# Experience with Safety Integrity Level (SIL) Allocation in Railway Applications

Peter Wigger

Institute for Software, Electronics, Railroad Technology (ISEB), TÜV InterTraffic GmbH,
a company of the TÜV Rheinland / Berlin-Brandenburg Group

## Abstract

The paper presents methods for defining Safety Integrity Levels (SIL) for Railroad systems. Methods for determination of risk targets are presented. Experience from a project is given and practical ways to define a SIL are presented.

## 1. Introduction

Probabilistic safety approaches are conquering more and more fields of application in safety technology. Railroad technology is one of these areas. The European Standards prEN 50126 [2], EN 50128 [3], ENV 50129 [4] have introduced the concept of a probabilistic safety approach to railroad technology. In many places, ideas have been taken from IEC 61508 [7]. Section two gives an overview on safety integrity levels in railroad technology and on methods. The third section presents experience with methods for defining safety integrity levels by presenting an example, the assessment of the Copenhagen Metro – a driverless automatic system. Conclusions are drawn in the fourth section.

## 2. Safety Integrity Levels in Railroad Technology

### 2.1 Definition of Safety Integrity Level

In the beginning of railroad technology the goal was to avoid accidents. Methods have been derived, e.g. to avoid braking of rails. Signalling systems have been introduced, to avoid collisions. The philosophy was to have methods, systems and procedures that prevent accidents. Obviously, this goal has never been reached, there were still accidents. The standards prEN 50126 [2] and ENV 50129 [4] have introduced a probabilistic approach into railroad technology. Probabilistic methods have first started in nuclear technology, aerospace technology and control technology. Consequently, a lot of material has been adopted from IEC 61508 [7].

The concept of Safety Integrity Levels (SIL) is a concept of classes of safety requirements for functions, systems, sub-systems or components. A SIL consists of two factors:

- A range of values for a rate of dangerous failures / tolerable hazard rate and
- measures to be implemented into the design during the design process.

A SIL can be assigned to any safety relevant function or system or sub-system or component.

The consideration is as follows. Regarding a safety relevant function or a system / sub-system / component performing a safety relevant function, the risks associated with this function are identified.

Then, a threshold is set for hazardous events that might occur caused by malfunction or failure of function. The threshold is given in the form of a rate, i.e. a probability per time unit.

## 2.2 Methods for Definition of Tolerable Hazard Rates

The figure for the tolerable rate of dangerous failures can be derived using different principles [2].

1. Globalement Au Moins Aussi Bon (GAMAB),

   "All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system."

2. As low as reasonably practicable (ALARP),

   Societal risk has to be examined when there is a possibility of a catastrophe involving a large number of casualties."

3. Minimum endogenous mortality (MEM),

   "Hazard due to a new system of transport would not significantly augment the figure of the minimum endogenous mortality for an individual."

Two of these principles will be explained later on.

Having obtained the rate of dangerous failures / the tolerable hazard rate, a Safety Integrity Level (SIL) is defined according to the following table:

Table1: Definition of SILs (2 Examples)

| Rate of dangerous failures per hour (Example from ENV 50129 [4] | Tolerable Hazard Rate (THR) per hour and per function (Example from prEN50129 [6]) | Safety Integrity Level |
|---|---|---|
| $< 10^{-10}$ | $10^{-9} \leq THR < 10^{-8}$ | 4 |
| $\geq 10^{-10}$ to $0.3\ 10^{-8}$ | $10^{-8} \leq THR < 10^{-7}$ | 3 |
| $\geq 0.3\ 10^{-8}$ to $<10^{-7}$ | $10^{-7} \leq THR < 10^{-6}$ | 2 |
| $\geq 10^{-7}$ to $0.3\ 10^{-5}$ | $10^{-6} \leq THR < 10^{-5}$ | 1 |

The table has to be used in the following way. For a rate of dangerous failures / the tolerable hazard rate, the coinciding class, i.e. the SIL, is searched up in the table. Then, design measures have to be applied during the design process. The design measures to be applied are also given in the standard. In many cases, these design measures are similar to those given by IEC 61508 [7]. Note, that the figures have been modified during the development of ENV 50129 [4] to prEN 50129 [6], as can be seen from the table above.

A very sensitive task is the definition of the tolerable rate of dangerous failures.

## 2.3 The ALARP principle

The ALARP principle is based on frequency classes and severity classes.

Severity classes can be defined as described in table 2.

