Statens Havarikommisjon for Transport

JB Report: 2007/02

REPORT ON SERIOUS RAILWAY INCIDENTS AT SLEPENDEN BLOCK STATION DUE TO WRONG-SIDE SIGNALLING AT SANDVIKA STATION ON THE DRAMMEN LINE 20 APRIL 2005

Date
February 2007

Accident Investigation Board Norway
P.O. Box 213
N-2001 Lillestrøm
Norway
Phone: +47 63 89 63 00
Fax: +47 63 89 63 01
http://www.aibn.no
E-mail: post@aibn.no

INDEX

REPORT ON

Safety system:	Interlocking system, Siemens type SIMIS-C
Train numbers:	13905 and 12207
Rolling stock:	Type 71 and Type 69
Nationality and registration:	Norwegian, airport express train 71005 and NSB train 69072
Owners:	Flytoget AS and NSB AS
Operators:	Flytoget AS and NSB AS
Crew:	An airport express train driver/locomotive driver was onboard each train.
Passengers:	None, (both of the trains involved were empty)
Accident site:	Sandvika station - Slependen block signal station
Date and time:	Incident 1, Wednesday 20 April 2005 at 0418 Incident 2, Wednesday 20 April 2005 at 0444

REPORTING OF THE INCIDENT

The Accident Investigation Board Norway (AIBN) was notified immediately of the serious incident by on-duty personnel at Flytoget AS and the Norwegian National Rail Administration. NSB AS made its report later that same day. This was because the serious incident was not reported immediately to the operations centre at NSB AS.

SUMMARY

Wednesday 20 April 2005, during the period 0418 – 0444, two serious incidents occurred in conjunction with a distant signal showing wrong-side signalling. Incident 1 occurred at 0418 when express train 13905 had passed distant signal A for Slependen, which indicated an “expect to proceed” signal, and approached block signal A 357 at Slependen

block signal station. Then the express train driver discovered that the block signal was showing the “stop” signal. The airport express train driver took immediate action by applying the emergency brake on the train, but since it was only a short distance up to the block signal he did not manage to stop in front of the signal, but passed the signal with the entire train. There were then two trains on the same block signal section.

Incident 2 occurred at time 0444 when the next train, 12207, passed the distant signal for Slependen block signal station and this was showing the “expect to proceed” signal. The train’s ATC equipment was showing “proceed” on the main indicator, and the train continued along the block section at a speed of almost 82 km/h. When the train neared the Slependen holding point the locomotive driver detected 2 red lights (the rear lights on airport express train 13905) on one of the lines and immediately applied the emergency brake. He managed to stop the train a few metres away from the airport express train, which had stopped on the same line a few minutes before. The distance from airport express train 13905 was then approximately 30 metres. It was only the alertness and quick-thinking of the locomotive driver that prevented this becoming a collision.

During a review of the safety system, there proved to be a programming error in the computer-controlled interlocking system. This programming error was identified as being in the generic software. For this error to arise, 4 conditions would have had to occur in a specific sequence. This would have triggered the interlocking system to ensure that the distant signal displayed an incorrect (non-restrictive) signal aspect. All safety systems with similar interfaces were taken out of operation until the system error in the computer-controlled interlocking system had been corrected, tested and operationally tested.

1. FACTUAL INFORMATION

1.1 Sequence of events

Wednesday 20 April 2005, during the period 0418 – 0444, two serious incidents occurred in conjunction with a distant signal showing the wrong-side signalling. The current distant signal was located on the same mast as main exit signal N 4323 at Sandvika station, and was a signal that gave advance warning of what block signal A 357 at Slependen block signal station was indicating in the Asker direction. Block signal A 357 at Slependen block signal station indicated the “stop” signal, (red light) at the same time as the distant signal at signal N 4323 showed an “expect to proceed” signal (see fig. 1 and 2): The interlocking gear in the interlocking system should be designed to ensure that it is impossible for this combination to occur.

Summary of the sequence of events over time

- Maintenance work train 51006 has use of the line between Billingstad and Hvalstad for works up to time 0500.

- At time 0400, train 13903 passes signal B Slependen block signal station, comes to a halt in front of main entrance signal A at Billingstad to wait for oncoming train 3701 to pass on the main track Drammen – Oslo.

- At time 0417, train 13905 passes main exit signal N (4323) at Sandvika station.

- At time 0419, train 13905 passes signal A Slependen (passes with the entire train set and the line block section is freed up behind the train set). The airport express train driver notifies the traffic controller of the signal fault. Two trains are now on the same block signal section

- At time 0422, train 13903 is given the "proceed" signal in to Billingstad station

- At time 0438, train 12207 arrives on line 1 at Sandvika station.

- At time 0441, the main entrance signal at Billingstad is set to a "proceed" signal for train 13905, but the train remains standing since the airport express train driver does not see the signal from this position.

- At time 0442, the main exit signal is set to "proceed" for train 12207 to leave from line 1 at Sandvika station

- At time 0444, train 12207 is standing on the line block immediately in front of signal A Slependen block signal section.

- At time 0454, train 13905 drives in to Billingstad station (passing signal A 351)

Incident 1:

Express train 13905 had passed the distant signal for the block signal station, which indicated an "expect to proceed" signal, and approached block signal A 357 at Slependen block signal station, when the airport express train driver discovered that the signal was showing signal "stop". The airport express train driver immediately applied the emergency brake, but since it was only a short distance up to the block signal he did not manage to stop in front of the signal. The train passed the signal by the entire length of the train set and stopped with the rear end of the train set a few metres past the block signal, such that the block section to the rear of the train was train-free (see figure 4). The airport express train driver immediately notified the train controller and provided the information that the signal aspect in the distant signal and block section signal A at Slependen block signal station did not correspond. He also informed the train controller that the train's ATC panel had indicated three dashes, meaning that the Slependen block signal station should be showing the "proceed" signal.

Figure 1: The distant signal for Slependen block signal station (located at Main Exit Signal N 4323 at Sandvika station) was showing an "expect to proceed" signal.

Figure 2: Block signal A Slependen was showing a "stop" signal. (Not corresponding with the signal aspect of the distant signal)

The reason for block signal A 357 at Slependen block signal station showing a "stop" signal for airport express train 13905, was that airport express train 13903 had been given a "stop" signal ahead of entrance signal A at Billingstad station and was on the block section between Slependen block signal station and Billingstad station (see fig. 3). Airport express train 13903 had been given a "stop" signal in the main entrance signal at Billingstad station because train 51006 was carrying out maintenance work on the railway line between Billingstad and Hvalstad stations. The train controller was therefore unable to send airport express train 13903 on towards Asker station. The distance between airport express trains 13903 and 13905, positioned on the block section, was around 670 metres. During this incident, there was no danger of a collision between these two trains. (see fig. 4)

