Risk management of Operators Interpretation of Information from New Technology

IRSC 2019, Eva-Lotta Högberg, Swedish Accident Investigation Authority

Introduction

New innovations and technology make our every day life and work life easier, inspiring and more efficient. It enables Infrastructure Managers and Railway Undertakings to develop innovative, high-tech operational systems, vehicles and safety barriers. At present, a large amount of information can be shared instantly through different mediums and devices. But how do we ensure and demonstrate safety in new technology? And how do we make sure that risk management keep up with the pace in innovation? Do the users have the competence to use the new technology in a safe manner?

This paper will discuss those questions based on the lessons learned from an accident in the north of Sweden. The accident occurred despite of a well thought through implementation of a new computer-based planning and documentation tool, STEG, that gave a dynamic, on-screen visualization of the train plan. A tool developed by the Infrastructure Manager in collaboration with a University. What was lacking in the risk management process?

Two freight trains (9207 and 6032) collided on a straight section of track on the single track line between the stations Arnemark and Piteå on 21 September 2016. Train 9207 was proceeding under clear signals at normal speed (90 km/h) while the other train, 6032, was travelling under speed restrictions (driver required to be able to stop the train within the visible distance of track, max 40 km/h), after being permitted to proceed past signal at “Danger” when leaving Piteå.

At the moment of impact, train 6032 had come to a standstill, while train 9207 was still moving at approximately 50 km/h. Both locomotives sustained serious damage and a number of cargo wagons were irreparably damaged. However, no one was seriously injured.

The checks that the traffic controller performed before allowing train 6032 to proceed past signal at ”Danger”, had failed to show that train 9207 was in fact still occupying the line section.

Why did the checks fail? Why did the traffic controller come to the conclusion that it was safe to allow train 6032 to proceed past signals at ”Danger”? And what kind of support did the newly introduced, planning and documentation tool give the traffic controller?

This paper will describe how the traffic controller from the information he could gather and evaluate, concluded that the occupation of the line section was due to an improperly occupied track circuit (a technical problem) and that train 9207 had in fact arrived in Piteå. The paper will describe how the traffic controller also trusted the notes on a form more than the information provided by the traffic control system and the planning and documentation tool.

Furthermore, the paper will discuss the underlying causes on a systemic level such as the fact that the Infrastructure Manager had not examined how the newly graduated traffic controllers regarded the status of the different tools (both computer and paper–based) and how they interpreted the information from those tools. When co-developing the new planning tool the Infrastructure Manager used only experienced traffic controllers as reference group. In addition, the Infrastructure Manager had not anticipated that the introduction of the new planning tool would have an impact on the principles for the documentation of traffic events.

Finally, the paper will summarize key points in risk management that are easily forgotten when applying the methodology.

Background – traffic control, monitoring and documentation

The line Nyfors–Arnemark–Piteå is a single track line, under centralized traffic control (CTC) from Boden. Technically, CTC requires electric interlocking plants at the stations and automatic line blocking system for the line sections between stations. The actual, technical safety of operations is realized in the local systems (interlocking plants and line block systems), but monitoring and operative maneuvers are done by remote control systems in the traffic control centre (TCC). See figure 1.