The frequency classes are usually defined in steps delimited by a factor of 10. An example is given in table 3

Then, three regions are defined for combinations of severities and frequencies:

I: Intolerable risk, either severity or frequency must be reduced.

T: Tolerable risk, should be reduced. However, risk reduction might be stopped when the costs are too high.

N: Negligible, no action is necessary.

Table 2: Severity classes (example)

| Safety Failure Class | Consequence | Severity Class |
|---|---|---|
| Insignificant | Minor injuries | IV |
| Marginal | Major injuries | III |
| Critical | 1 fatality | II |
| Catastrophic | > 10 fatalities | I |

Table 3: Frequency Categories (example)

| Description | Frequency Range (in events per year) | Category Designation |
|---|---|---|
| Frequent | $10^{-1}$ | A |
| Probable | $10^{-2}$ | B |
| Occasional | $10^{-3}$ | C |
| Remote | $10^{-4}$ | D |
| Improbable | $10^{-5}$ | E |
| Incredible | $10^{-6}$ | F |

Table 4: ALARP region (example).

Frequency

| | | | | |
|---|---|---|---|---|
| A | T | I | I | I |
| B | T | T | I | I |
| C | T | T | I | I |
| D | N | T | T | I |
| E | N | N | T | T |
| F | N | N | N | T |
| | IV<br>Insignificant | III<br>Marginal | II<br>Critical | I<br>Catastrophic |

Within the ALARP method, collective risks are considered. That means, always the risks arising from the system to all persons using the system, environment and material values are taken into account.

Starting from the ALARP region, for each technical function, system, sub-system or component requirements for tolerable hazard rates in the different severity classes are derived. It must be shown that the tolerable hazard rates of all functions, systems, sub-systems and components of the overall system meet the ALARP requirement.

The hazard rates are computed by

$$HR(S) = \textbf{Fehler!}. \qquad (1)$$

Here, the following notation has been adopted:

$HR_j$ hazard rate of the j-th hazard,
$C_{jk}$ consequence probability for the j-th hazard leading to accident $A_k$,
$S_k$ Probability of occurrence of an event with the given severity in accident $A_k$,
$D_j$ Duration of the j-th hazard.

This hazard rate still depends on the severity S. Then, for each severity the hazard rate can be computed from the hazard rates of the separate hazards. It can be seen that the hazard rate HR(S) depends on the duration of the hazard and probabilities of occurrence of accidents and events with given severity. All these factors have to be multiplied in order to compute the hazard rate HR(S).

Now, hazard reduction has to take place as long as the HR(S) falls into the “T” (tolerable) region or the “I” (intolerable) region. The process may be stopped in the “T” region if the effort of further hazard reduction is too high.

Resolving (1) for $HR_j$, it is possible to define $HR_j$ for a given threshold value HR(S).The latter can be taken from the ALARP region.

## 2.4 Minimum Endogenous Mortality

The minimum endogenous mortality is based on an individual risk [5]. Consideration starts at the point of the lowest rate of mortality for human individuals. The rate is minimal for a 15 year old individual and reads $2\ 10^{-4}$ per year. From the requirement that a technical system shall not contribute more than 5% it can be derived that a technical system shall not lead to a fatality of a single person at risk with a rate larger than $10^{-5}$ per year. This figure can then be apportioned further to sub-systems.

The risk for a technical system has to be computed by the following algorithm. All hazards in the system have to be identified that can lead to dangerous events as e.g. fatalities. Then, the individual risk of fatality (IRF) is computed as [5].

IRF = **Fehler!**.

Here, the following notation has been adopted:

N number of uses of the system by the considered individual,
HRj hazard rate of the j-th hazard,
$C_{jk}$ consequence probability for the j-th hazard leading to accident $A_k$,
$F_k$ Probability of fatality for the considered individual in accident k,
$D_j$ Duration of the j-th hazard,
$E_j$ exposure time of the individual to the j-th hazard.

Again, several factors are involved into the computation of the risk of a system. Obviously, various probabilities can reduce the hazard rate HRj of the j-th hazard.

## 3. Experience with SIL allocation for the Copenhagen Metro

### 3.1 Introduction

Currently, the new Copenhagen Metro is under construction. This first Danish metro will be an automatic driverless system, in the first project phase connecting downtown Copenhagen with the university, the new fair area and the developing suburb Ørestad on Amager island. Up to 19 trains - consisting of 3 cars each - will travel with a headway of 90 s between 14 stations on a permanent way of 19 km double track. While the system will be operated in downtown Copenhagen as an underground it will run aboveground and even across bridges and viaducts in the Amager area. In later project phases the system will be extended to the north-west of Copenhagen and in the south-east to the international airport.

