TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CLC/TR 50451

May 2007

ICS 45.020;93.100

Supersedes R009-004:2001

English version

Railway applications – Systematic allocation of safety integrity requirements

Applications ferroviaires – Allocation systématique des exigences d'intégrité de la sécurité

Bahnanwendungen – Systematische Zuordnung von Sicherheitsintegritätsanforderungen

This Technical Report was approved by CENELEC on 2006-02-18.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

This Technical Report was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways.

The text of the draft was circulated for vote in accordance with the Internal Regulations, Part 2, Subclause 11.4.3.3 and was approved by CENELEC as CLC/TR 50451 on 2006-02-18.

This Technical Report supersedes R009-004:2001.

____

Contents

Executive summary

This Technical Report presents a systematic methodology to determine safety integrity requirements for railway signalling equipment, taking into account the operational environment and the architectural design of the signalling system.

At the heart of this approach is a well defined interface between the operational environment and the signalling system. From the safety point of view this interface is defined by a list of hazards and tolerable hazard rates associated with the system. It should be noted that the purpose of this approach is not to limit co-operation between suppliers and railway authorities but to clarify responsibilities and interfaces.

It is the task (summarized by the term Risk Analysis) of the Railway Authority

- to define the requirements of the railway system (independent of the technical realisation),
- to identify the hazards relevant to the system,
- to derive the tolerable hazard rates, and
- to ensure that the resulting risk is tolerable (with respect to the appropriate risk tolerability criteria).

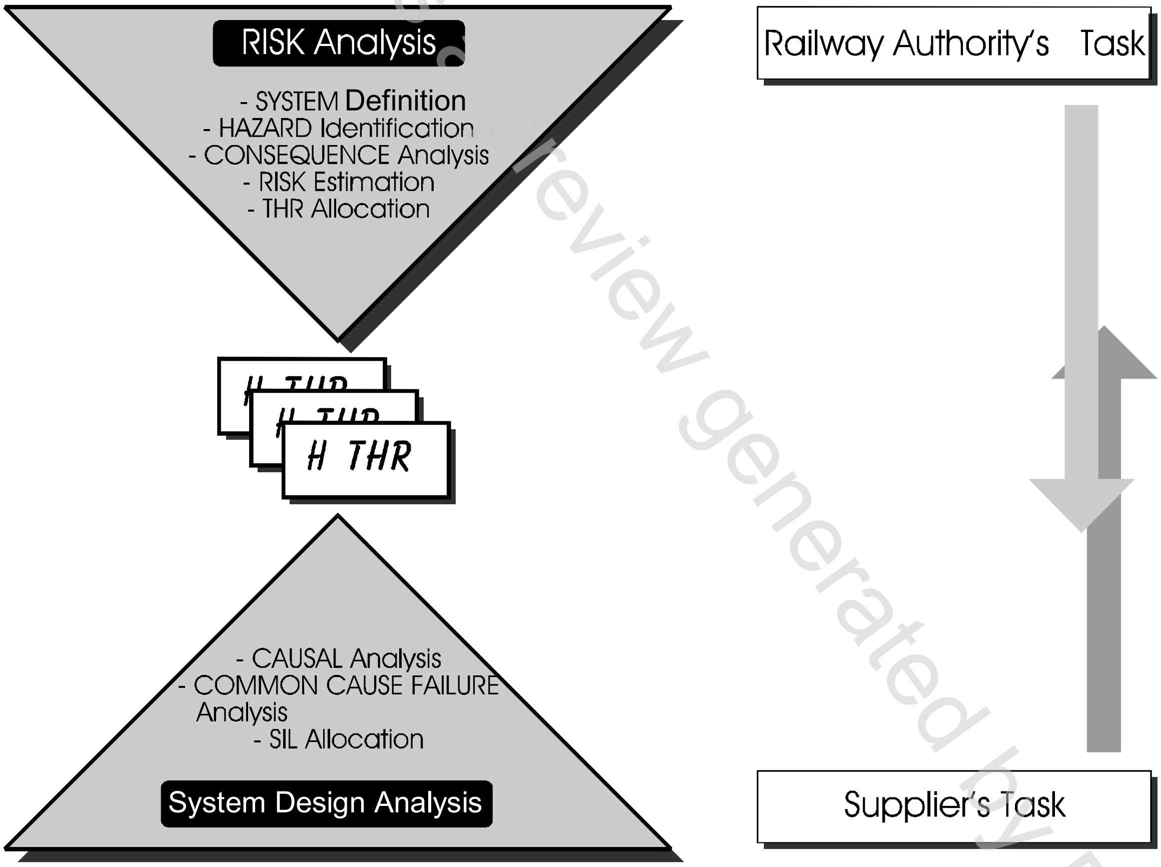


Figure 0.1 - Global process overview

The only requirement is that the tolerable hazard rates must be derived taking into account the risk tolerability criteria. Risk tolerability criteria are not defined by this Technical Report, but depend on national or European legislative requirements.