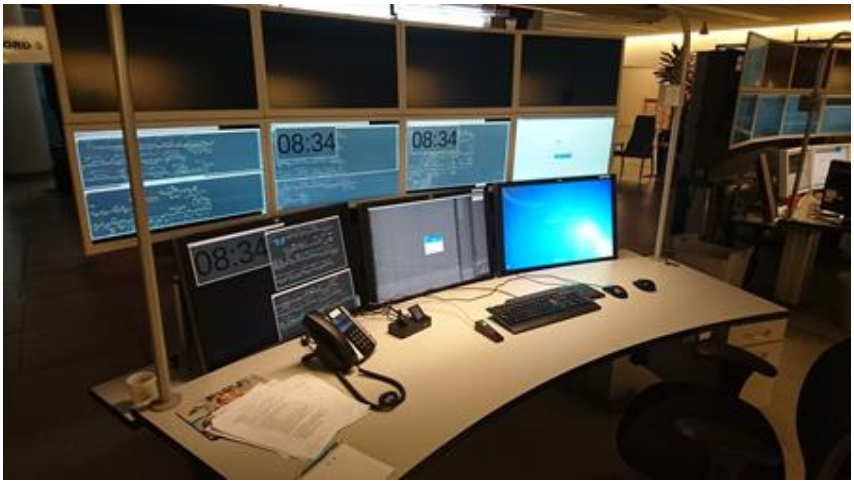


Figure 1. Traffic control centre.

In the TCC, traffic controllers watch their respective areas on screens (or equivalent equipment) and ascertain that train routes are set in accordance with the train plan and the actual situation and perform whatever changes that are needed to handle deviations from the plan (delays, early trains etc.).

Station track layout and line sections are presented visually on monitors where set routes, signal aspects and vehicle movements can be seen. Interaction with the system is by mouse clicks and object menus. Indications given by the remote control system are not considered to be reliable by themselves, but indication changes, in conjunction with logical vehicle movements, and as responses to object orders (e.g. re-setting a switch) given by the traffic controller, are considered reliable. In Boden TCC, the control and monitoring system is called Argus. See figure 2.

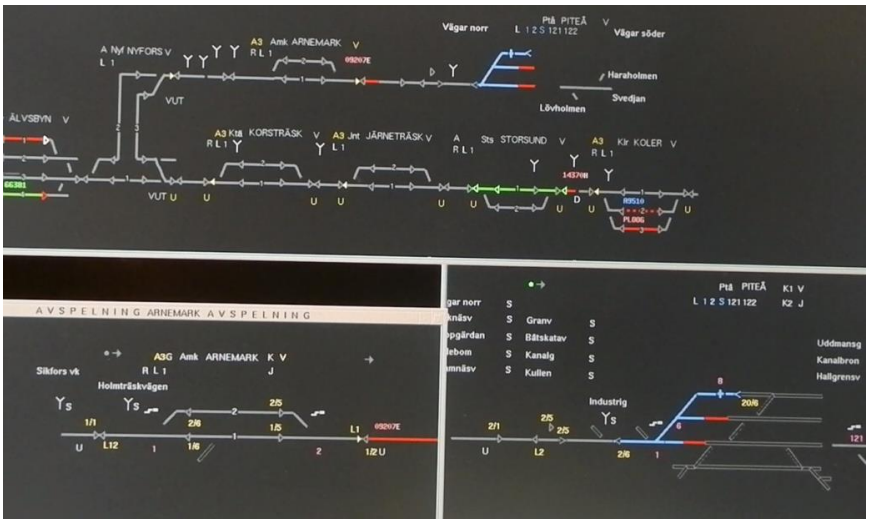


Figure 2. Traffic control system "Argus".

A traffic controller normally manages an area with more than one railway branch/line, each with several stations and line sections. In the case at hand, the Nyfors–Arnemark–Piteå branch is only a small part of the area to be managed by the particular work shift allotted to the traffic controller who was in charge when the accident occurred.

As a result of the Train Plan (established yearly by the Infrastructure Manager) a “train order” can be derived for every single track line section between two stations; it shows the successive order in which trains are allowed to occupy a line section between stations. In a system with manual traffic control (telephone block), this “train order” is all-important, as it in actual practice constitutes the work instruction for the traffic controllers controlling the line section. Changing the train order requires a fairly complicated process involving more than one person. In a CTC area, with fully operational technical safety systems, the traffic controller can change the train order without consulting anyone, according to the needs of the situation.

The train plan for each 24-h period is available on paper in graphical format, “the graph”. Trains are presented as lines in an X-Y diagram, with “time” on the X-axis and “distance” (stations and line sections) on the Y-axis. This plan, “the graph”, is the base for traffic controller planning and actions. Deviations are noted on the paper, together with any other pertinent information, according to special instructions about annotations for traffic control duty.