As Denmark had no legal framework for the approval of systems like the Copenhagen Metro, the Danish Government decided to rely on a proven German approval procedure. In Germany, public tracked mass transit systems fall under the German regulation for the construction and operation of tramways (BOStrab) [1]. This regulation does not only apply to conventional tramway systems - as the title may imply - but also to new, unconventional types of tracked transport systems including fully automatic rapid transit systems. The European Union already stated some years ago that the use of BOStrab does not hinder competition and thus it may be used throughout the countries of the EU.

The German BOStrab regulation requires a strongly regimented approval procedure under the supervision of a Technical Supervisory Authority (TSA). The respective Danish Authority (the Railway Inspectorate Jernbanetilsynet, an authority under the Ministry of Transport) asked for safety assessment by an independent Assessor.

TÜV Rheinland with their competence and experience in the certification of complex, safety relevant systems for railway applications was chosen after the tender phase to play the role of the independent Safety Assessor in the Copenhagen Metro project.

BOStrab calls for compliance with the orders of the Technical Supervisory Authority, and with the "generally accepted rules of technology" (GARTs). These rules consist of standards and regulations that represent the opinion of the majority of the experts in the field of public transport technology.

For the Copenhagen Metro the VDV papers in connection with the new European Standards for Railway Applications prEN 50126 [2], prEN 50128 [3], and ENV 50129 [4] have been assigned to be GARTs for the safety assessment. These standards are supplemented with further fire standards and Danish national standards. All safety activities as well as the generation of the safety documentation are performed according to these standards.

For the complete system a safety case must be assessed. The safety assessment of the Copenhagen Metro includes the assessment of safety function / system / sub-system / component specific allocations of Safety Integrity Levels (SIL), which will be described in the following.

### 3.2 Overall Safety Target for the Copenhagen Metro

For the new Copenhagen Metro it was required, that the risk created by the planned operation of the transport system is As Low as Reasonable Practice (ALARP) and at least as low as comparable modern automatic light railway systems with several years of operation history, e.g. the SkyLine in Vancouver, Canada and VAL in Lille, France. For the risk acceptance criteria the ALARP principle was chosen in order to ensure a reasonable balance of economic feasibility against risk level.

On that basis it was required, that the concept of Safety Integrity Levels (SIL´s) shall be used and that the overall SIL for the entire Metro shall be four. Hazard and Risk analyses and classification can be employed to identify adequate lower-level SIL´s to sub-systems and/or safety functions.

### 3.3 Normative Background for SIL Assignment

prEN50126 [2] states: When the level of safety for the application has been set and the necessary risk reduction estimated, based on the results of the risk assessment process, the safety integrity requirements can be derived. Safety integrity can be viewed as a combination of quantifiable elements (generally associated with hardware, i.e. random failures) and non-quantifiable elements (generally associated with systematic failures in software, specification, documents, processes, etc.). External risk reduction facilities and the system risk reduction facilities should match the necessary minimum risk reduction required for the system to meet its target level of safety. Confidence in the achievement of the safety integrity of a function within a system may be obtained through the effective application of a combination of specific architecture, methods, tools and techniques.

Safety integrity correlates to the probability of failure to achieve required safety functionality. Functions with greater integrity requirements are likely more expensive to realise. Safety integrity is basically specified for safety functions. Safety functions should be assigned to safety systems and/or to external risk reduction facilities. This assignment process is interactive, in order to optimise the design and cost of the overall system.

CENELEC Report prR009-004 [5] states: The CENELEC standards assume that safety relies both on adequate measures to prevent or tolerate faults (as safeguards against systematic faults) and on adequate means to control random failures. Measures against both causes of failure should be balanced in order to achieve an optimum safety performance of the system. To achieve this the concept of Safety Integrity Levels is used. SIL´s are used as a means of creating balance between measures to prevent systematic and random failures.

### 3.4 General Approach for the Copenhagen Metro SIL Assignment

The methodology used to apportion SIL´s to safety functions / sub-systems is derived from the CENELEC standards and has been performed according to the following steps:

Functional Analysis of the overall Metro to identify all safety related functions.

Identification of the required level of safety / SIL assignment to safety related functions.

