Provisioning of Safe Train Control in Nordic Countries

Harold "Bud" Lawson

Lawson Konsult AB, Albavägen 25, Lidingö, SWEDEN; bud@lawson.se

Abstract: The safety of train traffic is a vital societal function. During the mid-1970s, the availability of inexpensive microprocessors and electronic components led to the first computer-based systems solution to this critical function. Sweden was the first country in the world to develop and deploy a computer-based solution for Automatic Train Control (ATC). The major suppliers Ericsson Signal Systems and ITT Standard Radio developed solutions for both of the functions required; namely the track to train transmission system as well as the onboard system. Both system functions have been further developed by companies that have taken over ownership of these system products; namely, Bombardier, respectively Ansaldo. In the original delivery to the Swedish Railways (SJ), Ericsson Signal delivered the track-to-train transmission system; whereas, Standard Radio the onboard system for SJ trains and Ericsson Signal delivered the onboard system for the Stockholm Local Traffic (SL) trains. We describe the functions provided by both systems; however, we place focus upon the unique properties of the Standard Radio onboard system that has had a stable architecture for over twenty-eight years. The two track-to-train transmission systems delivered by Bombardier and Ansaldo are compatible; in Norway, both suppliers have delivered their products for both of the functions. Further, the X2000 and Öresund bridge trains that travel between Sweden and Denmark utilize the Ansaldo onboard and track to train transmission products in combination with a Siemens system. In addition to the details of the Swedish ATC solution, a brief historical perspective of train control as well as the implementation of train control in the other Nordic countries is provided. The need for a holistic view of train control is cited in examining two actual train accidents in Sweden and Norway. Finally, we discuss the movements toward a European Rail Traffic Management System standard in respect to interoperability of train control.

Keywords: Automatic train control (ATC), real-time systems, safety-critical, systems engineering

1. Introduction

The safety of millions of train passengers is dependent upon reliable safety related equipment and functions in the entire railway system. One of the most important functions is the monitoring of the behavior of train drivers; that is, assuring that they abide by speed limits, signal status, and other conditions. There have been numerous train accidents in Europe and elsewhere in the past where the availability and proper operation of this function would have hindered these

incidents. This function, now often referred to as Automatic Train Protection (ATP), came into being since 1980s in Sweden as the Automatic Train Control (ATC) system.

In this paper, we present key properties of the Swedish ATC system. We place particular focus upon the onboard system conceived and developed by Standard Radio and Telefon AB, now owned by AnsaldoSTS (Ansaldo Sweden), and further developed and maintained by Teknogram AB of Hedemora, Sweden. We cite the major reasons for the success of this onboard system in providing safe train control for over twenty-eight years. In addition, we discuss the utilization of the Swedish solution in Norway and partially in Denmark as well as the solution utilized in Finland. The reasons for two train accidents in Sweden and Norway are presented. These accidents highlight the need for a holistic perspective concerning the technical and non-technical issues related to ATC and its deployment. Finally, we introduce developments concerning the European Rail Traffic Management System.

Harold Lawson, Sivert Wallin, Berit Bryntse and Bertil Friman, all were key players in the Standard Radio ATC onboard system solution; namely, as architect, developers and maintainers, and verifier of the later versions of the software. After twenty years of successful operation, they wrote about the properties of the Standard Radio onboard system [10]. Some parts of the current paper include that earlier presentation.

2. Train Safety: A Brief Historic Perspective

Railways as we know them today had their origin in the United Kingdom with the first public railway in 1825. At that time, there were 25 miles of track and two locomotives. In 1829, Stevenson introduced the steam engine called "The Rocket" and in competition with other engines, it attained a speed of 29 mph (unloaded) and 25 mph hauling 13 tons of wagons. This catalyst led to the rapid development of railroads around the world. By 1875, there were approximately 160,000 miles of track and 70,000 locomotives in the world. This is an astounding development especially considering the primitive means of international transportation and communication available at that time. It is interesting to compare this with the rapid expansion of automotive traffic as well as computing technology and the internet.

Early accidents due to human errors in the UK and elsewhere rapidly led to the development of signaling to control traffic. To provide this critical function, several mechanical interlocking solutions where developed in order to prevent signalmen from accidentally setting conflicting routes. Interlocking developments then proceeded through generations of an ingenious variety of more complex mechanical and electromechanical systems.