In Boden TCC, the paper (hardcopy) system has been superseded by a computer-based system called STEG that gives a dynamic, on-screen visualization of the train plan and the actual result of planning and actions taken by the traffic controller. “The graph” is shown on a screen, with a section for “the future” and a section for “the past”, divided by a line showing the real time, which moves as time passes. See figure 3.

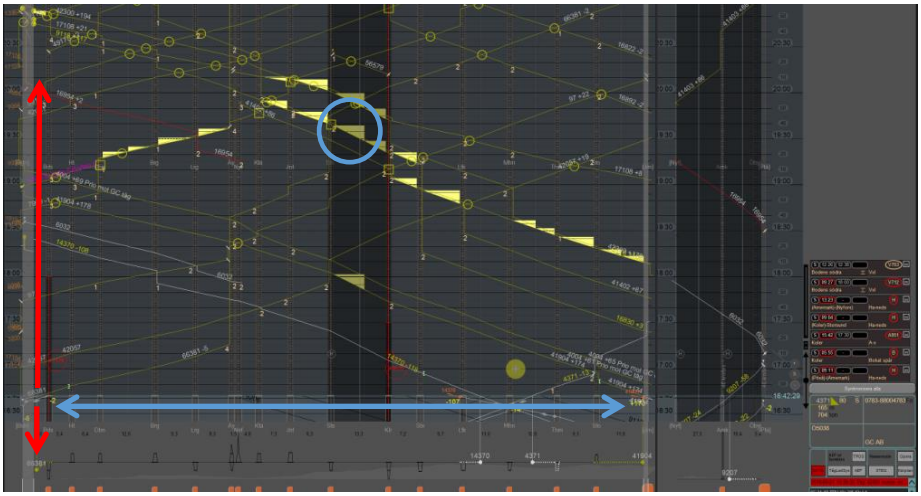


Figure 3. STEG. The red arrow upwards shows present to future and the red down arrow shows the past. Along the blue arrow is the stations on the line. The trains are represented by yellow lines and the yellow triangles are a help function to avoid train conflicts.

Trains are still presented as lines in an X-Y diagram, but in STEG “time” is on the Y-axis and “distance” (stations and line sections) on the X-axis. Planning into the “future” is done by the traffic controller by manipulating the elements of the plan, e.g. moving the line of a delayed train, or marking a track closed for a possession, but actual events (“the past”) are recorded with the aid of information collected from the traffic control system.

The STEG system has a module called AEF, that can transfer instructions directly to the traffic control system, according to the plans laid by the traffic controller, but this module is not used regularly and

not by all traffic controllers. When used to its full capability, the system could be said to realize the idea “doing by planning”, but reliability has not been good enough to encourage a full-scale implementation of the AEF module.

Annotations corresponding to the ones made on the paper plan (“the graph”) can be made in STEG using the graphical interface and a mouse/keyboard. Some notations, e.g. a particular train running through a particular station, are noted automatically by STEG, using information collected from Argus (train number, occupied track circuits, signal aspects) and from Opera, a system with schedule information; thus a train can induce a “plot” at a station, shown on the STEG screen, showing if it is on time, or if there is any deviation from schedule, in plain text (minutes).

STEG has no plausibility checks built-in. Planning in “the future section”, by moving a line representing a train along the time axis to handle a delay, is of course a quite reasonable thing to do, and it corresponds to the notation that would be performed in the paper graph as well. It is also possible to re-plan a train “back in time”, even though it has been plotted at a station with information from Argus. This means that factual information can be overridden/ignored.

