White Paper

FreelanceSafe
Safe data transmission in the Freelance System up to SIL 3 requirements

Plant operators often implement safety-related functions separately from the process control system, because their certification in accordance to safety standards such as SIL 2 is cost-intensive. The FreelanceSafe data interface avoids this hardware and programming effort by enabling fail-safe data transmission between the control station and the safety controller via SIL-certified software, thus increasing the flexibility of the systems.

This white paper presents a solution approach based on ABB's Freelance control system and subordinate safety-programmable logic controlers (S-PLC) that offers the convenience of end-to-end operation of a safety system. The solution allows the observation and operation of a safety application within the standard Freelance visualization level “Freelance Operation”. In addition to the ease of operation, the consistent report structure is also a benefit. The established standard technology of the S-PLC can be retained. The described solution is an excellent cost-effective and easy-to-maintain alternative, even for new installations.

Typical deployments and uses of safety applications

When using a distributed control system (DCS) for operating and observing the process and for monitoring and managing the safety-relevant control and regulation systems, a separate safety system is usually used exclusively as a shutdown system.

Experiences with a process control system and a separated safety PLC in a production demonstrate, that for large sections one or more control tasks have to be reproduced not only in the control system, but also in the safety control. Not only is this a constant duplication of programming effort, it also makes it difficult to find errors in order to synchronize the coordination of processes in the safety PLC and the control system.

This increased coordination effort continues when the control and monitoring of the plant has to work with new parameters (e.g. safety-related limit values) due to a product change. Inputs at the operator station of the DCS that have an effect on the control sequence in the safety control system are not permitted. Therefore, an additional hardware effort is necessary.

Furthermore, the typical older safety applications are implemented and operated without a visualization level. Here, only error messages are linked to any visualization systems and displayed as notifications.

These planned safety applications run completely autonomously and are independent of the process control system in terms of operation.

New operationg philosophy for safety applications

FreelanceSafe now offers the possibility to manage safety applications and to control them during operation. This new philosophy means a data interface which can be used to operate the safety applications from the Freelance control system software “Freelance Operation”. This new SIL-certified software ensures that a safe data transmission takes place between the operator station and the S-PLC. A so-called "gray" communication channel is provided for the operation of a safety application.

The communication between the operating station / controller and the S-PLC is managed and monitored by this interface. Malfunctions and errors which have occurred on the data path, e.g. due to electromagnetic interference, and influence the data integrity, are detected with the highest possible probability. This provides the overall system with an SIL3 level.

The aim of such a solution is to enable users the ability to operate and adapt their safety installations with existing Freelance DCS systems during the ongoing operation.

Functionality oft he secure data transmission

To enable the processing of the data, binary and digital signals must be generated in the DCS and transmitted to the S-PLC. The transmission of both signal types are based on the following functionality. The user starts the execution of the transmission by selecting a faceplate in the operator station. Via specific signal transmission paths, the data is sent to the S-PLC as well as to the DCS controller and checked for syntax and other operating errors. If both controllers detect no errors, an approval instruction is transmitted from the S-PLC to the DCS. Afterwards, the DCS generates a polynomial and sends it to the S-PLC. This polynomial is a data word which is composed of several pieces of information that are necessary for the transmission. In the S-PLC, the failure-free transmission of the polynomial data is checked by complex data evaluations, and if it is indeed failure-free, it is sent back to the DCS. The controller of the DCS verifies this feedback with the same evaluations. Are the data packages generated by the operator during selection identical to those received by the DCS after evaluation of the feedback, then the data transfer was error-free.

Parallelly to the entire data transmission, the same procedure is performed on another communication channel with the two's complement of the polynomial, so that the polynomial values of both communication channels are compared with each other.

Due to the complex verification mechanisms, it is ensured that errors are detected during data transmission. All control and status words, as well as discrete control commands, are exchanged between the controllers in up to three channels.