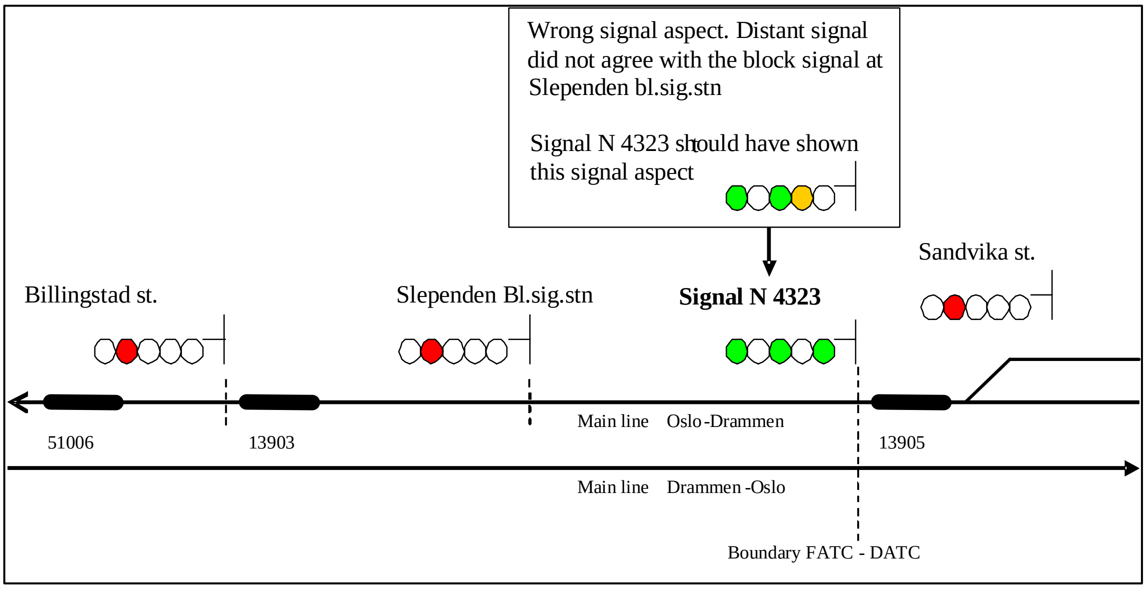

Figure 3: Airport express train 13905 departs at time 0417 from Sandvika station

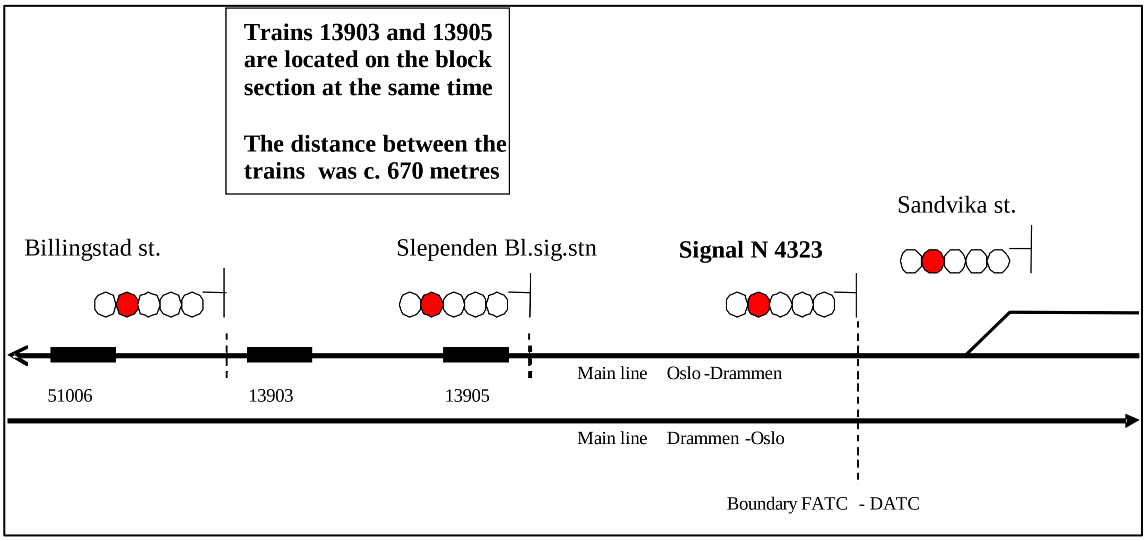

Figure 4: Airport express trains 13903 and 13905 are located on the same block section at time 0419

The airport express driver in train 13905 had phoned the train controller immediately after the first serious incident and informed the controller that the signal aspects in the distant signal and block signal A 357 in the Slependen block signal station did not correspond.

The train controller did not immediately react to this report, since the train route was set for train 12207. In the meantime, the airport express train driver in train 13905, in consultation with the airport express train's operations manager, had moved to the opposite driver's cab on the train set. He then discovered that a train had stopped only a few metres away from his train set. The airport express driver phoned the train controller once more (after incident 2) and informed him of this.

Incident 2:

A route was set for the train to depart on line 1 at Sandvika station for train 12207, with main exit signal N 4323 showing a “proceed” signal for NSB train 12207. The train went past the main exit signal and the distant signal for Slependen block signal station was showing the “expect to proceed” signal (see figure 5). The train’s ATC equipment received the same information and the train continued out onto the block section at a speed of almost 82 km/h.

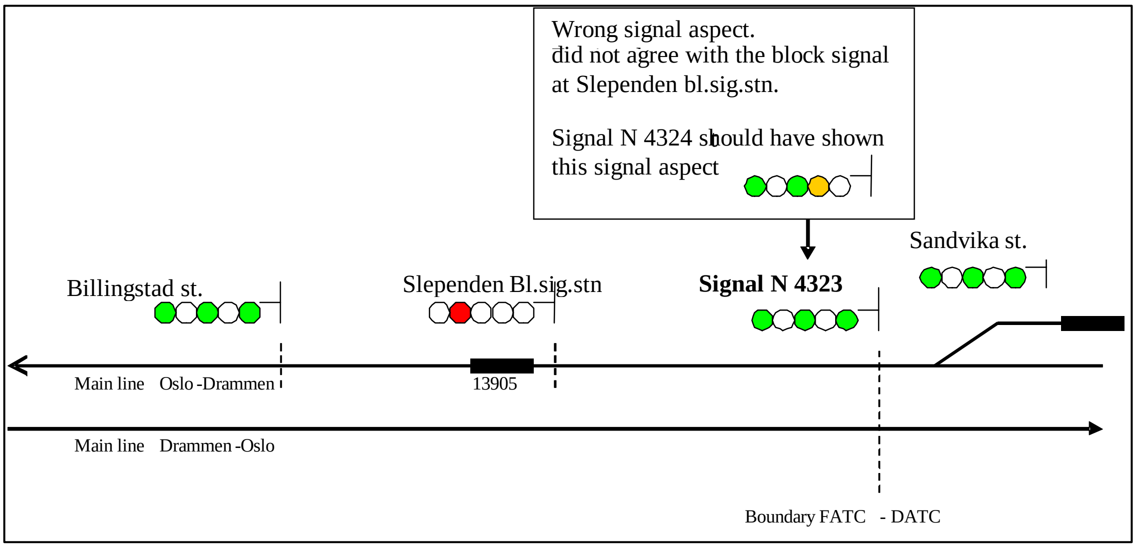

Figure 5: The situation at time 04:42:46, immediately before the second serious incident occurred. Train 12207 started to depart on line 1 at Sandvika station.

When the train approached the Slependen holding point, the locomotive driver began to have doubts when he discovered 2 red lights on one of the lines. These were the rear lights on train 13905 which was standing on the block section after Slependen block signal station. He was unable to ascertain which of the main lines the red lights were located on, but for safety’s sake he immediately applied the emergency brake and gradually discovered that train 13905 was standing on the very main line on which he was travelling. Because the emergency brake had been applied, the locomotive driver was able to stop the train just in front of the signal at Slependen block signal station. The person involved estimated that his distance from airport express train 13905 was approx. 30 metres. It was only the alertness and quick-thinking of the locomotive driver that prevented this becoming a collision.

The locomotive driver had been working on night duty and was at the end of his duty period, and was not able subsequently to remember which signal aspect had been on the distant signal, but reacted to the fact that the ATC had not intervened. A report about this serious incident was not sent immediately to the train controller. This first became known around 1.5 hours later, once the operations centre at NSB had been in touch with the locomotive driver in train 12207 and then notified the train control centre.

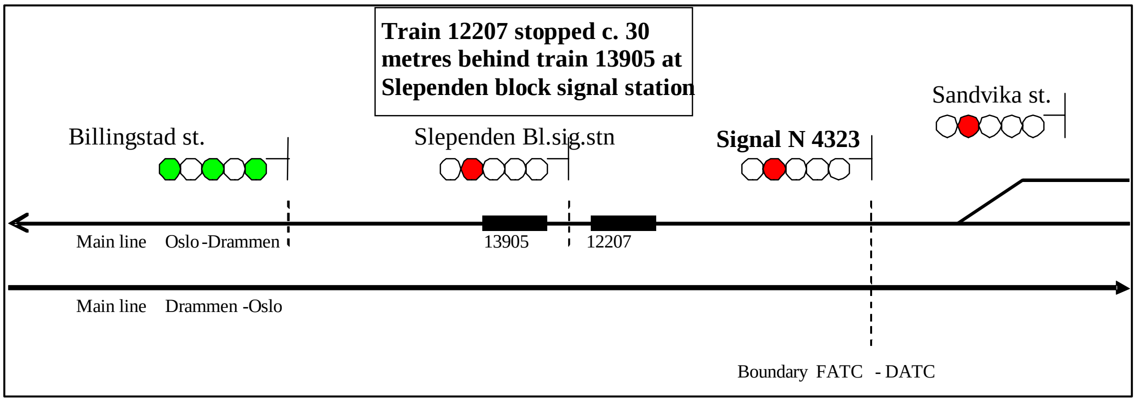

Figure 6: At time 04:44:31, the scenario after the locomotive driver had applied the emergency brake and stopped train 12207 in front of the signal at Slependen block signal station.

When two serious incidents had been reported, questions were raised of the train controllers about the interlocking system. The duty controller decided that the train crew onboard airport express train 13907 should observe the signal aspect in the distant signal and report when the train passed main exit signal N 4323 at Sandvika station. The train crew confirmed that signal N 4323 actually showed the signal aspect described in the two serious incidents. At this time, further action was taken by the train controllers, and faults in the safety system were notified to the on duty signal man.