3. Automatic Train Control in Sweden

The availability of inexpensive microprocessors and electronics in the mid-1970s offered new solution possibilities for interlocking as well as for protecting against driver errors. The Swedish National Railways (SJ) was quick to exploit these new possibilities and developed the worlds first computer-based interlocking and speed control system. The investment in this solution was motivated as follows:

To meet demands of increased efficiency of railway transportation on both existing and new tracks, the train speed must be increased and the trains must operate with shorter intervals. This requirement increases the demands on both the safety system and the train drivers thus leaving little room for human errors. The high degree of accuracy of the ATC system minimizes the risks for driver error.

Initially (in 1980 when the first ATC systems where installed), the plan for the Swedish State Railways (SJ) was that the train should be driven entirely according to the external optical signals, and that the ATC system should be considered only as a safety back up. With the advent of the X2000 high-speed trains (200 km/h), it turned out that the optical system was insufficient for presentation of all information needed, e.g. earlier warning for restrictions ahead, and different speeds for various train types. In addition, after they accumulated operational experience with the ATC system, it turned out that the ATC system could be trusted for presentation of information not otherwise available along the track. The resulting system nowadays is a very efficient, robust, and safe combination, well matching more expensive and more complicated systems used elsewhere in the world.

If the driver should lose concentration for a moment, the ATC will then take over the control of the train by applying the brakes. This brake application continues until the driver manually acknowledges to the system that he is once more capable of controlling the train. If the driver should fail to regain control, the ATC will continue to brake the train to a standstill.

The two major technical function constituents of the ATC system are the track to train transmission system product and the onboard system product.

3.1 Track-to-Train Transmission System

The wayside equipment consists of track-mounted transponders (called balises) transmitting messages (telegrams) to the vehicle when activated by the antenna mounted on the vehicle (see Figure 1). The information transmitted includes signal status as well as the speed limit followed until the next transponder group. Each type of information generates a unique message (telegram). The transponders combine into groups of minimum two and maximum five transponders. A transponder group can be valid for the current or the opposite direction of travel, or for both travel directions.

The transponders in a group either can have a fixed code or coded by an encoder connected between the signaling system and the transponder, in such a

way that the transponder group can give information corresponding to the current signal aspect to the onboard equipment.

When a vehicle with an active ATC travels over a transponder group, each transponder activates from the energy received from the antenna of the vehicle. The coded message is continuously transmitted to the vehicle equipment as long as the transponder is active. A valid combination of transponders will transmit all the information necessary for the vehicle equipment to evaluate the message and take the required action. The onboard equipment will detect either a faulty message or an invalid combination of transponders and notify the driver accordingly.

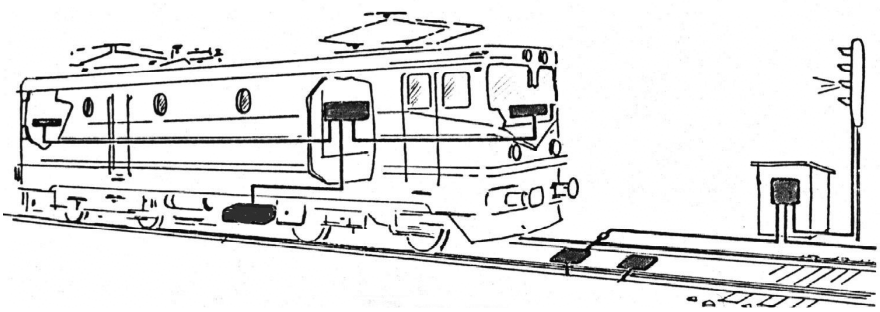

Figure 1. ATC Track to Train Transmission System

3.2 The Onboard System

Figure 2 portrays the vehicle onboard equipment and it consists of the following major components:

It uses an antenna mounted underneath the vehicle that activates the track equipment (transponders) by continuously transmitting a powering signal and receiving transponder messages that the system will evaluate and use to supervise the safe travel of the train.

It contains a set of computer equipment that evaluates the transponder messages. It presents the information to the driver that will break the train to a safe speed level if the driver should fail to take the correct actions. That is, if the driver does not brake the train or exceeds speed limits. The driver has to cancel manually each ATC brake application by pushing a brake release button.

It contains cab equipment consisting of a driver's ATC panel used by the driver to enter into the ATC system the data that is relevant to that specific train, and all other communication with the ATC equipment. The panel also keeps the driver informed of current speed limits and target speed limits at speedboards and signals ahead.