Among the risk analysis methods two are proposed in order to estimate the individual risk explicitly, one more qualitative, the other more quantitative. Other methods, similar to the GAMAB principle, do not explicitly determine the resulting risks, but derive the tolerable hazard rates from comparison with the performance of existing systems, either by statistical or analytical methods. Alternative qualitative approaches are acceptable, if as a result they define a list of hazards and corresponding THR. The specification of the system requirements comprising performance and safety (THR) terminates the Railway Authority's task.

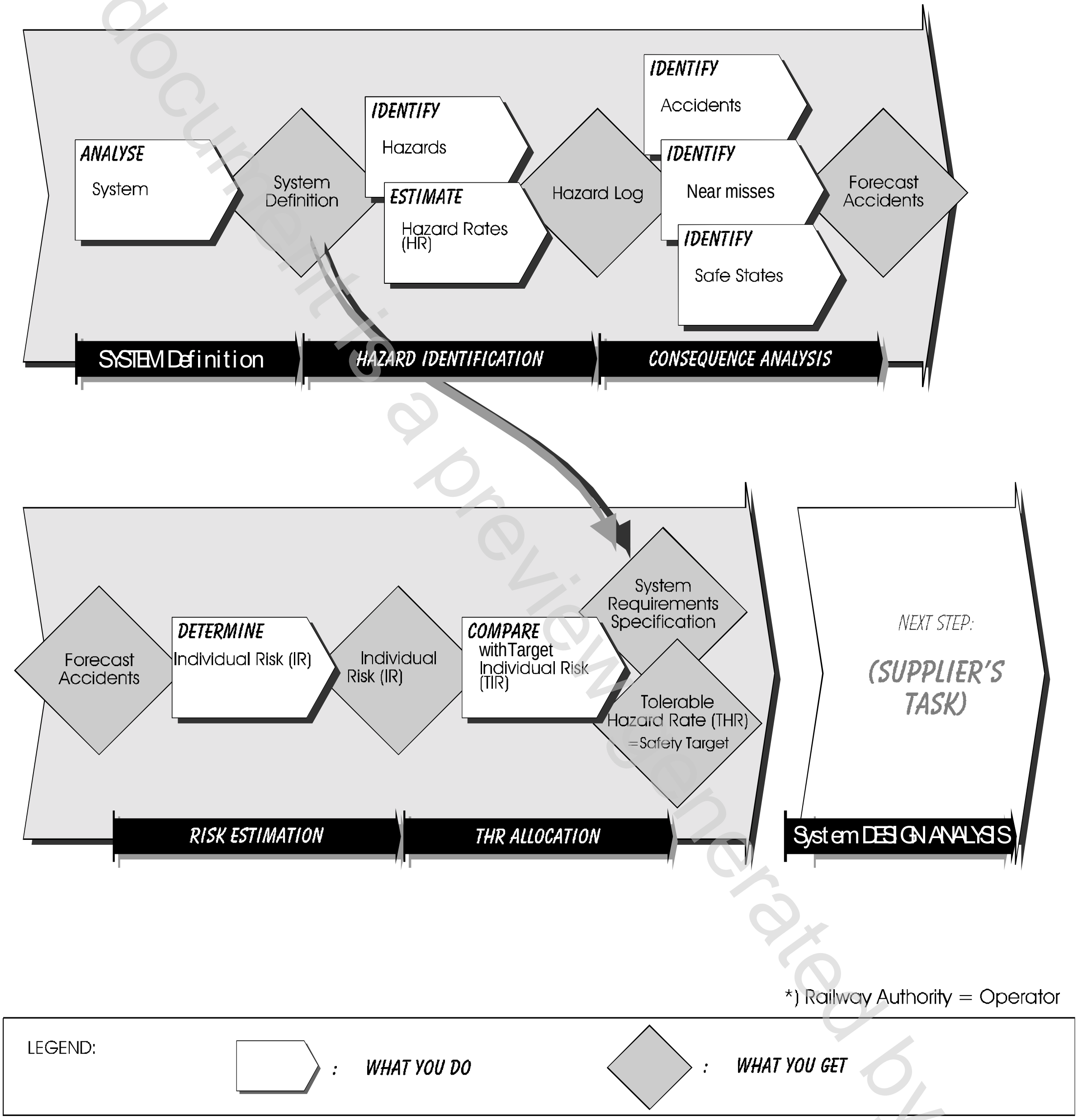


Figure 0.2 - Example Risk Analysis process

The supplier's task (summarized by the term System Design Analysis) comprises

- definition of the system architecture,
- analysis of the causes leading to each hazard,
- determination of the safety integrity requirements (SIL and hazard rates) for the subsystems,
- determination of the reliability requirements for the equipment.