Piteå station is best described as a “special case”. The part of the interlocking plant that can be fully controlled and monitored from the TCC in Boden does not cover the entire track system, but comprises only the home signal 1/5 (seen from Arnemark), which is followed by an end-of-route stop lantern and a shunting signal, 2/5, that can be set to permit shunting movements further into the station area (which extends several km). Seen in the other direction, there is a shunting signal 2/6 to signal permission to leave the shunting area and to proceed to the exit block signal Ptå L2. The exit block signal can only show “Clear” if the line section Piteå–Arnemark is clear and the line block system is set in the direction towards Arnemark.

All movements inside the end-of-route stop lantern are considered to be “shunting”. Several shunting activities can be going on at the same time and the overseers must be aware of one another to avoid conflicts. Every overseer and every driver of incoming or outbound trains are required to call the traffic controller and state which area they need to occupy, together with their name and phone number. All this information is set down on a special form (paper note), “Hjälpblankett”.

When shunting activities are finished, the overseer (or the driver of a train) calls up and notifies the traffic controller, and then the time when activities end is noted in the form. Train numbers were at the time of the accident not noted, but traffic controllers may of course make mental connections between e.g. incoming trains and drivers' names.

The train situation prior the accident

In the situation at hand, the pre-planned train order for the line section between Arnemark and Piteå was as follows: 9231, 9229, 6032, 9207 (“two down, one up, one down”). Figure 4 shows the original train plan in graphical format for Nyfors – Piteå the current day. Train 9207 (Driver C) was planned to wait to meet train 6032 (Driver A) in Arnemark.

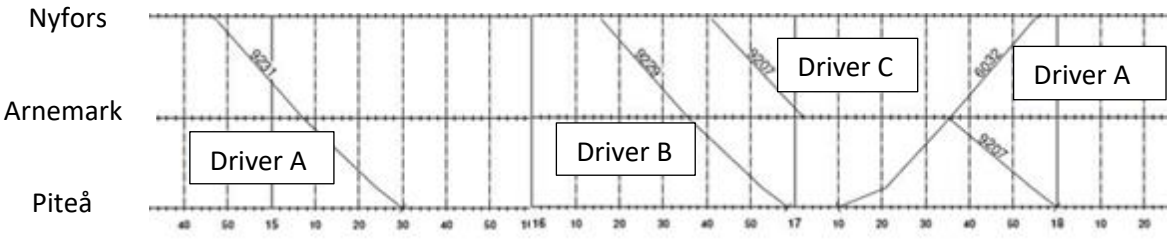


Figure 4. The original train plan for Nyfors – Piteå the current day.

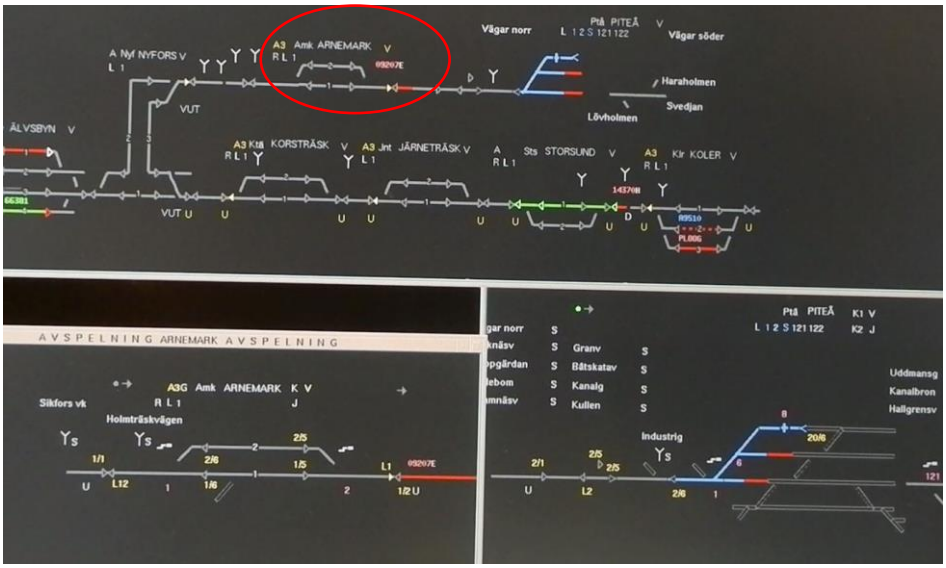
The traffic controller decided to change the train order because two down trains were ahead of schedule. The new train order was: 9231, 9229, 9207, 6032. Instead of waiting for train 6032 at Arnemark, train 9207 was planned to proceed all the way to Piteå before train 6032 could depart from Piteå.