The track of the line between Sandvika and Billingstad is curved. Because the superstructure at Slependen holding point is screened from view, it was not possible for the locomotive driver to detect signal A 357 at Slependen block signal station until the train was right at the Slependen holding point.

After these two serious incidents, it came to light that it earlier the same week as these two serious incidents occurred, on Sunday 17 April at time 0112, the locomotive driver in airport express train 3816 had reported to the train controller about a similar signal observation involving the distant signal on signal N 4323 at Sandvika station. The AIBN did not receive any report on this incident, and it is not aware of whether this case was reported further by the train controller internally within the Norwegian National Rail Administration.

1.2 Injuries to persons

No injuries to persons were reported in these serious incidents. The AIBN has been informed that the locomotive driver in train 12207 went on sick-leave for a time after the incident and was given physiotherapy for muscular trouble.

1.3 Damage to the rolling stock involved

No material damage occurred to the rolling stock during any of these serious incidents.

1.4 Description of damage to infrastructure and track

No material damage occurred to the track or other parts of the infrastructure during any of these serious incidents.

1.5 Other damage

No other damage occurred to any third party's property during any of these serious incidents.

1.6 Personnel information

Not relevant to these incidents.

1.7 Rolling stock

The trains involved in these two serious incidents were:

Incident 1: Two multiple units, type 71 (airport express train).

Incident 2: Multiple unit type 71 (airport express train) and local train type 69 D (NSB train).

1.8 Infrastructure and track

Sandvika station is located on the remotely-controlled double-track section between Oslo S and Drammen on the Drammen line. The track route is on a curve on the Sandvika – Slependen – Billingstad section. The line of sight up to the main signals must, according to the National Rail Administration's regulation JD 551, permit the signal to be visible over the last 250 metres up to the signal. The line of sight to block signal A at Slependen block signal station was checked, and it proved to be precisely 250 metres. In addition, the view of the signals was reduced because an overhead conductor mast was located a few metres in front of the signal.

There were three signal fitters on duty on the day in question. Two were at Oslo S and one at Asker station. One signal fitter was called out from Oslo S and one from Asker station when they received a message from the train controller about a fault on a distant signal at Sandvika station. The system was reset to allow the fault to be signed off. The AIBN has been made aware that there have been repeated occasions on which there have been faults in the system at Sandvika station. These were resolved by signing off the fault by resetting the interlocking system. The faults normally involved the distant signal indicating a restrictive status due to element lock. This was a fault that occurred frequently, but which was not safety-critical. The AIBN recorded that provisional connections had been carried out, and recording equipment fitted to capture this fault both at the block signal station and in the interlocking system at Sandvika station.

1.9 Weather

The incidents occurred early in the morning. It was twilight, the weather was fine and it was not raining.

1.10 Traffic management and signal systems

The form of operation at Sandvika station is a section with remote control. Sandvika station is part of the remotely controlled Oslo S – Drammen section. The Oslo S – Asker station section is controlled remotely from the traffic control centre at Oslo Central

Station. The interlocking system can be connected automatically, ensuring that the signals are set automatically for trains in and out on the train lines block sections.

The signal system at Sandvika station is a SIMIS C computer-controlled interlocking system.

The section is equipped with automatic train stop, partially developed ATC (DATC), and with fully developed ATC (FATC) at Sandvika station.

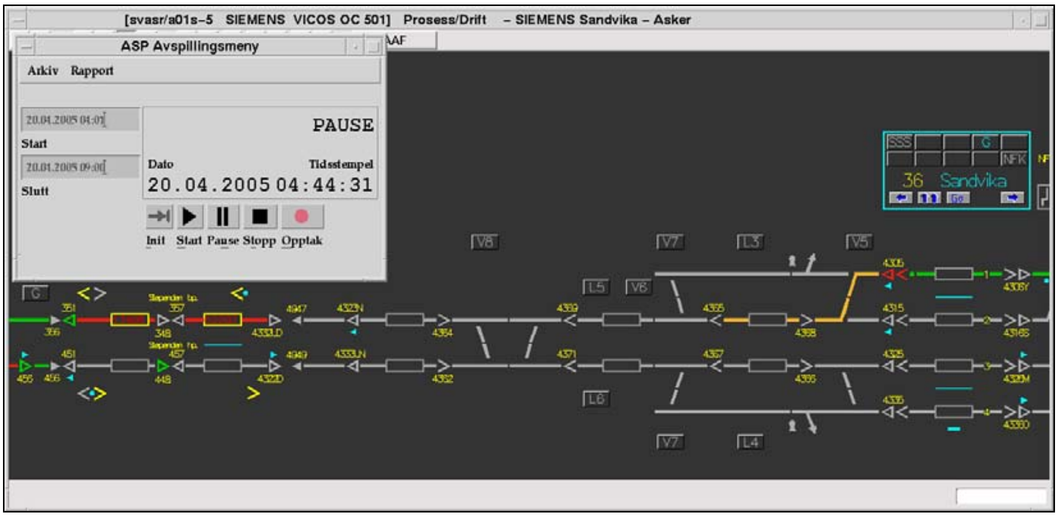

Figure 7: Printout of log from the second serious incident, at time 04:44:31, in which trains 13905 and 12207 are each standing on their own side of Slependen block signal station.

1.10.1 Interlocking system

Sandvika station is equipped with a safety system that is an electronic computer-controlled interlocking system. This safety system was brought into use in summer 2004.

The interlocking system that controls exit signal N 4323 at Sandvika is of the SIMIS-C type supplied by Siemens. This safety system is an electronic computer-controlled interlocking system with an overall configuration as shown schematically in figure 8.

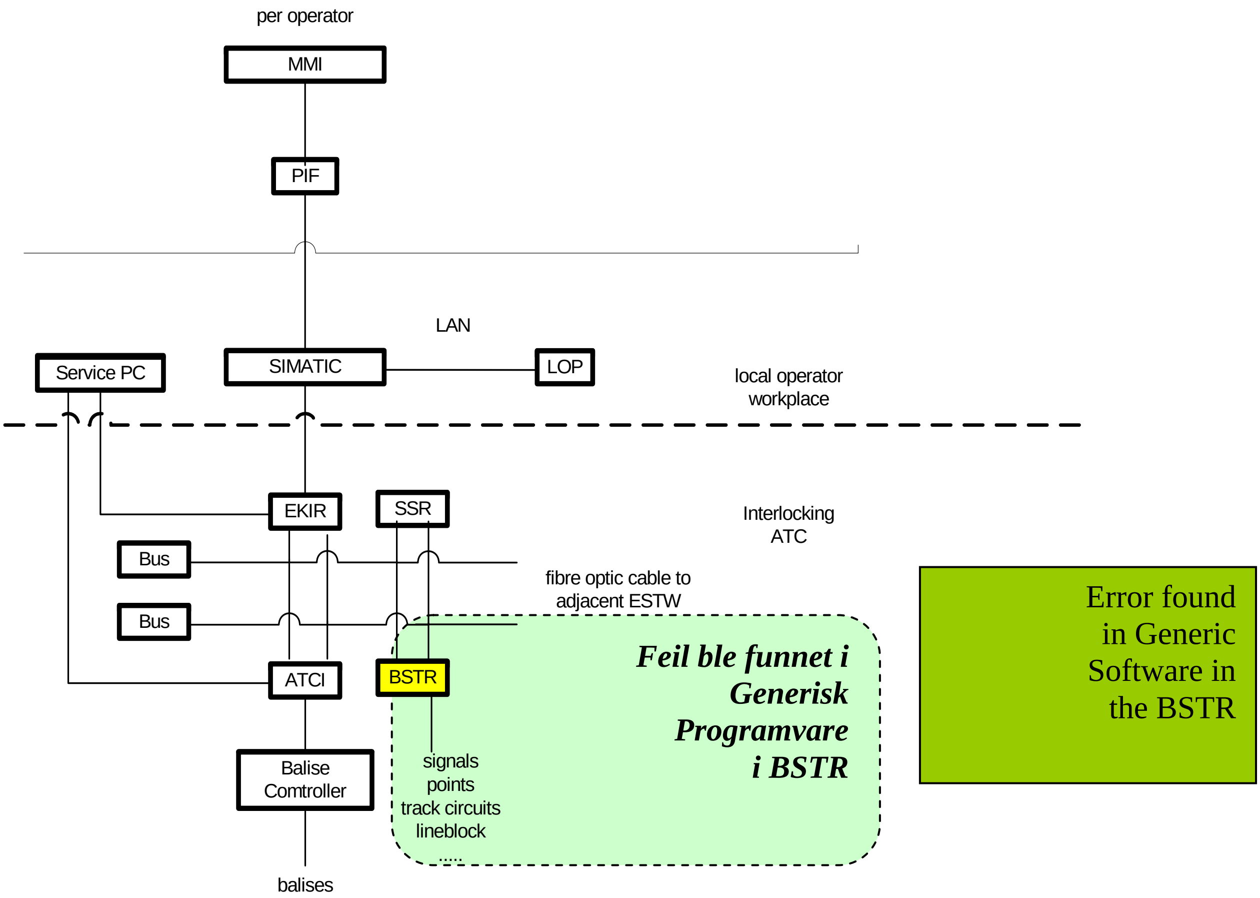

Figure 8: Showing how the fault was identified in the computer-controlled interlocking system

Explanation of the terms used in figure 8.