Causal analysis constitutes two key stages. In the first phase the tolerable hazard rate for each hazard is apportioned to a functional level. Safety Integrity Levels (SIL) are defined at this functional level for the subsystems implementing the functionality. The hazard rate for a subsystem is then translated to a SIL using the SIL table.

During the second phase the hazard rates for subsystems are further apportioned leading to failure rates for the equipment, but at this physical implementation level the SIL remains unchanged. Consequently also the software SIL defined by EN 50128 would be the same as the subsystem SIL but for the exceptions described in EN 50128.

The apportionment process may be performed by any method which allows a suitable representation of the combination logic, e.g. reliability block diagrams, fault trees, binary decision diagrams, Markov models etc. In any case particular care must be taken when independence of items is required. While in the first phase of the causal analysis functional independence is required, physical independence is sufficient in the second phase. Assumptions made in the causal analysis must be checked and may lead to safety-relevant application rules for the implementation.

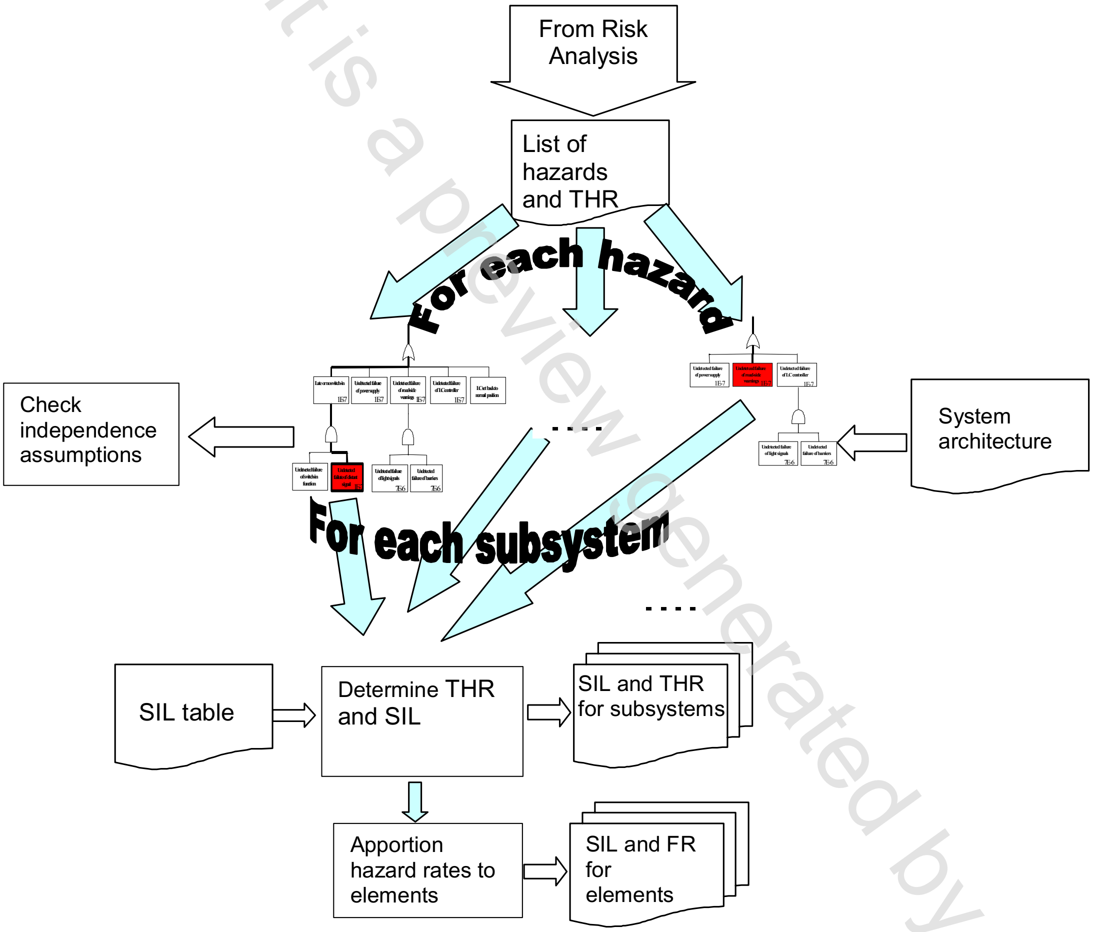


Figure 0.3 - Example System Design Analysis process

Both, the risk analysis and the system design analysis, have to be approved by the Railway Safety Authority.

