Dräger

ST-1220-2007

Functional Safety and Gas Detection Systems

Safety Integrity Level – SIL

DETECTION

Dräger. Technology for Life®

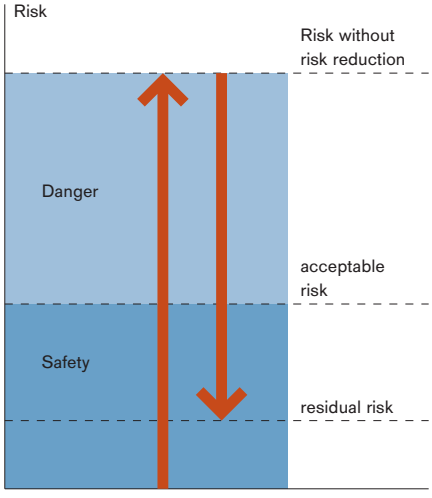
Safety Instrumented Systems are used to reduce the risk for the protection of people, plants, and environment.

Depending on the way a process is designed and what kind of dangerous goods (especially gases and vapours) are involved, industrial plants might pose a high risk to persons, property, and environment. In order to reduce the risk arising from those plants it might be necessary to automatically activate safety measures to avoid dangerous situations.

Depending on the acceptable risk the required reliability of protection systems can be ensured by employing the effective measures of
– failure avoidance,
– failure detection, and
– failure tolerance

This to a degree depends on the actual risk, the so-called Safety Integrity Level.

For gas detection systems, which have to activate safety relevant countermeasures in case of pre-defined gas concentrations, an important question comes up: What is the probability of failing to perform the required countermeasure (safety function) in case of a demand from the process (means when pre-defined gas concentrations have been exceeded) if an undetectable dangerous failure has occurred?



Risk assessment.
A process is assumed to be safe if the actual risk is decreased below the level of the acceptable risk by means of risk-reducing measures. Always a residual risk remains. If risk-reduction is performed by technical measures the term in focus is functional safety.

So, during development and design of devices and subsystems of safety relevant systems the main target is to keep the probability of failure as low as possible (failure avoidance), or to detect failures by diagnostic functions (failure detection) and – in case of a detected failure – to force the safety system to go into a safe state (failure tolerance).

Risk analysis
Depending on the extent of threat to persons, property and environment there are four different classes of risk. Generally a risk is a combination of the consequence to be expected and the probability of occurrence of such an unwanted hazard.

To classify the actual risk structured methods are used, e.g. the risk graph. The risk graph is based on four different consequence categories, and the probability aspect is implemented by the criteria “frequency of exposure of persons” and the “possibility of avoiding the hazardous event”.

Such risk analysis can only be conducted by highly qualified persons who are familiar with the process-specific conditions. As a result the risk analysis leads to the definition of the necessary risk-reducing measures, combined with the
– definition of the safety function and the
– required Safety Integrity Level

Residual risk
If the functional safety is realized by an electrical, electronic or programmable electronic system (“E/E/PES”), the applicable standard IEC 61508 or EN 61508 requires evidence of the remaining residual risk by identifying the so-called dangerous probability of failure as a measure of the protection system’s reliability.

Failures
Considering the entire operational time no E/E/PES is absolutely free of failures. Always there might be systematic or accidental failures, and wear-out parts need to be considered. However, consumable components are not subject to the SIL-consideration – they have to be replaced ensuring failures caused by consumption shall not occur.

Systematic failures
... are design- or development-failures, which already exist at the time of delivery and which are reproducible (e.g. software failures, incorrect rating or the operation of electronic components outside of their specification). By organizational measures and safety-orientated development procedures, systematic failures, especially software failures, can be minimized.

Accidental failures
... are inevitable characteristic properties of components. They do not exist at the time of delivery, but will occur at any time during operation. Accidental failures are specified by a so-called constant failure rate λ which says that during equivalent time intervals always the same percentage of components will fail. The manufacturer derives this failure rate by means of special stress tests with a large number of components and determines or forecasts the time at which 63 percent of the components have failed. The reciprocal value of the resulting time, the so-called MTTF +

λ is a mere statistical value which however enables engineers to calculate the probability that a failure will occur.