- MMI — Man Machine Interface
- PIF — Process InterFace
- SIMATIC — Designation of the Siemens PLS
- LOP — Local Operator Place
- EKIR — Eingabe Kommunikation Inpretator Rechner. (main calculator)
- SSR — Schnitt Stell Rechner. (Interface computer)
- Bus — Databus for the safety system
- BSTR — Communications unit with object control units. (local computer)
- ATCI — Automatic Train Control Interface. (For controlling ATC-track antenna)

In principal, SIMIS-C comprises one central machine (EKIR) with central interlocking logic. This communicates with object control units (BSTR) via a databus. BSTR contains both generic and application software to control external objects, including signals and interfaces with line block. ATCI obtains ATC information from EKIR and puts out the information in the balises. The SSR exchanges status indication and information about object statuses.

The cause of the fault situation at Slependen was found in the generic software in BSTR. This software was developed for the SIMIS-C on the Gardermobanen railway line (GMB) and was not subject to specific validation and approval in conjunction with the Sandvika project.

1.10.2 Line block including interface

Billingstad block signal station is of the standard 3-term relay line block type.
Main and distant signal instruction to/from a block signal station is transmitted via relay connections and an EF 180 transmission system (see figure 9) which is a transparent transmission of relay information to the SIMIS-C system. In these cases, block signal A 357 showed a “stop” signal at the same time as the associated distant signal at exit signal 4323N showed the “expect to proceed” signal.

Figure 9: Interface system EF 180 at Slependen block signal station. This transmits signal information between the relay system at the block signal station and the computer-controlled interlocking system at Sandvika station via a telecommunications cable.

1.10.3 Technical description of fault

The fault in the interlocking system arose primarily as a consequence of a programming error in the generic software in the BSTR for the safety system.

A series of incidents occurred in a specific sequence in the process. This led to an incorrect signal aspect occurring in the distant signal applying to Slependen block signal station. This distant signal was located on the mast of main exit signal N 4323 at Sandvika station. No allowance had been made for the relevant combination of incidents during the testing of the system prior to it being commissioned.

The four fault conditions causing the fault to become evident were:

1. The signal system had an "element lock" in a GUET element (normally not safety-critical) in the part of the system that processes the information from the interface with the block signal station at Slependen. Element locking normally occurs when the information is not interpreted correctly by the computer. In this case, where there was an error in the software, the system did not go to a safe status, although an element lock occurred.

2. After the first error message occurred, the system received a new error message. Filament failure (a burnt-out lamp filament) from the opposite signal main entrance signal UD 4332. This is the signal pointing the opposite way to main exit signal N 4323 at Sandvika station.

3. After this, the relevant BSTR (area computer with software that processes information to/from the interface with Slependen block signal station) was reset. This was carried out by the on-duty signal personnel.

4. At the same time as the BSTR (see fig. 10) was reset, block signal A 357 at Slependen block signal station was showing the "expect to proceed" signal.

   On these four criteria were satisfied in the sequence outline above, the signal system and control of the distant signal were locked in the status they had when the system was reset, in other words "permission to proceed" in the distant signal for block signal A 357. This happened as a consequence of the error in the generic software for the BSTR.

Figure 10: Picture of object controller for signal N 4323

1.10.4 Inspecting the interlocking system

Immediately after the two serious incidents had occurred, an inspection of the interlocking system was undertaken, including artificial simulation of train operations, collaboratively involving representatives of the Norwegian National Rail Administration, Flytoget, NSB and the AIBN. This inspection did not manage to induce the fault. Later on, the interlocking system was simulated with realistic train operation, but these tests did not manage to induce the fault either. Since the uncertainty surrounding the interface (EF 180) to the interlocking system was real, it was decided that all interfaces with interlocking systems using the same type of system should be taken out of operation until further notice. The examination of the software for the SIMIS-C system at Siemens base in Brunswick gradually uncovered the error in the software.

The AIBN has recorded that the Norwegian National Rail Administration, in collaboration with Siemens, held an open, positive process in which NSB and Flytoget were kept informed constantly of any findings made in connection with this case.

1.11 Communications channels

Ongoing works or circumstances in the infrastructure which affect train operations are announced to personnel via T-circulars. These are issued by the train control areas, on a weekly basis and sorted into line sections. Other circumstances linked to train operations are announced in S-circulars that are drawn up by the traffic management authority at the National Rail Administration and issued for the scheduled route areas.

Orders and circulars were issued concerning the track works on the section, but this had no direct influence on the sequence of events.

Train sets type 69 and 71 were equipped with onboard radio and mobile phone.

The communication between the airport express drivers and the train controller was done over the onboard radio, while communication between the airport express drivers/locomotive driver and the operations centre was done using the mobile phone.

1.12 Organisational structures and management

1.12.1 Legislation and regulations

The legislation and regulations relating to this are:

- Act no. 100 of 11 June 1993 relating to the establishment and operation of railways, including tramways, underground railways and suburban railways etc. (Norway’s Railways Act),
- Regulations no. 1334 of 4 December 2001 concerning requirements for railways, including tramways, underground railways and suburban railways etc. (requirements regulation),
- Regulations no. 136 of 5 February 2003 concerning permission to operate railways, including trams, underground lines and suburban lines, etc. plus permission to operate on the national railway network (permission regulation)
- Regulations no. 1679 of 18 December 2002 concerning the training of staff in tasks that are crucial to traffic safety on railways, including trams, underground lines and suburban lines (training regulation).

These specify general requirements and regulations for the people driving and operating railways in Norway.

Chapter 2 of the requirements regulation describes the overall principles for work on traffic safety. It states that work shall be done constantly to improve traffic safety, and reduce the risk in so far as this is feasible. Barriers must also be established to combat the serious consequences of individual faults (the single fault principle).

Chapter 5, section 5-1, part one, paragraphs 2 and 4, of the requirements regulation describe the requirements specified for the use of analyses and criteria for acceptable risk.

Chapter 11 of the requirements regulation deals with requirements for track operation. Section 11-3 describes requirements concerning the drawing up of safety principles, and section 11-4 describes requirements for inspection procedures for signalling and safety systems. Section11-5 describes requirements for technical documentation. Section11-6 describes requirements for maintenance.

After the incident, the requirements regulation was replaced by Regulations no. 1621 of 19 December 2005 concerning the requirements for railway operations on the national rail network (the Safety Regulations).

The permissions regulation has been superseded by Regulations no. 1490 of 16 December 2005 concerning licensing, safety certification and access to operate traffic on the national rail network, and on safety certification to operate infrastructure (the Licensing Regulations) on the national railway network.

This report has been commented on the basis of the requirements regulation of 2001, since this was the current one when the serious incidents occurred.

Project design, construction and commissioning of electronic computer-controlled interlocking systems must be executed in compliance with CENELEC standards EN 50126, -128 and -129.

1.12.2 Rules of operation

The JD 500 series is the National Rail Administration’s system of technical regulations and among the items it describes are general technical requirements on signals - construction, project design and maintenance.

1.12.3 Work organisation and chains of command

Sandvika station is subordinate to Oslo train control area. The Track Manager is the owner of the system, and is responsible for ensuring that it is always in a state that complies with regulations. An operations and maintenance agreement has been entered into between the Track Manager and Operations, describing roles and responsibilities. For the Track Manager, this has been taken care of by the Technical Manager – Signals and inspectors are responsible for ensuring that the generic procedures (visits and inspections) are performed. This means that they should have a general overview of the status of the system, analyse the status, make any requirements evident and prioritise activities, as well as ordering assignments from Operations and for then following these up. This means that it is the National Rail Administration’s own personnel who carry out inspections and visits, as well as operations and maintenance duties.

1.12.4 Qualifications requirements for personnel

Any personnel carrying out servicing and fault correction duties on the various types of signalling plant (including the electronic interlocking system SIMIS C) must be qualified signal fitters. The AIBN is aware that signalling personnel may be instructed to correct faults on new and complex types of system, without their feeling that they have been given sufficient training for carrying out duties of this type. This was also the case in the incidents in question.