However whilst the risk analysis may be carried out once at the railway level, the system design analysis must be performed for every new architecture. It is prudent to review the risk analysis and system design analysis when safety related changes are introduced.

Introduction

Historically the interoperability of European railways was not only hindered by incompatible technology but also by different approaches towards safety. The common European market is the main driving force behind the harmonisation of the different safety cultures. In a joint pan-European effort comprehensive safety standards have been established for railway signalling by the European Electrotechnical Standardisation Committee CENELEC:

- EN 50126-1, Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Basic requirements and generic process

- EN 50128, Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems

- EN 50129, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

These CENELEC standards assume that safety relies both on adequate measures to prevent or tolerate faults (as safeguards against systematic failure) and on adequate measures to control random failures. Measures against both causes of failure should be balanced in order to achieve the optimum safety performance of a system. To achieve this the concept of Safety Integrity Levels (SIL) is used. SILs are used as a means of creating balance between measures to prevent systematic and random failures, as it is agreed within CENELEC that it is not feasible to quantify systematic integrity.

A shortcoming of the CENELEC standards as of today is (similar as in other related standards like IEC 61508 [1)] [IEC] or ISA S84.01 [ISA]) that while the guidance on how to fulfil a particular SIL is quite comprehensive the process and rules to derive SILs for system elements from system safety targets or the tolerable system risk are not adequately covered. A general convincing solution to this problem is still an open research problem, see [LM][ZD][YB2][GAM] for some divergent examples. However in order to achieve cross-acceptance of safety cases and products for railway signalling applications it is necessary to fill the gap.

This has been realized by SC 9XA in 1997 and consequently a working group has been set up in March 1998 in order to find a joint harmonized approach at least for railway signalling applications. This work resulted in the publication of R009-004:2001, which is presently being converted into CLC/TR 50451.

Although the major driving forces behind this work were novel signalling applications which are required to be interoperable throughout Europe, the scope and applicability of the approach presented in this Technical Report should not be limited to signalling or interoperable applications.

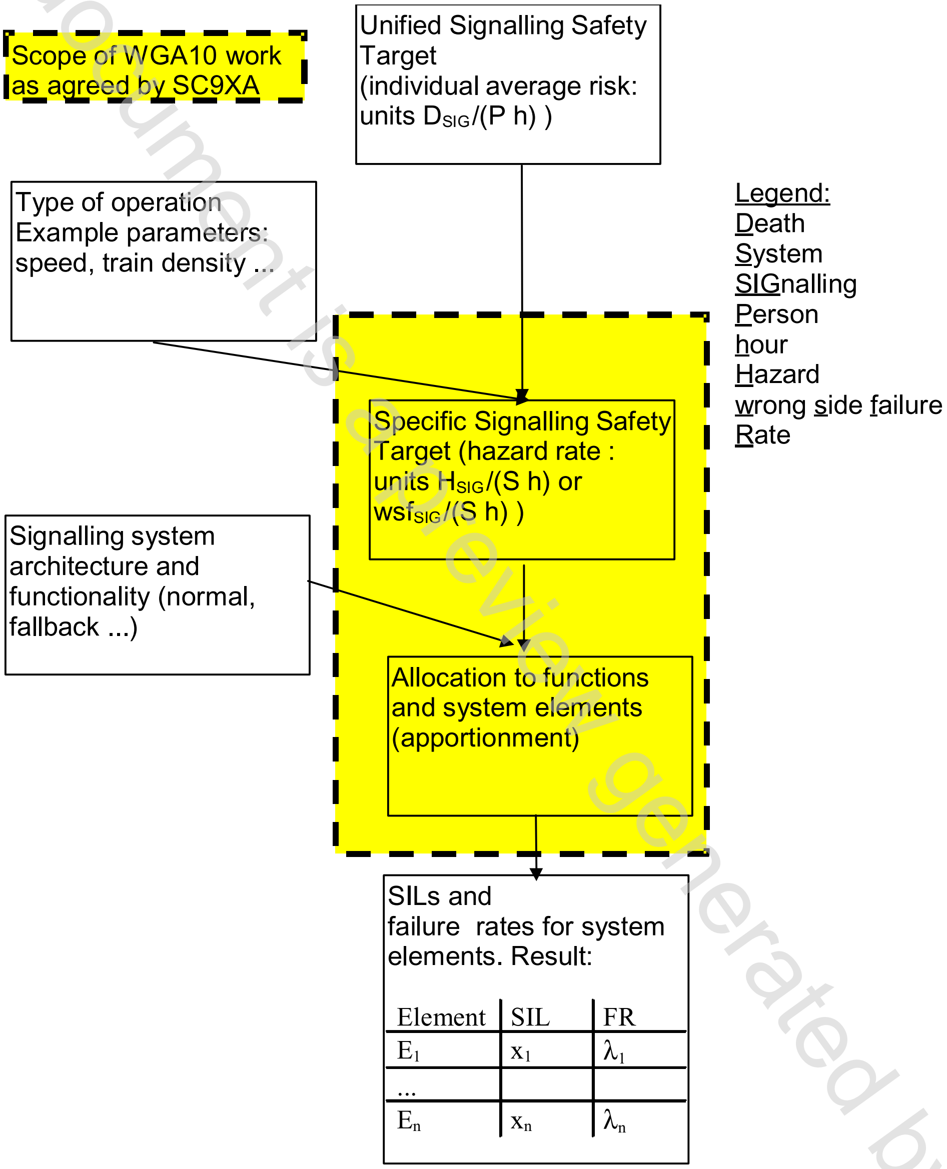
[1)] IEC 61508 series has been harmonized as EN 61508 series "Functional safety of electrical/electronic/programmable electronic safety-related systems"