Probability of failure

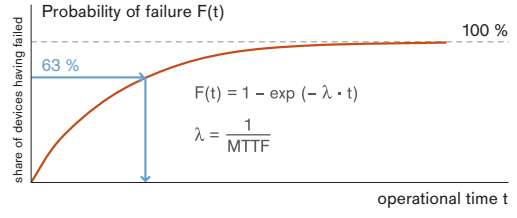
And statistics predict even more: If for example 340 of 1000 equivalent devices have failed after 12 months in operation, then statistics predict a probability of failure of 34 percent for a single device.

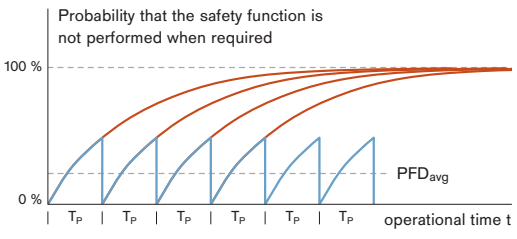
The probability of failure continuously rises with operational time, and at the time of MTTF for a considered device this probability is 63 percent.

Needless to say that this can also be transferred to the safety function: Considering a system which in case of danger needs to perform the safety function, then the probability not to perform the safety function is zero at the time of function test (time 0), and the device is absolutely reliable. But the probability of failure rises continuously, and so does the probability that the safety function will not be performed. However, after having tested the safety function again, e.g. after reconditioning, and the test proved to be successful, then again the probability of failure is zero. So one can reset the probability of failure at regular intervals, because at least at the time of successful proof test of the safety function the system is 100 % reliable!

The average value of the resulting zigzag-curve can be expressed as a number: Multiplying half the proof test interval TP with the failure rate λ leads to the average Probability of Failure On Demand or PFD: $PFD_{avg} = 0.5 \cdot \lambda \cdot T_P$

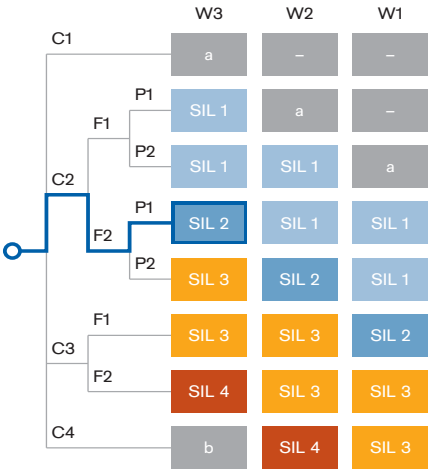
It is called On Demand because although the safety system is continuously in operation a demand to perform its safety function is seldom, say less than once a year. This kind of operation called Low Demand Mode is typical for safety systems in the process industry. If a demand is expected to be more often the plant design engineers should think about the implementation of further protection systems for risk reduction or to keep the process less dangerous by other means.





Probabilities to fail.
The probability of failure of one component or device with the failure rate λ continuously rises during operational time. At the time of the MTTF the probability of failure is 63 %.

The probability of failure that in case of demand the safety function cannot be performed also rises continuously. If however the successful performance of the safety function is demonstrated by regular proof tests, then at the time of test the probability that the system will perform correctly is 100 %, meaning that the probability of failure has been reset to zero with each successful proof test (blue zigzag-curve).



a no special safety requirements
b a single safety system is not sufficient

Risik graph acc. to IEC 61508 / 61511.
Assumed that in case of the unwanted event, and because persons are frequently exposed to the hazardous area (F2), the consequence might be the death of one person (C2) and avoidance of the hazardous event is only possible under certain conditions (P1) and the probability of the unwanted occurrence is relatively high (W3), then the protection system should be at least SIL2-rated.

Consequence (C)
C1 minor injury or damage
C2 serious permanent injury to one or more persons; death to one person; temporary serious damage
C3 death to several people, serious or permanent environmental damage
C4 very many people killed

Frequency of, and exposure time in, the hazardous zone (F)
F1 rare to more often
F2 frequent to permanent

Possibility of avoiding the hazardous event (P)
P1 possible under certain conditions
P2 almost impossible

Probability of the unwanted occurrence (W)
W1 very slight
W2 slight
W3 relatively high

Failures are allowed ...
... as long as the safety system provides a safe condition.