Train 9231 (under control of driver A) arrived in Piteå on time, train 9229 (driver B) arrived 20 minutes before schedule. Train 9207 (driver C) was initially some 20 minutes early and was re-planned to skip the cross with 6032 in Arnemark and to proceed directly to Piteå, running almost an hour early on the last line section. This re-planning was quite in order, as rules in CTC areas permit changing of the train order without any particular precautions. Figure 5 shows the re-planned order in the computer-based planning and documentation tool STEG.

Figure 5. The changed train order in STEG (92315, 9229, 9207, 6032). *Train 9231 is hidden in the past section.*

However, train 9207 ran into technical problems with the ATP[1]-system between Nyfors and Arnemark, and was delayed as a consequence. The driver called up the TCC and informed the traffic controller about this. When train 9207 finally ran through Arnemark, it was almost 20 minutes delayed in respect to the replanned situation. No actions were taken by the traffic controller to handle this change in the situation.

The traffic controller had laid the plan so that train 9207 would arrive at Piteå before train 6032 would be allowed to leave Piteå. As the driver of train 6032 contacted the traffic controller to prepare for departure, the traffic controller noted on the Argus screen that the line section between Piteå and Arnemark was occupied. See figure 6.



Figur 6. Argus screen indicating the line section occupied by train 9207.

The occupied line section precluded the direction of the line blocking system to be changed, and following this, the starting signal (2/6) and the exit block signal (Ptå L2) in Piteå could not show a "Clear" aspect for train 6032.

From the information the traffic controller could gather and evaluate, he concluded that the situation was due to an improperly occupied track circuit (a technical problem) and that train 9207 had in fact arrived in Piteå. The train 6032 was given clearance to proceed past the restrictive signals.

[1] *Automatic Train Protection.*

Why did the traffic controller come to the conclusion that it was safe to allow train 6032 to proceed past signals at "Danger"?

The conclusion that the traffic controller drew was based on information from two sources:

1) Information on the "Hjälpblankett" (paper note for shunting movements), see figure 7. The names noted on the paper note were those of drivers A and B, which were mistakenly assumed to be those of the drivers of train 9229 and 9207, when in actual fact it were those of the drivers of train 9231 and 9229. The driver of train 6032 was the same person as driver of train 9231. The driver of train 9207 never gave his name to the traffic controller when they conferred over the ATP problem which caused train 9207 to become delayed.

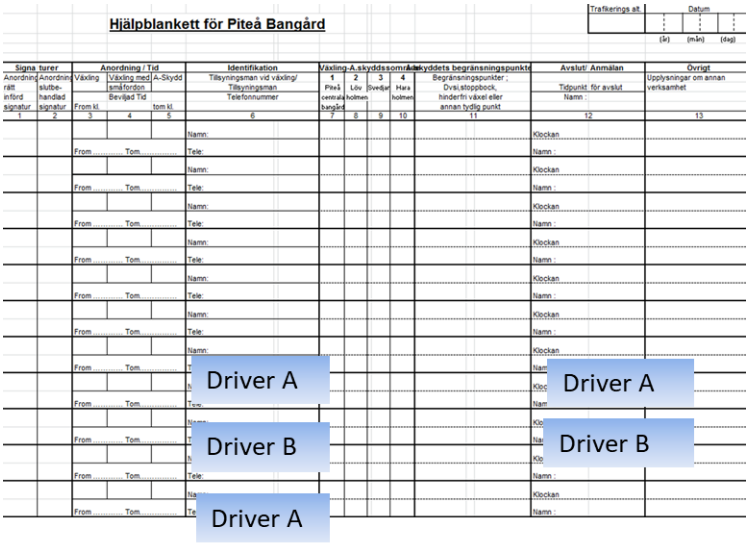


Figure 7. Paper notations for start and end of shunting movements in Piteå.