1 Scope

The scope of this Technical Report is to define a method to determine the required Safety Integrity Level of railway signalling equipment taking in consideration

- the operational conditions of the railway, and
- the architecture of the signalling system.

The following picture may be used in order to detail more precisely the scope of this Technical Report:


Scope of WGA10 work as agreed by SC9XA
Unified Signalling Safety Target (individual average risk: units $D_{SIG}/(P\ h)$)
Type of operation Example parameters: speed, train density ...
Legend:
Death
System
SIGnalling
Person
hour
Hazard
wrong side failure
Rate
Specific Signalling Safety Target (hazard rate : units $H_{SIG}/(S\ h)$ or $wsf_{SIG}/(S\ h)$)
Signalling system architecture and functionality (normal, fallback ...)
Allocation to functions and system elements (apportionment)
SILs and failure rates for system elements. Result:

Element	SIL	FR
E_1	x_1	λ_1
...		
E_n	x_n	λ_n

Figure 1.1 - Scope of WG A10

From a mechanistic point of view the task of this Technical Report is to define a method of calculation, which determines the integrity requirements (qualitatively and quantitatively) from the inputs stated above.

2 References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.1 Normative references

EN 50121-5, Railway applications - Electromagnetic compatibility - Part 5: Emission and immunity of fixed power supply installations and apparatus

[126] EN 50126-1:1999, Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process

[128] EN 50128:2001, Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems

[129] EN 50129:2003, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

2.2 Informative references

[0056] UK Ministry of Defence, Safety Management Requirements for Defence Systems, Def Stan 00-56

[GAM] CASCADE: Generalised Assessment Method <GAM>, Part II: Guidelines, ESPRIT 9032 report, ref. CAS/IC/MK/D2.3.2/V3, 1996

[HK] Kumamotu, H. and Henley, E.: Probabilistic risk assessment and management for engineers and scientists, IEEE Press, 1996

[IEC] Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508 series

[ISA] ISA: Application of Safety Instrumented Systems for the Process Industries, ISA S84.01, February 1996

[ISO] ISO/IEC: Information technology - System and software integrity levels, ISO/IEC 15026

[Lev95] Leveson, N. G.: Safeware - System safety and computers, Addison-Wesley, 1995

[LM] Lindsay, P. A. and McDermid, J. A.: A systematic approach to software safety integrity levels, in: Peter Daniel (Ed.): SAFECOMP'97 , Springer Verlag, 1997, 70-82

[R01] Railway applications - Communication, signalling and processing systems - Hazardous failure rates and Safety Integrity Levels (SIL), R009-001:1997

[RSH] Railway Signalling Hazards, Swedish National Rail Administration, Technical Report 1999:1

[SAH] System Safety Analysis Handbook, 2nd edition, System Safety Society, 1998

[VIL] Villemeur, A.: Reliability, Availability, Maintainability and Safety Assessment, Volume 1: Methods and Techniques, Wiley, 1992

[YB2] Engineering Safety Management System, Issue 2.0, "Yellow Book", Railtrack, 1997

[ZD] Zerkani, H. and Dumolo, D.: System Safety Lifecycle Based on IEC 61508 and its Use for Railway Applications, Proc. 16th International System Safety Conference, Sept. 14-19, 1998, Seattle