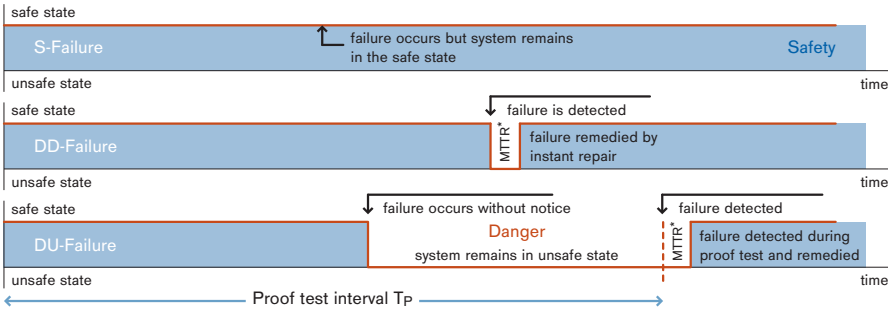
Safety Function

The safety function or Safety Instrumented Function SIF of a gas detection system is to trigger gas alarm if gas concentrations exceed the alarm thresholds. If – in case of failure – the system cannot trigger gas alarms it must go into the safe state.
The safe state of a gas detection system is defined as an action which is equivalent to gas alarm. At least the same measures as for gas alarm are activated, and additionally a fault signal is generated e.g. to ensure maintenance and repair promptly being performed.

But to achieve a safe state at all, failures need to be reliably detectable. This is why the failure analysis (Failure Modes, Effects and Diagnostic Analysis FMEDA) concerning the effects differentiates between detectable and undetectable and between safe and dangerous failures.

Safety-related failures

Surely there is no problem with a failure of type λ_{SD} which signals itself, and moreover



* MTTR = Mean Time To Repair (mostly 8 h)

is not dangerous at all because the safety function can be performed even if this kind of failure occurs. As a system can always achieve a safe state as long as a failure is detectable, any detectable failure (λ_{SD} and λ_{DD}), independent of the fact whether it impacts the performance of the safety function or not, is tolerable.
However, dangerous failures (λ_{DU}), which cannot be revealed by any diagnostic measure, can derogate the entire safety system's concept. They may occur at any time and can only be discovered by regular inspection and proof test. Performing periodical proof tests is the one and only method to discover failures which cannot be revealed by diagnostics, at a stage so early that severe consequences can be avoided with sufficiently high probability.

The DU-failure is in focus

In the statistical mean the DU-failures occur at half of the interval between two tests (proof test interval):
$PFD_{avg} = 0.5 \cdot \lambda_{DU} \cdot T_P$

The proof test interval T_P implies the periodical test of the safety function performed by the customer. Not only the PFD_{avg} must not exceed certain values for a given SIL, but also the Safe Failure Fraction SFF, a measure for the share of tolerable failures, needs to be regarded when designing a safety relevant system with SIL-requirement.

PFD_{avg}	system or subsystem fails once of ... demands	SIL
≥ 0.01 ... < 0.1	11 ... 100	1
≥ 0.001 ... < 0.01	101 ... 1000	2
≥ 0.0001 ... < 0.001	1001 ... 10000	3
≥ 0.00001 ... < 0.0001	10 001 ... 100 000	4

Necessary PFDavg to achieve a given SIL.
To achieve SIL 2, the PFD_{avg} must be less than 0.01, meaning that at more than 100 demands the system in the statistical mean may fail once. For the Low Demand Mode (one demand per year max.) this is equivalent to "the system fails once in 100 years".

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

Safe Failure Fraction SFF.
The SFF reflects the ratio of the share of safe and tolerable failures in proportion to the total amount of failures. The complement 1 - SFF indicates the share of the dangerous undetectable failures which should be as low as possible.

Four failures types to be considered

λ_{SD}	**safe detectable** safe and detectable failure	SIF can always be performed
λ_{SU}	**safe undetectable** safe but not detectable failure	SIF can always be performed
λ_{DD}	**dangerous detectable** dangerous but detectable failure	SIF cannot be performed but system will quickly go into the safe state
λ_{DU}	**dangerous undetectable** dangerous failure, which can only be revealed by proof test	failure occurs without notice and in case of demand the safety system cannot perform the SIF

(SIF = Safety Instrumented Function)

Each safety chain consists of at least three subsystems, they detect, react, and avert.