2) Information gathered from the "past section" in the STEG presentation of the graph. It has been made clear, that the traffic controller checked the STEG screen in conjunction with his procedure for allowing train 6032 to leave Piteå. The screen view that he used (the screens are continuously recorded and can be reconstructed) is somewhat ambiguous, but the information shown, may be interpreted in a way that shows that 9207 had indeed reached Piteå. See figure 10.

With the information at hand, the traffic controller became convinced that the occupied line section between Arnemark and Piteå was free to use for train 6032, in the firm belief that the indication of an occupied line section was a result of a technical problem (which is not unheard of), and he then went on with the actions needed to allow train 6032 to proceed towards Arnemark past signal at "Danger".

When trains are allowed to proceed past signals at "Danger", the technical systems for route protection etc. are not active. The operational safety comes to rest on the person involved, the traffic controller. When a train is to be allowed to leave a station past restrictive signals, into a line section, the procedure aims at assuring that the line section is indeed free and will remain so, until the train has left the line section and entered the station at the other end.

The checks include, but are not limited to:

a) Ascertaining which train was on the line section last, and

b) where is that train now, and

c) making sure that signals at the station in the other end of the line section are locked in the "Danger" aspect.

Investigating the whereabouts of a train is normally not too complex, it will show up as an occupied track circuit somewhere. In this case, the train was supposed to have entered Piteå station. The entire station cannot be monitored from the TCC in Boden as it does not have track circuits on all tracks. After a train has left the outer part (see above), the 900 meters inside the home signal, it will not be distinguishable at the TCC monitoring system.

In that situation, the traffic controller may consult his/her documentation, that is, checking "the graph" and any notations made on it. In Boden, STEG has taken the place of the paper-system and the documentation is, in actual practice, the electronic traces that are recorded there as a result of interaction between Argus and STEG. Unfortunately, the traffic controller had altered the electronic notations for train 9207 when he was going through his planning status earlier, se figure 8 and 9. That had created a false depiction of the situation, but at this later stage it proved to be a vital part of the information that he relied upon when he decided that the line section Piteå – Arnemark was free from trains. The train was indeed still showing on the TCC monitor, but it was deemed to be a technical problem with a track circuit; the train was believed to have arrived in Piteå, based on the information in STEG.