Figure 1: Binary signal input

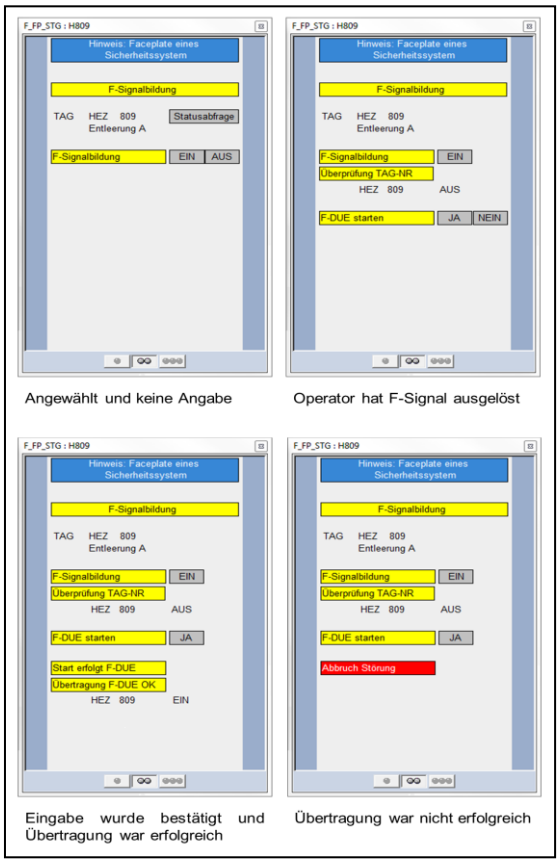
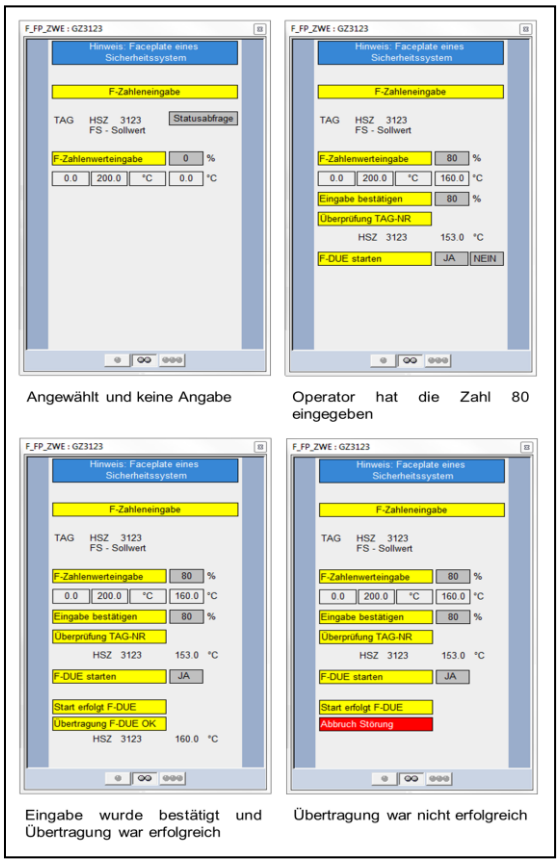


Figure 2: Digital number input



Advantages of FreelanceSafe

Compared to the conventional handling, no further settings are required. This means that the user does not have to learn any additional system software, there is no need for any training, etc. The user can continue working with the existing devices and systems. Neither does the software require an additional system, and the limit value amplifiers are no longer required for the hardware. This has the advantage that neither a new setting of the limit values nor a subsequent function check is necessary.

This is associated with time savings during operation and thus a gain in production time, which increases the productivity of the plant enormously. The increase in safety is also decisive for the user.

In addition to the mentioned advantages, there is the possibility to further optimization of the process. The entire data is now available at the control station and can be managed.

- The responsible persons are still using familiar systems
- Teams can now use the same "language"
- No further training is needed to introduce a new system
- The application is familiar and changes can be implemented quickly
- The application can now be operated

Cost savings

Batch processes are an established term in process industries for a special case of discontinuous production. This means that different production steps have to be processed strictly one after the other. These batches can be started several times a day if necessary, possibly also with different input materials. This implies that production has to run with different process variables and therefore also with different safety limits.

The way in which changes to safety functions, e.g. to limit values, must be carried out, is precisely regulated in the "Life cycle of the safety management system" of IEC 61508.

Finally, a complete functional test of the safety loop with all its organizational activities is required.