Subsystems
A safety-relevant system or Safety Instrumented System, SIS, consists of
– sensors (transducers), which make a potential danger detectable and produce an appropriate electrical signal,
– logic controllers, which detect the electrical signal exceeding a given threshold, and
– actuators to perform the safety function.

In the simplest case a SIS is a single channel or linear system, e.g. a gas detection system consisting of gas detection transmitter, central controller unit, and relay. Depending on the subsystem's type (complex or not) the subsystem must feature a certain minimum SFF. If there is no high-complex or programmable electronics the subsystem is mostly considered to be simple or type A.

The HFT (hardware fault tolerance) can be increased by means of the system's architecture. If two sensing elements are operated redundantly, one may fail without affecting the performance of the safety function. As one failure does not impact safety the HFT is 1 in case of redundancy or a 2-out-of-3-voting ("2oo3"). A triple redundancy ("1oo3") will result in an HFT of even 2.

Even if two sensing elements fail the safety function can still be performed. When designing redundancies failures need to be considered which can impair redundancy if both the sensors are affected by the same cause. These are common-cause-failures, mostly only estimated as a share of e.g. β = 1, 2, 5, or 10 % of the DU-failure.

True redundancy without common-cause-failures can only be obtained by diversity, meaning the use of different products, and even of different manufacturers, if possible.

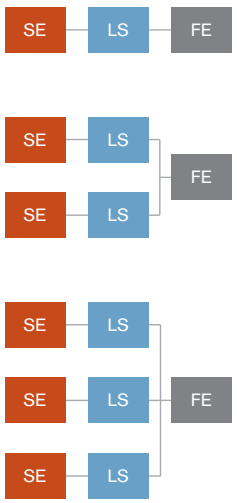
Single channel system (HFT = 0)
By means of a FMEDA each subsystem needs to be assessed concerning its safety-relevant parameters, and when combining three subsystems to an entire system their individual PFD_{avg} have to be added to obtain the PFD_{sys} of the system:
$PFD_{sys} = PFD_{SE} + PFD_{LS} + PFD_{FE}$
where the individual PFDs are the product of half the proof test interval and the DU-failure rate. E.g. to obtain SIL 2 it is necessary to have $PFD_{sys} < 0.01$ and (because the HFT is 0) the individual SFF for complex subsystems must be higher than 90, for simple subsystems higher than 60 %.

SFF (Share of tolerable failures)	HFT for simple subsystems (type A)		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 ... < 90 %	SIL 2	SIL 3	SIL 4
90 ... < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Simple subsystems (type A).
These are e.g. relays, simple sensors, devices with analogue – and to a certain level – also digital electronic circuits.

SFF (Share of tolerable failures)	HFT for complex subsystems (type B)		
	0	1	2
< 60 %	–	SIL 1	SIL 2
60 ... < 90 %	SIL 1	SIL 2	SIL 3
90 ... < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Complex subsystems (type B).
These are e.g. software-based programmable logic-controllers, microprocessor-controlled devices, ASICs, etc.



HFT = 0 Single channel architecture "1oo1"
Only in case of no failure the safety function can be performed.

HFT = 1 Dual redundancy "1oo2" (1-out-of-2) or 2-out-of-3-voting "2oo3"
Even in case of one failure in the sensing elements or logic solvers the safety function can still be performed.

HFT = 2 Triple redundancy "1oo3"
Even in case of two failures in the sensing elements or logic solvers the safety function can still be performed (fault condition to be realized).

SE sensing element, transducer to **detect** a dangerous condition (e.g. sensors, detectors, gas detection transmitters)

LS logic solver, programmable or simple controller to **react** to a dangerous condition, e.g. activate counter measures (programmable logic controllers, computerized systems, signal converters, central controllers of a gas detection system)

FE final element, equipment to **avert** a dangerous condition (in gas detection systems: solenoid valves, electric fans, shut-down-relays, water sprayers and extinguishing systems.)