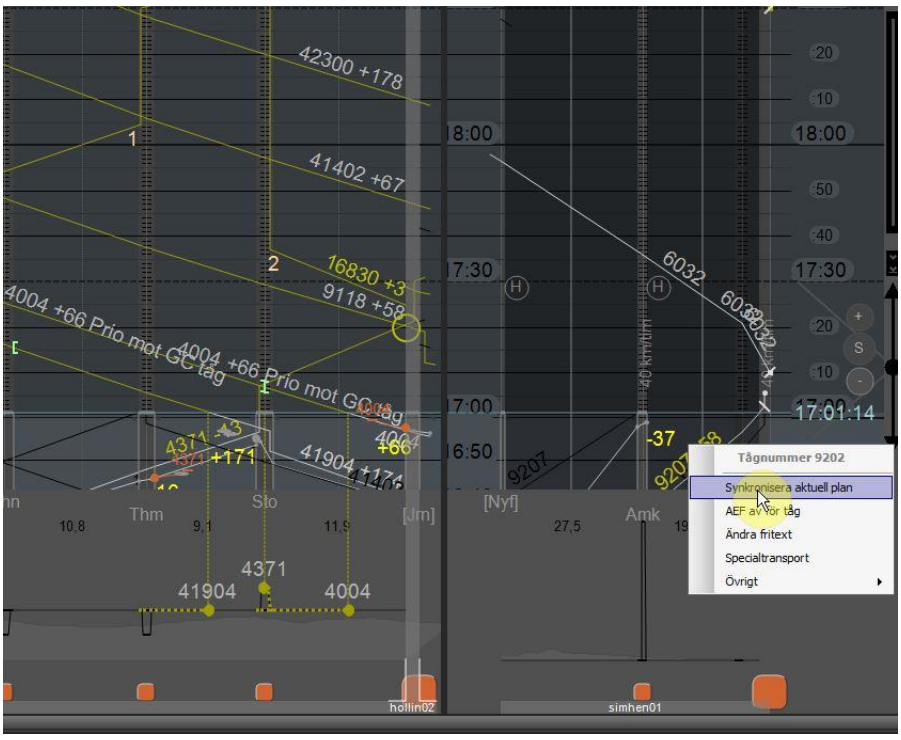
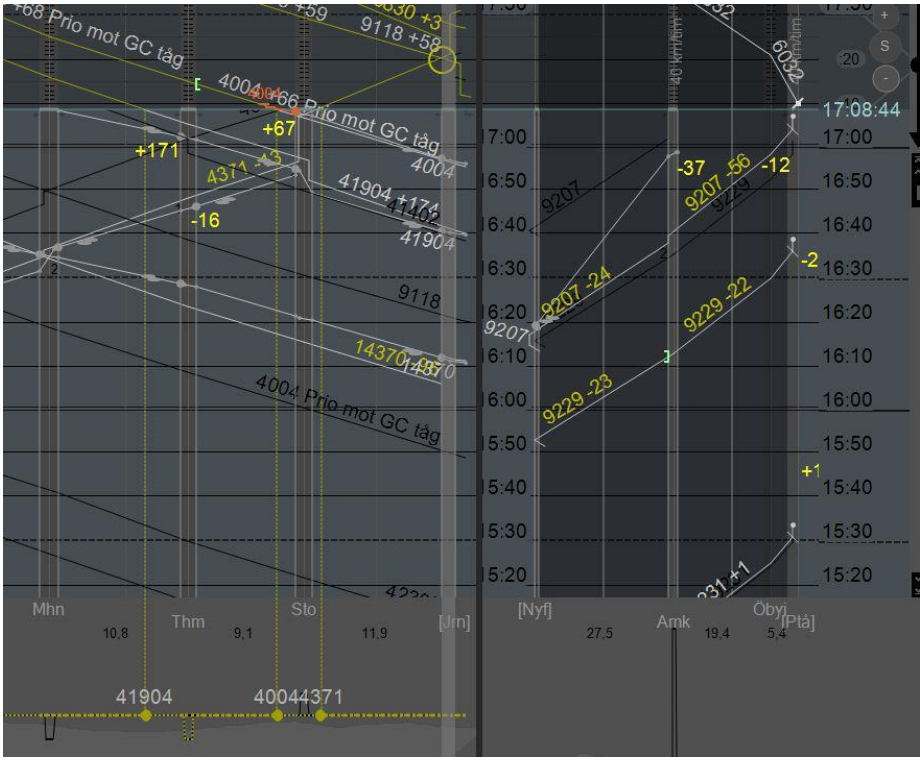


Figure 8. The traffic controller synchronized STEG . Information sent from the maneuversytem and a schedule system updated the trainline for 9207.

Figur 9. The traffic controller adjusted back train 9207 manually. He was convinced the update was wrong.



Figur 10. The screen before the traffic controller admitted 6032 to pass signal at ”Danger”. It shows that 9207 has yet not reached Piteå but the information shown may be interpreted in a way that shows that 9207 had indeed reached Piteå

The traffic controller deemed the information he found on his paper note of shunting activities in Piteå more relevant than the information that could be gathered from the Argus traffic control system or the STEG planning and documentation tool.