Example assumption:

A batch process, that is started on average twice per working day with changed input materials. Due to the new batch, the limit values of five safety loops must be changed.

Process	Saving
Modification of a limit value	10 minutes
Function check of a limit value	20 minutes
Modification of the five safety loops	5 x 30 minutes = 150 minutes = 2,5 hours
Two adjustments of the batch per day	2 x 2,5 hours = 5 hours
Hourly rate of 50 € Cost per working day	5 hours x 50 €/h = 250€/d
200 production days per year	200 days x 250 €/d = 50.000 €

The investment costs must be differentiated according to whether a DCS system with a S-PLC is already available or whether a system must be installed. In this case, there may be one-off costs ranging from €10,000 to €28,000.

Savings due to increased production times, savings in energy consumption, etc. are not taken into account in the listing.

Linking options

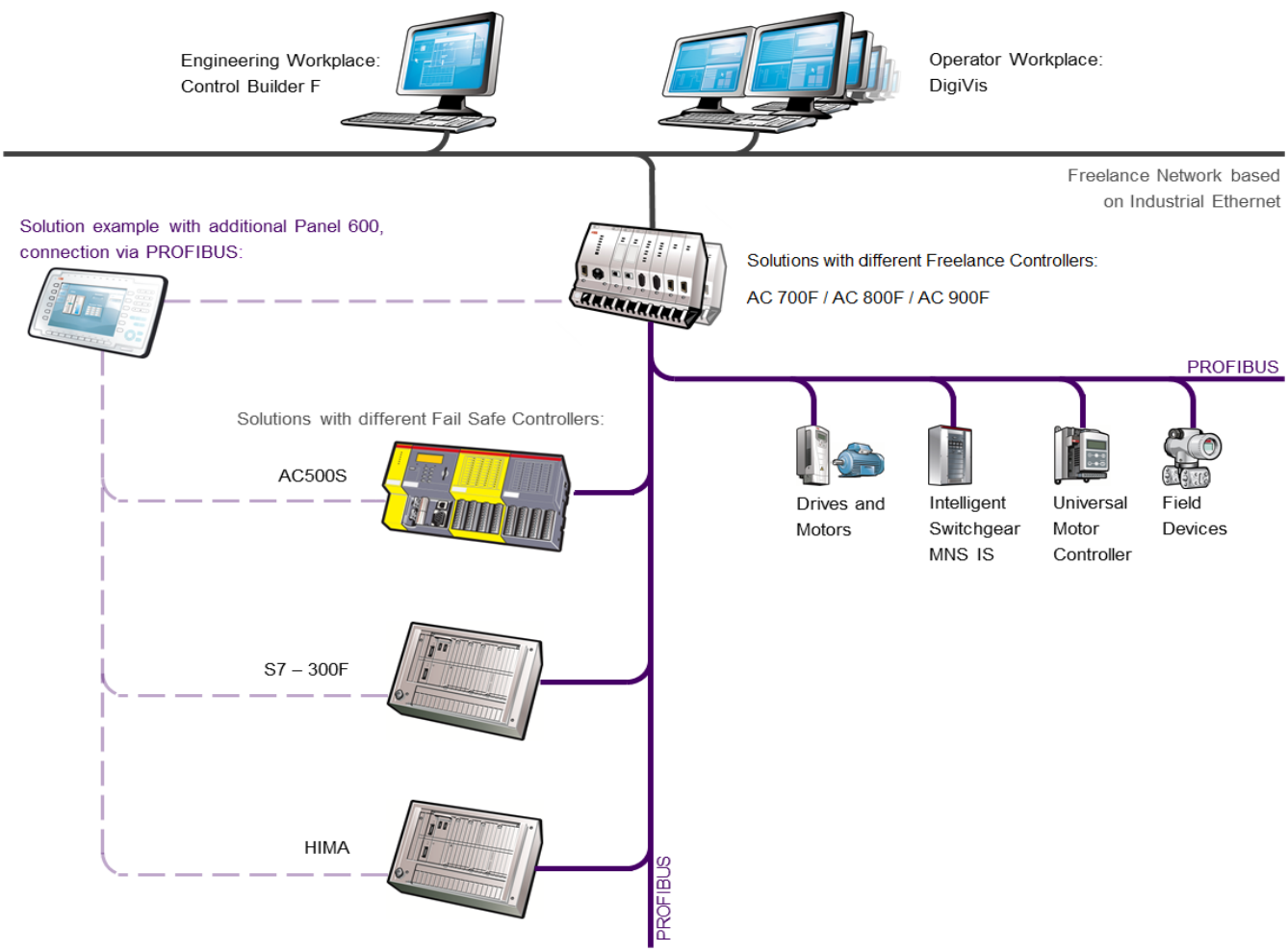
In the topology of couplings for the safety-related data transmission, the Freelance DCS system, consisting of the Engineering Station “Freelance Engineerung”, the visualization software “Freelance Engineering” and a controller, is connected to S-PLC’s from other manufacturers via Profibus / Modbus RTU / Modbus TCP. This topology shows a lean possibility to certify existing S-PLCs with a standard Freelance system as SIL3. For this purpose, an additional software package must be installed in the Freelance system and on the engineering stations of the S-PLCs, which guarantees a safe connection with a SIL3 level.