Different kinds of system architectures and their HFT.

SIL for gas detection systems
Example of a safety chain.

Dual redundancy (HFT = 1)
At first the PFDs of the redundantly designed subsystems have to be calculated and to be introduced as PFD_{SE}, PFD_{LS}, or PFD_{FE} into the equation
$PFD_{sys} = PFD_{SE} + PFD_{LS} + PFD_{FE}$.

Because of HFT = 1 the SFF of redundantly designed subsystems may be less than 90 or 60 % resp. to achieve SIL 2. For non-diverse redundancies always the common cause failures need to be considered, e.g. as 5 %, meaning $\beta = 0.05$.

Redundant subsystem
Using similar products (e.g. gas detection transmitters) to achieve redundancy the PFD is calculated by:

$$PFD_{avg} = \frac{1}{3} \cdot (\lambda_{DU} \cdot T_P)^2 + \beta \cdot T_P$$

Using however different products (with failure rates λ_{DU1} und λ_{DU2}) one achieves diverse redundancy and thus the common cause failure β can be neglected:

$$PFD_{avg} = \frac{1}{3} \cdot \lambda_{DU1} \cdot \lambda_{DU2} \cdot T_P^2$$

SIL-conformity
With the declaration of SIL-conformity a manufacturer of subsystems publishes the essential data necessary to design a safety chain by means of subsystems.

Furthermore there are hints included to indicate under which circumstances the Safety Integrity Level is obtained, which maintenance actions have to be performed (especially if wear parts are included) and how to test the safety function during the proof test procedure.

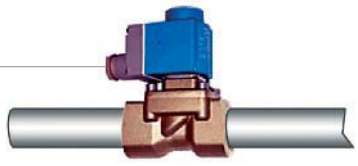
SE – Sensing Element.
The gas detection transmitter **detects** the potential dangerous condition.

Polytron 7000
with sensor
Type B
PFD_{SE} = 1.56E-03
T_P = 8760 h
λ_{DU} = 3.57E-07 h^{-1}
SFF = 90 %

LS – Logic Solver.
The controller **reacts** to the potential dangerous condition and activates countermeasures.

4-20-mA-Module REGARD
incl. REGARD Master Card
Type B
PFD_{LS} = 2.23E-04
T_P = 8760 h
λ_{DU} = 5.10E-08 h^{-1}
SFF = 94 %

FE – Final Element.
The activated solenoid valve **averts** the dangerous condition by closing the gas pipe reliably.



Solenoid valve
(open if energized)
Type A
PFD_{FE} = 5.20E-03
T_P = 8760 h
λ_{DU} = 1.20E-06 h^{-1}
SFF = 68 %

Example of a gas detection system in single-channel-architecture, thus HFT = 0
As the individual SFF for type B ≥ 90 % and for type A ≥ 60 %, and the sum of the three PFD, calculated by PFD_{sys} = 1.56E-03 + 2.23E-04 + 5.2E-03 = 6.98E-03 is less than 0.01, this is a SIL2-rated safety instrumented system if it is operated according to the safety hints of the manufacturers and the proof test is conducted once per year (every 8760 hours).

SIL is not a product's property but a continuous sustaining process - a system's lifecycle.

DRÄGER-TRANSMITTERS FOR THE USE IN SIL2-RATED SYSTEMS AND THEIR "SIL-PARAMETERS"

Transmitter	Measuring principle	SFF at HFT = 0	λ_{DU}	PFD_{SE} for T_P = 1 year
Dräger Polytron IR Type 334	Infrared, for the detection of flammable gases and vapours	96 %	3.00E-08 h^{-1}	1.28E-04
Dräger Polytron 7000	Electrochemical, for toxic gases and oxygen	90 %	3.57E-07 h^{-1}	1.56E-03
Dräger Polytron Pulsar	Open-Path infrared, for the detection of flammable gases	92 %	1.09E-07 h^{-1}	4.77E-04
Dräger PIR 7000	Infrared, for the detection of flammable gases and vapours	94 %	4.70E-08 h^{-1}	2.04E-04
Dräger PIR 7200	Infrared, for the detection of carbon dioxide	94 %	4.70E-08 h^{-1}	2.04E-04

Lifecycle of a SIS

Commonly a SIS is planned, designed, installed and commissioned by experienced system engineers. Just this process requires a high degree of diligence, documentation depth and verification.