3) Assignment of each safety related function to safety systems.

4) Identification, where applicable, of external risk reduction facilities. Redundant or back up risk reduction measures can be a combination of system design, procedures and external facilities.

These steps are explained in further detail in the following.

#### 3.4.1 Functional Analysis

Based on the Hazard Identification Analysis, for each hazard category (derailment, collision, death/injury, fire/smoke, electrocution, emergency situation), functions required to avoid the occurrence of the hazard, or its evolution into an accident, are identified.

Table 5: Hazard categories and the related safety functions (extract).

| SAFETY FUNCTION | REFERENCE HAZARDS | COLLISION | DERAILMENT | DEATH/INJURY | FIRE/SMOKE | ELECTROCUTION | EMERGENCY STOP |
|---|---|---|---|---|---|---|---|
| **Supply of Electric Power**<br>Supply of power to traction and essential/auxiliary equipment along the line | Hazard No. xx, yy, zz | | | X | | | X |
| **Vehicle Containment**<br>Support and guidance to vehicles | ... | | X | X | | | |
| **Safe Movement Control**<br>Maintain safe train separation, conflicting route prevention, safe speed enforcement, control of interlocking. | ... | X | X | X | | | |
| **Vehicle resistance**<br>Provide a safe vehicle under all foreseen riding conditions | ... | | X | | | | |
| **Guideway protection - persons**<br>Protect guideway from persons (e.g. persons falling onto the track) in stations and at tunnel entrances | ... | | | X | | X | |
| **Vehicles' doors management**<br>Closure while running, unscheduled door opening, doors' management under emergency conditions | ... | | | X | | | |
| **Fire detection / alarm on board / in stations**<br>Acquisition of fire relevant data and transmission to Central Control. | ... | | | | X | | |
| **Electrical short circuit protection**<br>Breaking function to cut power whenever a short circuit is detected on line or on a vehicle | ... | | | | X | | |
| **Emergency ventilation / lighting in tunnels**<br>Emergency ventilation / light and lit signals in tunnels | ... | | | X | | | X |
| **Communication between passengers and Control Centre**<br>Voice communication under emergency conditions | ... | | | X | | X | X |
| **Remote traction power cut off**<br>Third rail de-energisation from Control Centre | ... | | | | | X | X |

### 3.4.2 Identification of the Required Level of Safety

This step is based on the Hazard Identification and Analysis, comprising Hazard Identification (comprehensive identification of the hazards associated with the system, identification of the safeguards and protection features, identification of the consequences of the hazards) and Risk Analysis (analysis of the consequence severity, analysis of the occurrence frequency, analysis of the level of risk from the severity and frequency).

The further methodology is the following:

a) each safety function is associated to the most restrictive hazard among those to which the safety function refers to,

b) the frequency class associated to the referenced hazard is assumed as a frequency target; it is to be noted that the frequency class refers to a hazard developing into an accident; the frequency target is therefore associated to the accident;

c) the safety function participates in the development of a hazard into an accident as a risk reducing measure;

d) the level of integrity to be assigned to the safety function is the minimum necessary to verify the frequency target for the accident.

With reference to step b) above, frequency classes for hazards have been defined. For protective systems working continuously or in high demand mode, the required SIL is directly related to the frequency target associated to the reference hazard. This is due to the fact that the hazard is directly due to the absence of the protective function and always evolves into an accident. Therefore, the dangerous failure rate of the safety function shall not exceed the safety target.

On these premises, it is possible to derive a direct correspondence between the hazard frequency classes and the SIL ranges. Results of this process are summarised in Table 6 below.

Table 6: Hazard Frequency Classes and Correspondence to SIL´s

| **Description** | **Frequency Range (ev/year)** | **Frequency Range (~ ev/hour)** | **Category Designation** | **Corresponding SIL** |
|---|---|---|---|---|
| Frequent | > 1 | $> 10^{-4}$ | A | 0 |
| Probable | 1 - $10^{-1}$ | $10^{-4}$ - $10^{-5}$ | B | 0 |
| Occasional | $10^{-1}$ - $10^{-2}$ | $10^{-5}$ - $10^{-6}$ | C | 0 |
| Remote | $10^{-2}$ - $10^{-4}$ | $10^{-6}$ - $10^{-8}$ | D | 1 |
| Improbable | $10^{-4}$ - $10^{-6}$ | $10^{-8}$ - $10^{-10}$ | E | 3 |
| Incredible | $<10^{-6}$ | $<10^{-10}$ | F | 4 |

Following the above described method, for each individual safety related function the most restrictive hazard among those to which the safety function refers has been classified.