1.12.5 Resetting systems

Faults that remain in the system over a period of time are detrimental. To maintain the system's level of safety, a short response time is a precondition for fault correction. If this condition is not met, it may lead to a risk of simultaneous faults arising in the system, something that can have an effect on the level of safety. The supplier of the system believes that the safety-related conditions of use and preconditions are not being transferred satisfactorily from the project to the operational organisations, and that the signalling personnel who maintain the systems are therefore not familiar enough with these preconditions. It is important that the personnel should receive rapid, correct and supplementary fault information from the train controller prior to any intervention and potential resetting of the system being undertaken.

1.12.6 Procedures for internal checking and monitoring

It is the National Rail Administration's Track Manager for the section in question who is in control of the section of track on a daily basis. It is the National Rail Administration's own signalling personnel who receive first notification of faults, and who have to ensure that any faults in the interlocking system are corrected.

1.12.7 Procedures for managing contractors

Siemens had an engineering, procurement and construction (EPC) contract for supplying the safety system. The National Rail Administration had entrusted Siemens with delivery of the system, but performed testing while delivery was underway in collaboration with the supplier. The National Rail Administration's personnel themselves undertook final operational testing of the safety system prior to its commissioning.

1.12.8 Manuals and materiel procedures

No procedures had been drawn up for resetting this type of safety system at the time when the serious incidents occurred. The AIBN has been informed that procedures for resetting computer-controlled interlocking systems have been drawn up since then.

1.12.9 Norms for project design and construction, (Standards)

Gardermobanen (GMB):

According to the contract between Siemens and the GMB project, development, project design and construction of the safety system was supposed to be executed in compliance with the CENELEC standards EN 50126, -128 and -129. The standards were in the form of preliminary issues at this time.

The following versions of the standards were identified in the GMB agreement (Contract no. 1836 – Signalling system for the Gardermobanen railway line):

- Draft pr EN 50126
- Draft pr EN 50128
- pr EN 50129

At the outset, SIMIS-C was developed in accordance with MÜ 8004 (from 1997 in accordance with Safety Case ESTW) which is a product-oriented standard. It has been described in the safety documentation for Gardermobanen that the software amendments in SIMIS-C, in conjunction with its adaptation for the Gardermobanen railway line, have been carried out in accordance with EN 50128.

Sandvika-Asker:

The safety system on the Sandvika – Asker section was supposed to be developed, project designed and constructed in accordance with CENELEC standards EN 50126, -128 and -129. The system was supposed to be based on the generic system developed for Gardermobanen, and it was requested at the outset that amendments to this should be avoided. It was therefore the RAMS phases that covered the project design and construction that were relevant to this project.

1.12.10 Rules for maintenance of infrastructure

The National Rail Administration's technical regulations JD 552 describe maintenance – Signals on National Rail Administration infrastructure.

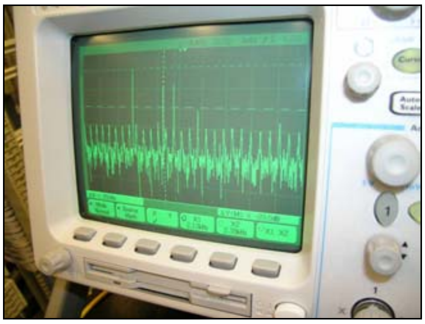

Figure 11: Oscilloscope measurement of noise conditions from cable to interface EF-180

During the course of the AIBN's investigation, abnormal flashing frequencies were observed in the LEDs in the EF-180 interface system. During test measurements, it was confirmed that there was variable noise on the interface with Slependen block signal station (see fig. 11). EF-180 is an interface for transferring signal information between the safety system at the block signal station and the interlocking system at the station.

The AIBN has obtained information that the telecommunications cable used to transfer data has been joined together out of new and existing cables.

This interface is sensitive to noise, and it is therefore important that cables used for this interface are of a good standard. This is admittedly not safety-critical, but it could give rise to operational faults due to an element lock occurring. Such a circumstance could have been a contributory factor in inducing and making evident the software error in the interlocking system.

1.12.11 Balises/ATC

Balises in partially equipped areas (DATC) are controlled by the signals on the section. The balises on fully equipped ATC areas (FATC) are controlled by the process in the computer for the electronic interlocking system. In this case, the interface between a fully equipped ATC area and a partially equipped ATC area was at main exit signal N 4323 at Sandvika station.

1.12.12 Train control centre and traffic management

The traffic control centre controlling Sandvika station is located at Oslo Central Station.

The reason for the fault report by the driver of the airport express not being responded to earlier, was that the train controllers on duty were in some doubt as to whether it really could be a fault in the safety system. In addition, incident 2 was not reported to the train controller immediately by the locomotive driver in train 12207. Nevertheless it was gradually decided that the signal aspects should be tested when another train passed by. The driver on Airport Express 13907 was given the instruction to observe the signal aspect on N 4323 as the train passed. This observation proved to agree with previous reports of an incorrect signal aspect. At that time, the on duty signalman was contacted and two men travelled immediately to Sandvika station and reset the system.

There was previously a lack of clarity concerning the way the onward journey of airport express 13905 should be arranged, since the train controller had not been involved in the telephone conversation between the airport express train driver and the operations manager of the airport express and the choices that had been made. It is important to emphasise that it is the train controller who is responsible for the flow of traffic.

1.12.13 Locomotive driver/airport express train driver

The AIBN has interviewed the locomotive driver of NSB train 12207. The information from the airport express train drivers has been retrieved from the call log at the traffic management centre at Oslo Central Station.

1.13 Recording speed measurement equipment and datalogger

1.13.1 Call log/telephone log

The call log was played back in the traffic control centre at Oslo S in conjunction with the National Rail Administration's accident commission.

1.13.2 Signal log

After the incident, logs of the different train movements before, during and after the serious incidents were extracted. The fault in the interlocking system at Sandvika station was not identified using these logs, but the printouts were very helpful in establishing the time of the incidents and the movements in the interlocking system.

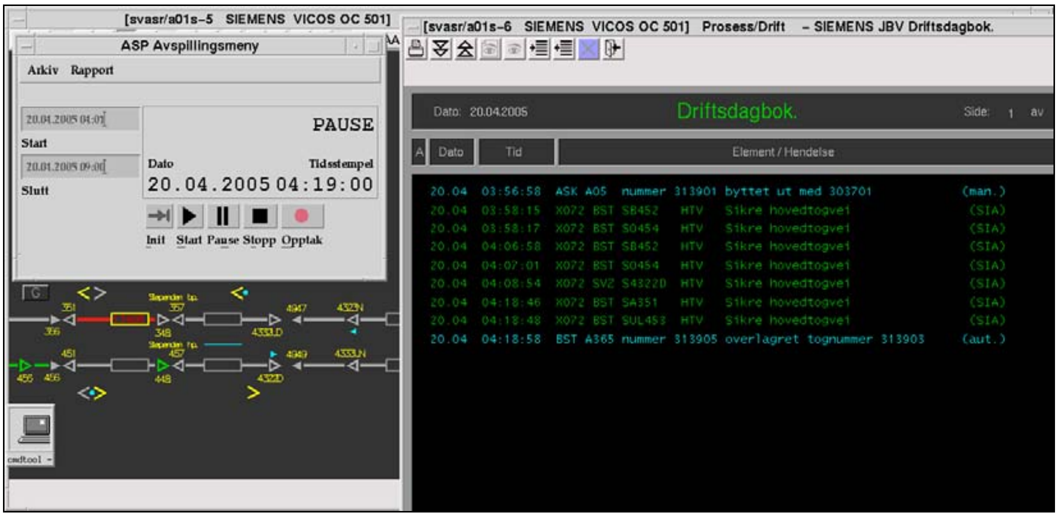

Figure 12: Signal log printout

The printout of the signal log in figure 12 shows the time when train 13905 entered the same block section as train 13903, and the display of train numbers on the screen were placed on top of one another.