What kind of support did the newly introduced, planning and documentation tool give the traffic controller?

The purpose behind the STEG-system was that the traffic controller by planning further in the future could solve conflicts in time and follow and monitor that the plan was executed. Focus on planning ahead was encouraged during the traffic controllers practical training.

Such a one-sided focus on what lies ahead in the future, however, can lead to a possible distraction of what actually happens and has happened.

From the logs of STEG, it is clear that the traffic controller the hour before the accident was focused on what would happen later. The timeline on the screen was far down, which limited his ability of simultaneously monitor the outcome of the planning. The traffic controllers strong focus on planning ahead to solve conflicts can thus have caused the monitoring part of the tasks to suffer.

The researchers behind the system has emphasized that the benefit of a planning focus is best if you use the automatic execution function that automatically performs in Argus what you planned in STEP. However, this function was seen as technically unreliable in Piteå and was not used in this case, which means that the traffic controller must handle the entry in Argus manually, i.e. to some extent enter data twice.

What was lacking in the risk management process?

The accident occurred despite of a well thought through implementation of a new computer-based planning and documentation tool, STEG, that gave a dynamic, on-screen visualization of the train plan. A tool developed by the Infrastructure Manager in collaboration with a University and tested on traffic controllers. What was lacking in the risk management process?

The Infrastructure Manager carried out a risk analyse prior to the commissioning of STEG. One of the risk factors mentioned is stress by changing between the roll planner and the roll executer. The risk was categorised as harmless and in the area of production quality. However the risk was not related to the fact that it could also affect the safety if the traffic controller has such a large focus on planning that the execution gain less focus.

When developing STEG the Infrastructure Manager used only experienced traffic controllers as reference group. During the process of developing STEG, the developers made the reflection that the experienced train controllers could adapt very quickly to work in STEG. It was however not analysed to what extent the fast adaption was due to also having many years of experience as a traffic controller and a gained deep understanding of what the paper graph and STEG represents in reality.

Prior the commissioning of STEG in Boden, an analysis was also made of the differences between the conditions at the pilot traffic centre in Norrköping and the traffic centre in Boden. The Infrastructure Manager did not identify any differences that prompted changes in the system's design. Nevertheless, the local conditions had an unforeseen effect on the functionality of the plotting. This indicates the importance of testing and evaluating a system at local level.

The follow-ups on how the system was used and functioning in relation to the intended design was in this case not sufficient to detect and deal with the mentioned deviations. Besides indicating that the system was not used in an optimized way, this is a limitation that can also lead to a loss of the users' confidence in the system, which in turn can lead to increased safety risks.

The Infrastructure Manager had not looked into how the traffic controllers regarded the status of the different tools (STEG, Argus, “Hjälpblankett”) and how the information from these systems was perceived and interpreted.

End note

Today risk assessments are common practice before introducing a new system. And often well thought through. However not seldom are the risk assessment focused on one particular tool or new system. Lacking the perspective of how other tools might affect, or be affected by, the tool.

A more sociotechnical focus can highlight unforeseen risks that emerge when the system is used in a context. Questions such as which system the user will trust, if he is given different answers from different systems, needs to be examined. In order to do so it´s important to map local conditions, systems, knowledge and practices before the implementation and later follow up these aspects. Is the system used the way it was intended? And if not, find the answer to why. Are there technical, organisational, knowledge, trust or other obstacles?

There is also room for improvement regarding the procedures for selecting user representatives when developing and risk assessing new systems. An experienced traffic controller might for example read more from a line in a computer-based interface than a newly examined one.

Furthermore, new features in a system can shadow the original purpose of the system. To be able to discover such situations it is important to invest and commit not only in the development phase but also in the implementation phase. And to keep in mind that the implementation phase is not finished at the first pilot centre, or among the first group of people you introduce your system to.