Example 1: Safe Movement Control

The referenced hazard associated to the following classes:

- Hazard Severity Class II (Critical, 4 to 30 fatalities)
- Hazard Frequency F (Incredible, $<10^{-6}$ ev/year)
- Risk Ranking Category T (Tolerable)

This target corresponds to a SIL 4.

Example 2: Guideway protection - persons, sub-function Protection at Platforms

The referenced hazard associated to the following classes:

- Hazard Severity Class III (Severe, 1 to 3 fatalities or several injuries)
- Hazard Frequency D (Remote, $10^{-2}$ - $10^{-4}$ ev/year)
- Risk Ranking Category T (Tolerable)

This target corresponds to a SIL 1.

Example 3: Vehicles' doors management

The referenced hazard associated to the following classes:

- Hazard Severity Class III (Severe, 1 to 3 fatalities or several injuries)
- Hazard Frequency E (Improbable, $10^{-4}$ - $10^{-6}$ ev/year)
- Risk Ranking Category T (Tolerable)

This target corresponds to a SIL 3.

### 3.4.3 Assignment of safety related functions to systems

Following the SIL apportionment to safety related functions, the systems (i.e. sub-systems and or equipment) devoted to the function implementation are identified. Moreover, when existing, safe-guards, protection features, or alternative systems or procedures by which the function can be performed are identified.

It should be noted, that a further sub-division of the safety related functions into sub-functions is possible. Taking the vehicle braking as an example, the dynamic braking can be assigned to be non safety related as long as the vehicle design ensures, that the dynamic braking can be completely substituted by the mechanical fail-safe braking.

The following table 7 depicts the above used examples.

Table 7: Apportionment of Safety Related Functions to Systems

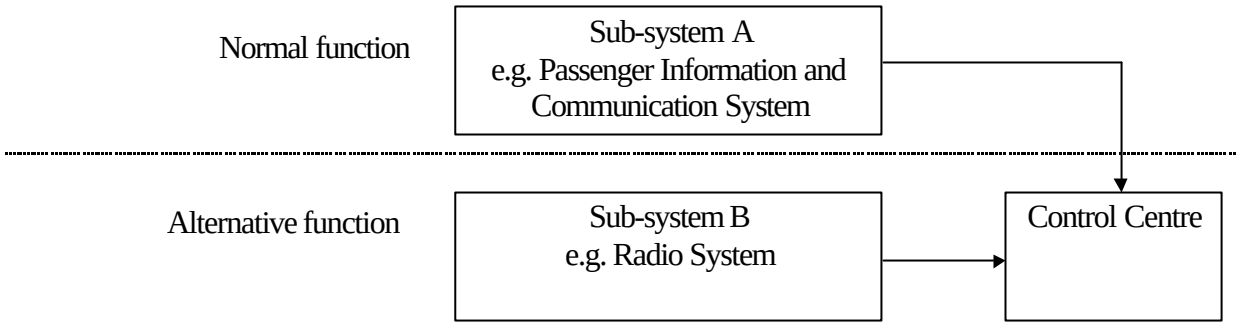
| Function Description | Required SIL | Sub-system / Equip-ment | Alternative System / Function |
|---|---|---|---|
| Safe Movement Control<br>• automatic vehicle protection<br>- conflicting route prevention<br>- speed profile control<br>- safe train separation<br>- control of interlocking | SIL 4 | - Wayside ATP<br>- Wayside + Vehicle ATP<br>- Wayside ATP<br>- Wayside ATP | None in automatic, driver-less mode. |
| Safe Movement Control<br>• vehicle braking<br>- dynamic braking<br>- fail-safe braking (mechanical) | SIL 0<br>SIL 4 | - Vehicle power inverter<br>- Vehicles brakes, safety magnet valves | Dynamic braking can be completely substituted by mechanical braking.<br>None for fail-safe braking. |
| Vehicles' doors management<br>• keeping doors closed and locked | SIL 3 | Rolling stock doors, doors control, door mechanical lock | None |
| Vehicles' doors management<br>• safe detection of the closed and locked status | SIL 3 | Vehicle ATP vital trainlines, door switches | None |
| Vehicles' doors management<br>• emergency opening function | SIL 3 | Emergency door release handle | None |
| Guideway protection - persons<br>• detection on unscheduled door opening | SIL 1 | Platform screen doors sub-system | Manual activation of Power Cut Off Handles will send an alarm to the way-side ATP to stop ap-proaching trains. |
| Guideway protection - persons<br>• stop of approaching trains | SIL 4 | Wayside ATP | See above |
| others<br>... | | | |

### 3.4.4 Identification of external risk reduction facilities

Redundant or back up risk reduction measures can be a combination of system design, procedures and external facilities. In these cases, the safety function can be performed by devices having SIL's lower than the one required to the safety function, provided that the required independence and functional diversity can be demonstrated.