1.13.3 Recording train speedometers

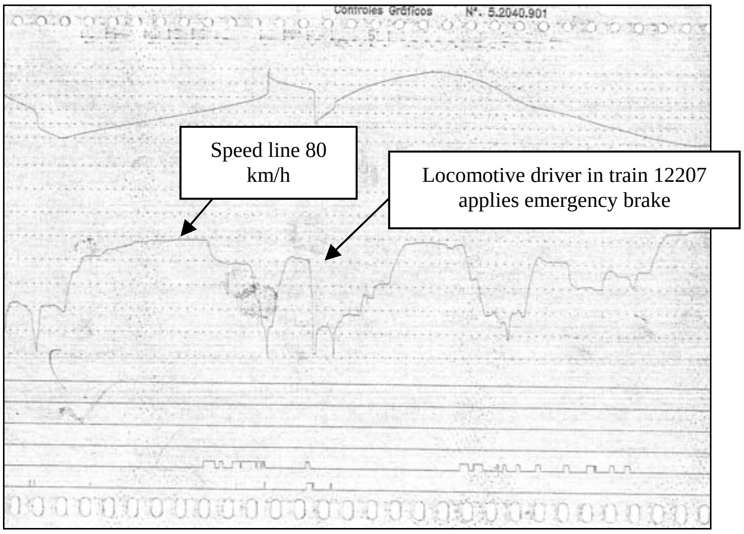

Figure 14: Speed printout (Hasler) for train 12207

Train 12207:

The printout of recording speedometer (Hasler) for train 12207 shows that the train was moving at a speed of almost 82 km/h just before the locomotive driver applied the emergency brake.

Airport express train 13905:

The Teloc printout from airport express train 13905 showed that the train had been moving at a speed of 80.45 km/h as the train passed block signal A 357 at Slependen block signal station showing the "stop" signal. The airport express train driver had actuated the emergency brake before the train passed the signal. Otherwise, the train's ATC system would have stopped the train when it passed the block signal at stop.

1.14 Medical information

Not relevant to any of these incidents.

1.15 Fire

No fire occurred during any of these incidents.

1.16 Survival aspects

There could have been serious consequences if the locomotive driver in train 12207 had not applied the emergency brake and managed to stop the train in time. He only had a time window of around 2 seconds to detect the airport express train's 2 red direction lights (end signals) in the area to the left of the superstructure at Slependen holding point. This is illustrated in figure 15.

Figure 15: The line of sight from the locomotive driver's cab in the direction of Slependen block signal station. Airport express train 13905 had stopped and was located behind the superstructure at Slependen holding point.

Figure 16: The trains' stopping positions after incident 2. This photo is a photomontage showing the estimated distance between the trains.

1.17 Investigations

The AIBN has undertaken its own investigations into the incidents. In addition, external consultants have been used, and they have gone through the safety documentation described in the appendix, and relevant approval processes.

1.17.1 Investigation concerning development, project design and construction of the safety systems

It was established that the fault in the safety system (SIMIS-C) at Sandvika station was linked to a generic software module developed in conjunction with adapting the safety system during the construction of the Gardermobanen railway line. For that reason, two different approaches have been chosen in this investigation:

- a review of the process for the development and adaptation of the generic system in SIMIS-C for Gardermobanen to find underlying reasons for the fault occurring

- a review of the process in conjunction with the project design and construction of a new safety system (SIMIS-C) at Sandvika station to evaluate whether the fault could have been identified before the system was commissioned.

The investigations are implemented as a combination of a document review and interviews with the people involved. Documentation has been obtained from the supplier (Siemens), the National Rail Administration and Sintef. Interviews have been held with personnel from the supplier and the National Rail Administration. In addition, interviews have been held with personnel who were involved in the GMB project, including Sintef as assessor.

Documentation that has been reviewed has been included in the list of documents, Appendix 1.

Adaptation of SIMIS-C for Gardermobanen

The sections below contain a description of a number of conditions that have been investigated and that could have had an influence on the process of adapting SIMIS-C for Gardermobanen.

Contractual conditions / project organisation

The Gardermobanen (GMB) contract was arranged as a turnkey delivery in which the supplier was responsible for the complete supply of signalling and safety systems, including remote control and ATC.

For GMB, the choice made was to use the standard contract NF92, which is a contract for engineering, procurement and construction (EPC) contracts. It was the first time this type of standard contract had been used for signal supplies, and neither the client nor the supplier had any experience of using this. At the start of the project, it was expected that the supplier would supply a finished system without particular involvement on the part of the GMB project. However, gradually, it was seen that the project required to a greater extent to get involved in the supplier’s process as things progressed. This was to ensure that the finished product would satisfy the requirements of Gardermobanen and the National Rail Administration, particularly functional requirements, and for maintaining progress in the project.

This involvement was generally carried out without any form of formal review or approval but, according to those involved in the project, documentation to a certain extent was in the form of minutes of meetings.

The project was under severe pressure of time to have the system completed for the opening of Oslo Airport Gardermoen.

Specifications

The specifications included as appendices to the contract were in Norwegian. They were translated into English and interpreted by the supplier who was using German as the working language. Clarifications from the National Rail Administration were also transmitted in Norwegian to the supplier. Basic data for developing the interface to the relay line block in the GMB project were generally based on relay schematics.
Since the requirements specification was in Norwegian, a translation agency was engaged to translate it to English. The translation had a poor technical foundation and was therefore designated “not a good process” (stated by the assessor). As regards the clarifications, these were translated by Siemens’ own people in Norway.

The relay schematics were interpreted by the supplier’s resource personnel in Germany and the functions implemented in the system. With Gardermobanen personnel, the supplier went through the functions as the project progressed in order to ensure the most correct functionality possible.

As regards the line block functionality in particular, experience from the GMB project indicated that the supplier personnel who carried out the work on developing and implementing this were highly competent and had had experience of developing similar functionality for other infrastructure administrations. This meant that the work was carried out without any significant changes or comments from Gardermobanen or the National Rail Administration.

Gradually it proved necessary in this project to have an extended, improved dialogue to ensure that the supplier’s solution would satisfy customer requirements. At first, this was dealt with in the form of working meetings and documented in minutes of meetings and, in the case of formal clarifications, in the form of letters and amendment orders. In retrospect, it was seen that this phase could advantageously have been implemented by having a more thorough and more formal review of the supplier’s design documents before the development started. In retrospect, it has been stated that many of the uncertainties that arose during the FAT (“Functional Acceptance Test”) could have been avoided.

RAMS process

SIMIS-C is a well-proven safety system that was developed before the days of the EN 50126, -128 and -129 standards. Adaptation of SIMIS-C for Gardermobanen should, in accordance with the contract between Siemens and Gardermobanen, take place in compliance with EN 50126, -128 and -129 standards.

At the time the contract in conjunction with Gardermobanen was entered into, the EN standards were provisional versions. They were subject to minor changes during the course of the project before eventually being issued in their present form.

At the time the project was implemented, the supplier had not fully implemented the EN 50126, -128 and -129 standards in its development process, but was in a transition from the MÜ 8004 to the EN standards.

MÜ 8004 is a product-oriented standard which focuses on building safe systems out of safe subsystems/components. MÜ 8004 also specifies requirements for how the programming and documentation of software in safety systems should be carried out. The EN standards are more process-oriented standards that focus more on an analytical approach. As regards the Safety Case, EN-50129 has adopted the structure for a technical safety report from MÜ 8004.

The Safety Case for ESTW (SIMIS-C) at Gardermobanen states that software amendments were performed in compliance with EN 50128. It also states that EN50126 was adhered to in the development and validation process for the amendments in the generic part and the application part.

Hazard analyses form an important part of the risk-based process described in the EN standards, and must be carried out in all phases of the project, right from the concept development phase. No hazard analysis was carried out in the GMB project during the course of the first four phases of the lifecycle process described in EN50126. A total of 3 hazard analyses have been identified in the GMB project:

- System Hazard Analysis
- Functional Hazard Analysis ATC
- Operating Hazard Analysis

“Wrong input/output in BSTR” is dealt with in the System Hazard Analysis, but only at a general level. The analysis does not go into individual modules, subsystems or the development process. Neither does it direct any particular focus onto the interfaces. It appears also that the analysis was performed at the end of the development and not at the beginning as is laid down in the standard.

The combination of the failure modes and incidents that led to the safety-critical incident at Slependen was not identified as a possible combination in the development process (by means of hazard analyses or testing).
Through a process in which the supplier identified non-conformances with the EN standards and in which the customer and assessor made the same assessment, it was found that the supplier’s safety process was satisfactory, although not all parts of the EN standards were adhered to. An important precondition for accepting the supplier’s method of implementing the project was that Siemens used an internal, independent party for verification and validation (Prüfleitstelle).

Sandvika – Asker project

The generic part of SIMIS-C (in which the fault was found) was regarded as having been validated and approved, and therefore this part was not validated specifically in conjunction with SIMIS-C at Sandvika station.

Project design and construction of a new safety system at Sandvika station was part of the Sandvika-Asker project that also included a new safety system at Asker station, and on the new double track between Sandvika and Asker.

The generic system at Gardermobanen was only formally approved (type approved) by the National Rail Administration in summer 2005. The reason behind there not being any formal approval has been stated as being formalities and not functional or safety-critical deficiencies.