During operation a SIS must be serviced according to the manufacturer's guidelines given in the safety operating manual and to be put into quasi-new-condition if necessary. Further on the periodically performed proof test of the safety function must be conducted in the compulsory intervals T_P, and organizational measures must be met to ensure prompt repair and spare part delivery in case of need.

Safety Integrity from Dräger

Not only is Dräger the manufacturer of subsystems such as sensors, gas detection transmitters and central controllers, but also Dräger system engineers can design complete safety related gas detection systems including documentation, SIL-evidence, installation, commissioning, and maintenance.

Our system engineers will competently give advice if safety integrity needs to be implemented in a system's safety concept.

CERTIFICATE

No. Z10 07 10 53474 004

Holder of Certificate: Dräger Safety AG & Co. KGaA
Revalstr. 1
23560 Lübeck
GERMANY

Factory(ies): 53474

Certification Mark:

Product: Safety Related Programmable Electronic System
Infrared Gas Transmitter

Model(s): Dräger PIR7000 type 334/340 (M25) / (NPT) for hydrocarbon
Dräger PIR7200 (M25) / (NPT) for carbon dioxide

Parameters:
Structure - Safety Integrity Level: 1oo1 - SIL2
Measuring range: 0 to 5...100%LEL / 0 to 5...100 Vol.%
Nominal current range:
4 to 20 mA current source or current sink
(automatically selected)
Transmitter failure mode: 0...3.6 mA or > 21 mA
Compliance voltage:
9 to 30 VDC / 13 to 30 VDC (HART)
Operating temperature range: -40° C to +77° C

The report no. DL70901 C is a mandatory part of this certificate.
The product complies with the following listed safety requirements only, if the specifications documented in the currently valid revision of this report are met.

Tested according to:
DIN EN 50271:2002
DIN EN 50402:2006
DIN EN 50402/A1:2007
IEC 61508 1-4:2000, SIL 2

The listed product was tested on a voluntary basis and complies with the relating standards or directives. The certification mark shown above can be affixed on the product. The certification mark must not be affixed in any way. See also notes overleaf.

Test report no.: DL70901 C

Page 1 of 1
Date, 2007-10-25

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstrasse 65 · 80339 München · Germany

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

In respect to its SIL2-capability acc. to EN/IEC 61508 the complete hardware- and software-development of the transmitter Dräger PIR 7000 has been supervised and certified by the German TÜV.

HEADQUARTERS
Dräger Safety AG & Co. KGaA
Revalstrasse 1
23560 Lübeck, Germany

www.draeger.com

SYSTEM CENTERS

P. R. CHINA
Beijing Fortune Draeger Safety
Equipment Co., Ltd.
A22 Yu An Rd, B Area,
Tianzhu Airport Industrial Zone,
Shunyi District,
Beijing 101300
Tel +86 10 80 49 80 00
Fax +86 10 80 49 80 05

GERMANY
Dräger Safety AG & Co. KGaA
Revalstrasse 1
23560 Lübeck
Tel +49 451 882-2794
Fax +49 451 882-4991

FRANCE
Dräger Safety France SAS
3c route de la Fédération, BP 80141
67025 Strasbourg Cedex 1
Tel +33 3 88 40 59 29
Fax +33 3 88 40 76 67

SINGAPORE
Draeger Safety Asia Pte Ltd
67 Ayer Rajah Crescent #06-03
Singapore 139950
Tel +65 68 72 92 88
Fax +65 65 12 19 08

UNITED KINGDOM
Draeger Safety UK Ltd.
Blyth Riverside Business Park
Blyth, Northumberland NE24 4RG
Tel +44 1670 352 891
Fax +44 1670 544 475

USA
Draeger Safety, Inc.
505 Julie Rivers, Suite 150
Sugar Land, TX 77478
Tel +1 281 498 10 82
Fax +1 281 498 51 90

90 46 256 | 04.10-2 | Marketing Communications | PR | LE | Printed in Germany | Chlorfrei – umweltfreundlich | Änderungen vorbehalten |