Currently Fail Safe controllers from ABB, Siemens and HIMA are possible.

The S-PLCs are configured via the standard engineering connection using their own engineering software. The engineering software packages are not displayed in this figure. If required, visualization panels can be used to illustrate the application, in our example ABB Panel 600. The visualization panels represent a further independent possibility to make the application available to the user, outside the operating room. Usually they visualize only partial masks of a main application. The main application is displayed as usual in the visualization station in “Freelance Operations”. This way, users can observe and operate the safety application and its limit values in the Freelance system.

To ensure continuous use of the process, FreelanceSafe can also be used in high-availability mode. In this case, two Freelance controllers are operated redundantly with the respective S-PLCs.

Figure 3: Topology of connection options



Description of the certified libraries

The functional safety of the data transfer from a non-safety-related to a safety-related control system is implemented by safety functions mainly in the software.

For this purpose, a fail-safe application block F_DUE is available for the user. This can be placed anywhere in the user safety program and has to be parameterized simply according to the user specification.

Additional fail-safe modules for the development of binary and digital control signals, for safety-related data transmission, for error detection and error reaction are already integrated in this application module.

This ensures that failures and errors are detected and appropriate reactions are initiated, which keep the fails-safe data transmission in or transfer it to a safe state.

How to install the software?

The necessary modules are implemented into an existing project via import/export or sets up on a exiting, predefined project. The user decides which method of copying is more advantageous. A detailed description of the procedures can be found in the manual.

Settings of the systems Siemens und Freelance

Safety-related systems have to transform the process into a safe condition within a required time frame, before people or the surroundings are endangered. For a correct estimation of the time frame, the information flow from the activation of sensor A to the corresponding reaction of actuator B must therefore be analyzed. This maximum permissible reaction time is largely hardware-specific according to the safety controller used. The safety-related data transfer (data transferred from the operator station to the SSPS) extends the cycle time by about 3-4 ms on average and is negligible compared to the cycle times of a user program (>200ms).

The Freelance and Siemens systems are thus still parameterized using their engineering tools as in a standard project and no further settings have to be made when using the new safety software..

Explanations of possible FreelanceSafe use-cases

With the use of the of safety-related FreelanceSafe libraries and thus ensure data transmission from DCS to a safety system, the control of automated production operations through consistent digital communication from the DCS to the field device gains flexibility and saves operating costs..

Now, safety-relevant instructions (setpoint and control inputs, execution commands, etc.) from an user and automatic switching of safety-relevant limit values from the controller of the process control system (from the operator station via the controller) reach the safety-related application. Manual changes of the safety-relevant limit value settings with subsequent timeintensive function testing are no longer necessary. In addition, the safety-relevant sensors can be acquired directly on site via safety-related remote I/O modules and transferred to the S-PLC by a safety-related field bus (Profisafe). In the control system, the sensors are monitored, checked according to the process requirements and safety-relevant output signals are generated. These are again transmitted via the safety-related fieldbus (Profisafe) directly to the actuator block in order to activate the process protective functions. Simultaneously, the current state variables of the sensors, the results of the monitoring of the sensors, etc. are transmitted via the standard Profibus to the control unit of the process control system. Here, information can be generated which enables the operator an optimal control of the process. The initiation of a process protective function is provided with the current time stamp in the safety-related control system and transmitted to the process control system (BPCS). Now an alarm can be activated in the control station in chronological order.