In the supplier's safety plan for the project, the safety strategy is defined as being:

- Identification of differences in requirements between the GMB project and Sandvika – Asker
- Show that the solution for Gardermobanen fulfils the requirements
- Come to agreement on a solution with the customer

The supplier has gone through all of the requirements for the Sandvika – Asker project and analysed whether the functionality of the generic system from Gardermobanen satisfies the requirements for Sandvika - Asker. This analysis is documented in "Safety Requirement Tracing Matrix" which concludes that it is not necessary to make any changes in the generic system (functions), only in project designed (system-specific) data.

On the basis of no changes having been made within the generic system (functions), the further safety process focused on the system-specific amendments from Gardermobanen. This has been documented, for example, in the supplier's verification and validation plan.

Neither in the generic safety documentation nor in the maintenance manuals for the system there was any limitations linked to the functions/situations connected to the fault situation in question (element lock function, "restart" of the BSTR, lamp filament failure, or combinations of these).

1.18 Useful investigation methods

No investigations have been carried out which require any special discussion.

2. ANALYSIS

Before its analysis of the incident, the AIBN gathered factual details and made investigations both in relation to the implementation of the new safety system at Sandvika station and the development process of the generic system for the SIMIS-C safety system on Gardermobanen.

In parallel with this, the National Rail Administration and the supplier, Siemens, undertook their investigations to find the causes of the fault. The direct cause of the incident at Slependen is described in the documentation from the National Rail Administration and the supplier. Once the fault had been discovered, the supplier undertook upgrading of the systems concerned both at Sandvika and Gardermobanen, and the National Rail Administration tested and commissioned the systems. In conjunction with the investigations, there has been a review and confirmation of faults being found, the software has been corrected, and the amendment has been tested, documented and evaluated.

So, the investigations have not been carried out with a view to finding the cause of the block signal showed "stop" at the same time as the associated distant signal showed "expect to proceed" since the fault had been found. The investigations have been made with a view to finding the underlying cause of the programming error "surviving" a verification and validation process carried out in conjunction with Gardermobanen and Sandvika station.

The analysis looks at both the development of the generic system that took place in conjunction with Gardermobanen, and its implementation at Sandvika station.

2.1 Technical and operational causal factors

2.1.1 Adaptation of SIMIS-C for Gardermobanen

This part of the analysis is directed at the development process for the safety system that took place in conjunction with the GMB project. In particular, the analysis is aimed at the part of the safety system in which the fault was located (interface with line block).

The analysis has concentrated on two circumstances:

1. identifying weaknesses in the process that was carried out in the development of the software concerned

and on that basis

2. evaluating whether processes and methods described in the EN 50126, -128 and -129 standards could have reduced the probability of having equivalent faults.

Contractual conditions / project organisation

The Gardermobanen (GMB) contract was arranged as a turnkey delivery in which the supplier was responsible for the complete supply of signalling and safety systems, including remote control and ATC.

In recent years, there have been several projects involving country-specific adaptation of safety systems in the National Rail Administration, and experience from these indicates an absolute requirement for the customer's strong involvement, in order to obtain a shared understanding both of requirements and functionality. This was also confirmed by the interviews held with personnel involved in the GMB project. The project perceived that it would have to become more involved as progress continued, although this was not in accordance with the intentions contained in the agreement with Siemens.

However, it is rather improbable that greater involvement on the part of Gardermobanen from the start of the GMB project would have contributed to the detection of the fault in the safety system. This is because Gardermobanen's resources could not be expected to possess the necessary knowledge of internal error situations and details of the software modules in the system.

Operating conditions

The personnel working on electronic computer-controlled interlocking systems ought to have had good training in this type of safety system, since these systems are fundamentally different to conventional relay-based safety systems in which a signal fitter is principally trained. The AIBN considers it to be unfortunate that only a limited number of people in the National Rail Administration had thorough competence in the correction of faults in this type of interlocking system.

The AIBN is aware that after the incident training courses were held under the direction of Siemens, to update signals personnel on electronic computer-controlled interlocking systems.

The train controllers did not immediately take action after the first incident. The AIBN would like to point out the importance of train controllers rapidly taking the necessary action in order to safeguard train operations when serious faults in signals are reported.

It became known after the two serious incidents that the engine driver of airport express train 3816 on Sunday 17 April at time 0112 reported to the train controller a corresponding signal observation involving the distant signal at signal N 4323 at Sandvika station. The AIBN was not notified of this incident. It is important to point out that serious incidents like this should be reported immediately within the National Rail Authority's internal systems, in order to ensure that similar problems are dealt with much earlier.

2.2 Causal factors related to safety control and management

2.2.1 Specifications

The specifications that formed appendices to the contract were in Norwegian. These were translated into English and interpreted by the supplier who was using German as the working language. Clarifications from the National Rail Administration were also transmitted in Norwegian to the supplier. The basis for developing the interface with the relay line block in the GMB project consisted primarily of relay schematics.

It is rather improbable that uncertainties concerning the specification were the reason for the fault occurring, but it is probable that a more formal and analytical process concerning examination of the supplier's design documents might have detected deficiencies in the design.

It is rather improbable that an improved process concerning the translation of the Norwegian requirements specification into English could have prevented this particular error arising in the software. This is because the failure situation is based on highly detailed system conditions that were not included in the original requirements specification. Neither, therefore, is it probably that the failure situation arose because of any weaknesses in the actual requirements specification, since it arose as a consequence of circumstances that are system-specific and that do no naturally belong in a function-oriented requirements specification.

There is nothing to indicate that deficient specifications for the line block function have been the cause of the fault occurring. Without the supplier's knowledge and experience in this field, and the customer's involvement, this could have become a problem area in the development process and have given rise to delays in the project.

2.2.2 RAMS process

SIMIS-C is a well-proven safety system that was developed before the days of the EN 50126, -128 and -129 standards. Adaptation of SIMIS-C for Gardermobanen should, in accordance with the contract between Siemens and Gardermobanen, take place in compliance with EN 50126, -128 and -129 standards.

For software development, it has been documented that EN50128 has been adhered to in most areas. This was accomplished by making crosschecks and documenting that requirements in EN 50128 were addressed within the process that Siemens has adhered to (based on MÜ8004). Methods have been used which correspond to the "HR" (Highly Recommended) requirements in the standard. This is made clear in the documentation both during development and during the validation of the system.

This was found to be adequate both by Siemens' internal and independent validation unit (Prüfleitstelle) and the assessor.

The documentation that has been reviewed in conjunction with this analysis and which describes the methods used by the supplier during development and testing of the software indicates that the error ought to have been discovered. However, it appears clear that the combination of input variables and failure states that led to the situation at Slependen, was not identified in either the development or the validation process. This is also confirmed by the supplier in conjunction with its own examination of the incident.

The question is whether, despite it being possible at the outset to establish that EN 50128 is being adhered to, the methods processed were still not good enough to prevent this type of fault.

The fault that arose was based on several incidents occurring in a specific sequence. To be able to look ahead, and to prevent this type of fault being able to occur, systematic methodology must be used to identify all conceivable states and failure modes that a system, subsystem or module can have. It is here that, in a systematic review of conceivable hazards at an early phase of the development, the EN standards should contribute to enabling the identification of possibilities for this type of fault, thereby obtaining an increased focus on these both during development and during validation.

To obtain a satisfactory analysis as described above, there is a series of circumstances that must be known:

- The properties and methods of working of the system, subsystem or module
- Adjacent systems' properties and methods of working
- Operations and maintenance procedures
- External influences

The challenge in this type of analysis is to bring together a group of people who prossess adequate competence in all of these circumstances. This can be a particular challenge for the system supplier when a system is to be adapted for a new, unknown infrastructure administration.

In the GMB project it was gradually realised that the project team and Siemens would have to work together to achieve the correct functionality. This method of working was used principally for reviewing clarifications and gaining the right functionality, and not for identifying failure modes or failure states for the system and its interfaces.

The three hazard analyses that were drawn up were at a general level and not designed to pick up on combinations of faults or failure modes in the various software modules or in the interface between the modules. These analyses were also performed largely after development and validation had been carried out. This was not in compliance with the intentions of EN 50126.

Based on the investigations that were undertaken, the following have been discovered:

- no hazard identification was carried out early in the project (phase 3 in the lifecycle model in EN 50126)
- no hazard analysis was presented by the client (Gardermobanen) (phases 1 and 2 in the lifecycle model in EN 50126) as a basis for the supplier’s analysis
- there was no special focus on interfaces

There are therefore reasons to state that EN50126 has not been adhered to in full for the adaptation of SIMIS-C, and that this could have contributed to the non-detection of the error that remained in the generic system.