As an example for redundant measures for the performance of a safety function, the safety function Communication between passengers and Control Centre (under emergency conditions) is depicted in figure 2. This communication function can still be performed by using the alternative function in case of failure and/or non-availability of the normal function.

Figure 2: Communication between passengers and Control Centre




For those safety functions performed by a unique sub-system, each failure occurring to the sub-system components negatively impacts the safety function. The extent of consequences of such failures on the safety function is analysed within the sub-system FMECA, included as part of the relevant Safety Cases.

## 4. Conclusion

This report has presented how the methodology for SIL apportionment, described by prEN5012x suite of norms, can be applied in different areas. The Copenhagen Metro system has been shown as an example.

Safety functions have been identified starting from the Hazard Identification and Analysis and relevant Safety Integrity Levels have been defined. Sub-systems in charge of the safety functions have been identified together with alternative measures to achieve the said function as a basis for the design requirement specifications.

Safety targets are defined using one of the principles ALARP, GAMAB, or MEM.

For the final system safety evidence, the demonstration of fulfilment of the numerical and qualitative requirements associated to the Safety Integrity Levels defined for each of the safety functions / sub-systems can be performed as follow:

for those sub-systems which are uniquely responsible for a safety function (e.g. the Automatic Train Protection sub-system), their Sub-system Safety Case should demonstrate fulfilment of the Safety Integrity Level allocated to the function.

Verification at the overall system level of compliance with the SIL assigned to safety functions should be performed considering both the reliability of those sub-systems and equipment involved in the safety function, and the alternative measures available, which reduce the residual risk of an accident.

The allocation of SIL´s can therefore be seen as an appropriate means to specify and design a safe system.

## References


[1] Verordnung über den Bau und Betrieb der Straßenbahnen – BOStrab
(Federal Regulation for the Construction and Operation of Tramways)
Issue: 11 December 1987

[2] prEN 50126
Railway Applications The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS)
Issue: June 1997

[3] prEN 50128
Railway Applications
Software for Railway Control and Protection Systems
Issue: June 1997

[4] ENV 50129
Railway Applications
Safety Related Electronic Systems for Signalling
Issue: June 1997

[5] Railway Applications
Systematic Allocation of Safety Integrity Requirements
CENELEC Report prR009-004
Issue: Final Draft March 1999

[6] prEN 50129
Railway Applications
Safety Related Electronic Systems for Signalling
Issue: December 1999

[7] IEC 61508, parts 1-6
Functional safety of electrical/electronic/programmable electronic safety-related systems

[8] Wigger. P. & Haspel, U.
Safety Assessment of Copenhagen driverless automatic mass transit system, Proc. of the sixth int. Conference COMPRAIL 98, Lisbon, Portugal, pp 63 - 72, 1998

[9] Schäbe H. & Wigger P.
Experience with SIL Allocation in Railway Applications, Proc. of the
fourth int. symposium on Programmable Electronics Systems in Safety Related Applications
Cologne, Germany, 2000

**Contacts and Web Sites**

Author Contact:

Dipl.-Ing. Peter Wigger
TÜV InterTraffic GmbH
Institute for Software, Electronics, Railroad Technology (ISEB)
Am Grauen Stein
D - 51105 Cologne
Phone: +49 221 806 3322
Fax: +49 221 806 2581
e-mail: wigger@iseb.com

Further information can be found on the following Web Sites:

Information on the TÜV Rheinland/Berlin-Brandenburg Group and the Institute for Software, Electronics, Railroad Technology (ISEB) can be found under

www.tuev-rheinland.de

www.iseb.com

Information on the Copenhagen Metro Project can be found under

| | |
|---|---|
| www.ansaldo.dk | (Copenhagen Metro System Supplier Ansaldo) |
| www.m.dk | (Copenhagen Metro System Owner Ørestadsselskabet I/S) |