Information about the Safety Certificate

The highest possible probability of detecting errors during data transmission, including the formation of the signals to be transmitted at the operating station, has been examined and tested by TÜV Rheinland and confirmed and certified by the certificate for SIL3.

Figure 4: Certificate secure data transmission with Siemens SIMATIC S7-300

TÜVRheinland®

ZERTIFIKAT
CERTIFICATE

Nr.: 968/EL 907.01/13

Prüfgegenstand	Sicherheitsgerichtete Softwareparametrierung - Bildung und Übertragung von binären und digitalen Signalen von einer SPS zu einer S-SPS	**Zertifikats-inhaber**	ASIA Industrieautomation GmbH Seestraße 18 68775 Ketsch Germany
Typbezeichnung	FSDUE-V 01A1308 (Bezeichnungen und CRC der Funktionsbausteinen siehe Anhang des Berichts)	**Hersteller**	wie Zertifikatsinhaber
Prüfgrundlagen	IEC 61508 Parts 1-7:2010 (auszugsweise) EN ISO 13849-1:2008 + AC:2009 (auszugsweise) EN 62061:2005 (auszugsweise) IEC 61511-1:2003 + Corr. 1:2004 (auszugsweise)		
Bestimmungsgemäße Verwendung	Das System, bestehend aus verschiedenen Funktionsbausteinen, ist geeignet, sicherheitsbezogene Parametrierung für eine SIL 3 Umgebung nach IEC 61508, IEC 61511 und EN 62061 sowie nach EN ISO 13849 PL e durchzuführen.		
Besondere Bedingungen	Die Hinweise in dem zugehörigen Handbuch sind zu beachten.		
	Dieses Zertifikat ist gültig bis 04.04.2018.		

Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht-Nr. 968/EL 907.00/13 vom 04.04.2013 dokumentiert sind.

Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen. Es wird ungültig bei jeglicher Änderung der Prüfgrundlagen für den angegebenen Verwendungszweck.

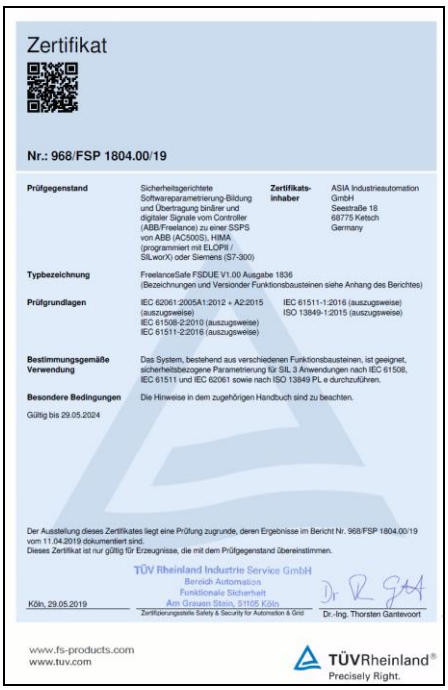
TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 19.04.2013