No automated tests were carried out on the software either. Had such tests been used, it would have been possible to a much greater extent to increase the scope of testing and test combinations that are not practically feasible with manual testing. With extended use of automated software testing, errors of the type identified in the SIMIS-C system would probably have been detected during testing.

Had the EN 50126, -128 and –129 standards been implemented fully in the development process, there would probably have been a greater chance of detecting the error that remained in the generic system in SIMIS-C. This is attributed primarily to the fact that a more thorough hazard analysis would have been performed at the start of development, and would have focused more on interfaces.

However, it must be emphasised that the EN standards were only available in early, provisional versions, and that no one had any substantial experience of using the standards, anywhere in Europe, at that time. It is therefore reason to assume that the effect of a more rapid implementation of the standards at Siemens, viewed as a whole, would not necessarily have made a positive contribution in relation to the established and familiar safety process they then had.

2.3 Causal factors related to operating permits and public authority approval

Causal factors relating to operating permits and public authority approval only concern the Norwegian National Rail Authority’s internal type approval.

2.3.1 Project design and construction of new safety system at Sandvika station

The generic part of SIMIS-C (in which the fault was found) was regarded as having been validated and approved, and therefore this part was not validated specifically in conjunction with SIMIS-C at Sandvika station.

The safety process selected in the Sandvika–Asker project is based on accepting principles about the generic part of an already approved system not having to be validated and verified again to gain approval. This is a principle also laid down in the EN 50126, -128 and -129 standards. Testing and approval would then be based on the system-specific part. The generic system is regarded as having been approved on the basis of associated generic safety documentation (the Generic Product Safety Case).

It is debatable whether a new validation of the generic system ought to have been performed in conjunction with Sandvika, in view of the fact that the process in compliance with the EN 50126, -128 and -129 standards had not been carried out in full at Gardermoen, and that the system had not been finally approved by the National Rail Administration. On the other hand, there are several arguments to indicate that this should not be necessary:

- there had been a 6-7 year period of operation/experience of the system on Gardermobanen
- the system had been in use for a longer period in other administrations (including VR in Finland).
- formalities were all that prevented a final approval from the National Rail Administration being given earlier.

3. CONCLUSION

The error that caused the serious incidents was related to the generic system that had been developed and validated in conjunction with the implementation of SIMIS-C on Gardermobanen. The error did not occur as a result of the implementation of SIMIS-C at Sandvika station. In accordance with established principles, which are in line with the EN 50126, -128 and -129 standards, it should not be necessary to validate a generic system that has already been approved. It may therefore be concluded that it could not have been expected that this type of error, which existed in the generic system, should be detected in the implementation of SIMIS-C at Sandvika station.

On the basis of the investigations that have been carried out, there is no evidence that the process in EN50126 had been adhered to in full in the adaptation of SIMIS-C for Gardermobanen. The necessary hazard identification and analyses had not been carried out during the earlier phases, as is required by EN 50126. This could have been an indirect cause of the error in the generic software not being detected in the development and validation process, despite adherence to MÜ8004, which generally satisfies the requirements of EN 50128.

If the technical fault that occurred is considered, the fault incidents; lamp filament failure, the element lock and restart of the BSTR are all normal incidents that can occur at a certain frequency. The fact that, with these occurrences as a background (although they have to occur in a specific sequence), it is possible for this type of fault to occur, it ought to be possible to identify them in order to enable measures to be introduced to prevent them from recurring. If most of the validation is based on testing, it is almost impossible to define all conceivable tests to allow an error such as this to be detected without, in advance, having had an analytical approach involving hazard identification and analysis. This is particularly important for gaining a necessary overview of the entire system, including external interfaces, forms of operation and other influences outside the system itself. If it is difficult to analyse different contexts and combinations, the testing methods used ought to include automated methods that would be able to compensate for this.

3.1.1 Deficient overview of documentation

During enquiries about documentation, it proved difficult to find the generic documents belonging to the systems at Sandvika – Asker and Gardermobanen. It might appear that the documents were not archived appropriately with regard to their belonging to a generic product used in several systems. As an example of the deficient document overview, it can be mentioned that to get hold of safety documentation for Gardermobanen a free-text search was run in the document database. The result of this search appeared rather random and unclear. Another example is the assessor’s report for Gardermobanen, to obtain which it was necessary to go to SINTEF.

3.1.2 Handover from development project to operation

In reviewing the documentation for Gardermobanen it was difficult to identify which documents and which conditions of use were transferred from the development project to operations. Important relationships and conditions of use can easily disappear in the huge volume of documents generated by a project of this kind.

3.1.3 Amendment of test procedures

The AIBN is aware that the supplier has made amendments to the test procedures for testing interfaces.

3.1.4 Operating conditions

When serious signalling incidents are reported, it is important for this immediately to be dealt with in a manner that is reassuring from a safety perspective, to ensure that hazardous situations are averted.

3.1.5 Other observations

Unnecessary flashing LEDs were observed on the interface at the Slependen block signal station. Using measurements it was established that variable noise was present on the interface. This could have been linked to the frequent faults (element locks) that had occurred. The interface is sensitive to noise, and it is therefore important that cables used for data transfer to this interface are of a good standard, in order to avoid operating failures. Loose gauge wires and temporary connections at Slependen block signal station, and in the relay room at Sandvika station, left an impression that the situation at the interlocking system was under observation with preparations for improvement.

The AIBN is of the opinion that Siemens has been dealing well with the problem, and has done a thorough job of finding the fault and the cause of this, and has been open and helpful during this process.

4. SAFETY RECOMMENDATIONS

The investigation of this railway accident/serious railway incident has discovered several areas in which the AIBN considers it necessary to put forward safety recommendations with the purpose of improving railway safety.

The investigation report was sent to Norway's Ministry of Transport and Communications which is taking the necessary action to ensure that due consideration is given to the safety recommendations (ref. section 16 of Regulations no. 378 of 31 March 2006 regarding public inquiries into railway accidents and serious railway incidents, etc (the Railway Inquiry Regulation).

No immediate safety recommendations were put forward as a result of these incidents. The AIBN recorded that the supplier of the safety system quickly recommended that the Norwegian National Rail Administration should take all interfaces of the same design out of operation on the other sections of the same type of safety system. All corresponding interfaces were therefore taken out of operation until the fault was corrected and new operational testing had been carried out.

Safety recommendation JB no. 2007/02

The AIBN advises the Norwegian Railway Inspectorate (Statens Jernbanetilsyn) to assess recommending to the Norwegian National Rail Authority that it should review its RAMS process in compliance with EN 50126 for all elements and phases of equivalent projects, both within its own organisation and at its subcontractors in order to ensure the best possible adherence to standards and their intentions. An understanding of why this is important ought to be created.

Safety recommendation JB no. 2007/03

Each time a new safety system is to be implemented, a safety-related challenge arises in relation to interfaces with existing safety systems, whether these are relay-based systems or electronic systems.

The AIBN advises the Norwegian Railway Inspectorate to assess recommending to the National Rail Administration that it should focus in particular on interfaces, both from a systems and an operations point of view when implementing new safety systems.

Safety recommendation JB no. 2007/04

The train controllers did not immediately take action after the first incident. It is important to point out that serious incidents like this should be attended to and reported within the National Rail Authority’s internal systems, in order to ensure that similar problems are dealt with much earlier.

The AIBN advises the National Railway Inspectorate to assess recommending to the National Rail Administration that it should review procedures for handling reports of signalling faults coming in to the train controllers, to see whether this is appropriate.

Recommendations in relation to other observations:

The AIBN is aware that the circumstances mentioned in the safety recommendations in subparas. 4.4 and 4.5 shall be taken care of by the safety regulations’ requirements for technical documentation and for a safety monitoring plan. The AIBN nevertheless chooses to encourage assessment of these circumstances based on the potential enormity of this incident.

Safety recommendation JB no. 2007/05

The AIBN recommends that the National Railway Inspectorate should assess recommending to the National Rail Authority that it should draw up an appropriate method of storing generic system documentation, including safety documentation, to ensure that this interconnects structurally, and that it should always be easy to find a current version of the documentation for all National Rail Administration systems and plant.

Safety recommendation JB no. 2007/06

The AIBN recommends that the National Railway Inspectorate should assess recommending to the National Rail Administration that they should focus more, when systems are being handed over from development project to operations, on identifying the documentation which forms the basis for operating and maintaining the system, and that there should be a system in place for forwarding and monitoring conditions of use. This is particularly important for RAMS-related conditions of use.

SUPPLEMENTS

None

5. APPENDICES

1. Summary of current documentation that is relevant to the fault, and which has been used as basic material for this report.

Accident Investigation Board Norway
Lillestrøm, 20 February 2007