 3. Its clear distinction between real-time and non-real-time communication ensures maximum machine safety and reliability. POWERLINK thus perfectly safeguards your equipment and your investments. www.ethernet-powerlink.org