Zertifizierungsstelle für FS-Produkte

Dipl.-Ing. Stephan Hilb

Figure 5: Certificate secure data transmission with Siemens, ABB and HIMA



Zertifikat

Nr.: 968/FSP 1804.00/19

Prüfgegenstand	Sicherheitsgerichtete Softwareparametrierung-Bildung und Übertragung binärer und digitaler Signale vom Controller (ABB/Freelance) zu einer SSPS von ABB (AC500S), HIMA (programmiert mit ELOP II / SILworX) oder Siemens (S7-300)	**Zertifikats-inhaber**	ASIA Industrieautomation GmbH Seestraße 18 68775 Ketsch Germany
Typbezeichnung	FreelanceSafe FSDUE V1.00 Ausgabe 1836 (Bezeichnungen und Versionder Funktionsbausteinen siehe Anhang des Berichtes)		
Prüfgrundlagen	IEC 62061:2005/A1:2012 + A2:2015 (auszugsweise) IEC 61508-2:2010 (auszugsweise) IEC 61511-2:2016 (auszugsweise)	IEC 61511-1:2016 (auszugsweise) ISO 13849-1:2015 (auszugsweise)	
Bestimmungsgemäße Verwendung	Das System, bestehend aus verschiedenen Funktionsbausteinen, ist geeignet, sicherheitsbezogene Parametrierung für SIL 3 Anwendungen nach IEC 61508, IEC 61511 und IEC 62061 sowie nach ISO 13849 PL e durchzuführen.		
Besondere Bedingungen	Die Hinweise in dem zugehörigen Handbuch sind zu beachten.		
	Gültig bis 29.05.2024		

Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. 968/FSP 1804.00/19 vom 11.04.2019 dokumentiert sind.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 29.05.2019

Zertifizierungsstelle Safety & Security for Automation & Grid

Dr.-Ing. Thorsten Gantevoort

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Which components are certified for FreelanceSafe:

	Process Control System		
	AC 700F	AC 800F	AC 900F
Software			
Operating station	Freelance Operations Version 2013	Freelance Operations Version 2013	Freelance Operations Version 2013
	or	or	or
	Freelance Operations Version 2016	Freelance Operations Version 2016	Freelance Operations Version 2016
Engineering Tool	Freelance Engineering Version 2013	Freelance Engineering Version 2013	Freelance Engineering Version 2013
	or	or	or
	Freelance Engineering Version 2016	Freelance Engineering Version 2016	Freelance Engineering Version 2016
Hardware			
Central unit (controller)	PM 783F: RAM: 2 MB S-RAM Program memory (battery buffered): 2 MB SRAM Internal memory 8 MB SDRAM, 4 MB FLASH ROM	PM 802F: RAM: 4 MB S-RAM for the application with battery buffering	PM 902F: RAM: 8 MB SRAM Battery buffering 16 MB DDR-RAM
		or	
		PM 803F: RAM: 16 MB SD-RAM for the application with battery buffering	
Interfaces	CI 930F: Profibus-DP-Module	FI 830F: Profibus-DP-Modul	CI 930F: Profibus-DP-Modul
	or	or	or
	Modbus RTU (onboard serial)	FI 820F: Modbus RTU	Modbus RTU (onboard serial)
	or	or	or
	Modbus TCP (onboard ETH)	EI 803F: Modbus TCP	Modbus TCP (onboard ETH)

The usage of a Freelance AC 800F controller with CPU PM 802F is only possible for small application sizes. Operation in high availability mode is not permitted for the AC 700F and the AC 800F, CPU PM 802F.

	Safety-PLC (1)	
	ABB AC 500S	Siemens SIMATIC S7-300
Software		
Engineering Tool		Simatic Software Automation License Manager Professional, Version V5.0 + SP1,
	ABB Automation Builder Version 2.x	Simatic Software Step 7 - 2010 - Professional, Version 5.5
	CoDeSys	Simatic Software S7 Distributed Safety Programm, Version V5.4+SP5
Hardware		
Central unit (S-PLC)	**PM 5xx** + **SM 560-S:** Program memory Flash EPROM and RAM: 1 MB Integrated data memory: 1 MB of which 120 KB stored	**CPU 315F-2 PN/DP:** Main memory: 512 KB 1. Interface MPI/DP 12MBIT/S 2. Interface ETHERNET PROFINET,with 2 PORT SWITCH, MICRO MEMORY CARD required
		oder
		CPU 317F-2 PN/DP: Main memory : 1,5 MB 1.Interface MPI/DP 12MBIT/S, 2. Interface ETHERNET PROFINET, with 2 PORT SWITCH, MICRO MEMORY CARD required
		oder
		CPU 319F-3 PN/DP Main memory : 2,5 MB 1. Interface MPI/DP 12MBIT/S 2. Interface DP-MASTER/SLAVE 3. Interface ETHERNET PROFINET, MICRO MEMORY CARD required
Interfaces	In Terminal-Base TB 5x1-ETH integrated (Profibus DP Slave, Modbus RTU, Modbus TCP)	CP 342-5 Profibus-Slave-Interface

	Safety-PLC (2)	
	HIMA HIMatrix	HIMA HIQuad
Software		
Engineering Tool	SILworX Version 6.48.0 - 12.28.0	ELOP II Version 5.1
Hardware		
Central unit (S-PLC)	**F1, F2, F3**	**H41q**
	or	or
	F20, F30, F31, F35	**H51q**
Interfaces	Profibus DP	Profibus DP
	or	or
	Modbus RTU	Modbus RTU
	or	or
	Modbus TCP	Modbus TCP

It should be added that in general any safety-oriented controller and any fieldbus can be used with FreelanceSafe, since the safety procedures are separated from the hardware and are implemented via the black channel principle. Hence, safety PLCs and fieldbus systems that have not been certified so far can also be certified.

How to get the software?

To establish the TÜV certified data transmission from Freelance DCS System to a S-PLC, function blocks are required. The libriarie, which contain these function blocks as well as the required license can be ordered from:

ASIA Industrieautomation GmbH
Seestraße 18
68775 Ketsch
Phone: +49 6202 / 760 226 0
E-Mail: info@asia-industrieautomation.de

About ASIA Industrieautomation GmbH

ASIA Industrieautomation GmbH was founded on 11/01/1989 by the current managing director Dipl.Ing. Hubert Ganshorn in Ketsch at the Rhine and is a progressive and innovative company in the field of functional safety and control and automation technology.

In more than 30 years of existence, ASIA Industrieautomation GmbH looks back on a wide range of worldwide reference projects in various industries, such as Oil & Gas, Power, Burner, Railway, Automotive, Factory Automation, Chemistry, Robotics, Amusement Rides and Port Logistics.

The development of integrated industrial control systems is one of the main tasks of our highly qualified employees. Planning and projecting in the electrical field with CAD/CAE systems are the basis of each assignment, which we solve individually for our customers. We are specialized in the development of user programs and visualizations for control and process control systems of different manufacturers in the automation technology. Our know-how for TÜV-approved safety controls up to SIL3 or PLe makes us a specialist in programming of safety-related control processes. Our customers can rely on the TÜV Rheinland certified qualification of our Functional Safety Engineers.

We support our customers in all required areas and situations by providing consulting, analysis, project planning, development, delivery and installation of the requested systems in the low current area up to commissioning and process optimization.

ASIA Industrieautomation GmbH can rely on a valuable network of cooperations with partner companies, as well as the departments of some renowned universities in Europe. In this course, ASIA Industrieautomation GmbH is encouraged by the Federal Ministry for Economy and Energy due to a decision of the German Parliament.

Close business contacts with many well-known companies and strict compliance with the terms of delivery and acceptance are a sign of the efficiency of the company, as well as proof of the quality of the provided services, and manufactured products.

What services ASIA can offer

Consulting, Project management	– Project management for all project phases – Temporary management
Safety engineering	– Risk assessment – Development of measures for risk reduction – Tasks of the safety management
Conception in the early project phase	– Inventory – Acquisition oft he target conception – Examination of variants – Specification of the target
Automation solutions	– Control engineering – Extension of old installations – Modernization of installations – Consulting to realization
Special control concepts	– Optimizations – Imrpoving efficiency – Tricky tasks
Implementation of concepts in concrete execution documents	– Specifications for the preparation of circuit diagrams – Selection, dimensioning and parameterization of technically suitable electrical equipment – Correspondence with potential suppliers – Technical calculations – Economic selection of equipment – Preparation of mass scaffolds and bills of quantities
Determination of suitable sensors (measuring points) in coordination with process engineering	– Processing of P&I diagrams – Development of the measuring point, consumer and cable lists – Selection and parameterization of technically and economically suitable field devices – Installation supervision – Commissioning

ASIA Industrieautomation GmbH

Seestraße 18
68755 Ketsch
Phone: +49 6202 / 760 226 0

Post adress:
Post office box 1114
68775 Ketsch
E-Mail: info@asia-industrieautomation.de

www.asia-industrieautomation.de

ABB Automation GmbH

www.abb.com/freelance
www.abb.com/controlsystems