It includes vehicle-interfacing devices such as a speedometer connection, a main-brake pipe-pressure sensor, and one or more brake valves.

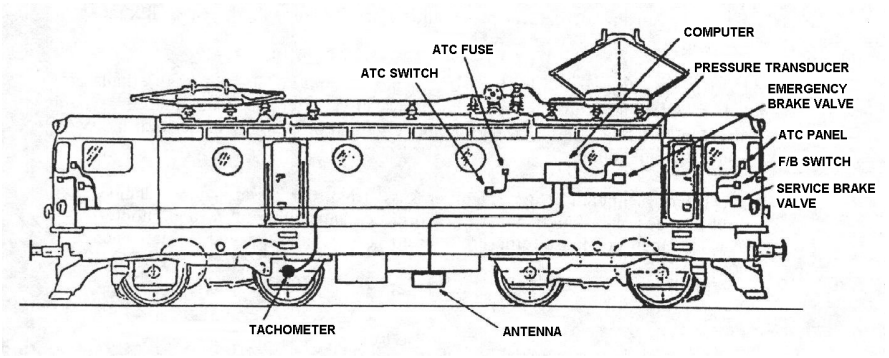

Figure 2. Onboard ATC System Product

To provide for fault-tolerance, a three-processor solution with majority logic comparison of outputs was utilized for the early versions of the onboard system. In the Standard Radio onboard system, the same program executes on all three processors thus the redundancy protects primarily against processor hardware failures. Due to the observed high reliability of the hardware based upon many years of operation, later versions of the onboard system only utilize two processors.

4. Time Line for the Onboard System Product

The Standard Radio ATC product became the property of ATSS (Ansaldo Transporti Signal System) in 1990. Since 1984, they contracted a significant part of the further development of the product and maintenance to Teknogram AB. Appendix A illustrates a timeline highlighting the major product events.

The two latter developments of the system led to ATC2.1 developed especially for the Västervik line where they employed a radio-based control instead of the balise transponder system. Further, they integrated ATC2.2 in the X2000 train sets and freight locomotives that travel over the Öresund Bridge. In this case, Teknogram also developed an interface PC-board and software based upon the same operating system as ATC2 for communication with the Siemens solution utilized on the Danish railways. This system began operation during the summer of 2000 when the bridge officially opened. Now, even the line between Helsingor in Denmark and Helsingborg in Sweden also deploy this dual solution. The different software versions are fully backwards compatible, i.e. ATC2.2 could be used in any train in Sweden and Norway if desired.

In addition to the main ATC onboard product, they developed a separate PC-board and software running under the same operating system solution to function as the “black box” recorder for ATC. The recorder collects information for up to three days of train operation and includes telegram information and all transitions of speed greater than 2 km per hour. The most recent version of the recorder

utilizes flash memories. Earlier versions utilized solid-state memories that required constant power (battery back up).

Standard Radio hoped that ATC would be an export product. Unfortunately, this market did not fully materialize until later and only a small project in Perth, Australia, utilized ATC1 (and it is still operating and expanding). Several potential customers, including British Railways examined the product, but decided not to buy it. This was very unfortunate since we now know that it has worked reliably for train traffic for over 28 years. This is a truly impressive record. The cost of one single serious accident would most likely pay for the installation of the system not to mention the personal loss and suffering associated with such accidents.

Since 1990, further exploited by Ansaldo (ASTS) and supported by Teknogram, the solutions utilized in ATC1 and ATC2 have been applied in several installations of ATC. The installations have included an ATP (Automatic Train Protection) system for Keretapi Tanah Melayu Berhard of Malaysia (installation 1996), ATP for Hammersley Iron Ore Railways in Australia (installation 1998), the ATC system for Roslagsbanan in suburban Stockholm (installation during 2000), ASES (Advanced Speed Enforcement System) for New Jersey Transit in USA, and the monorail system for Kuala Lumpur, Malaysia. All of these onboard systems have the same architecture and operating system core solution. However, the programs for the latter solutions are in the Ada programming language.

Further, Teknogram AB has successfully utilized the same architecture and operating system to develop and market more than twenty train simulators. Consequently, the ATC architecture has been the basis for the Teknogram business concept. For Teknogram and Ansaldo, this represents a truly exceptional example of the reuse of architectural concepts and operating system core for the implementation of new system products.

5. ATC Software Statistics

As indicated in the timeline of Appendix A, there have been two major versions developed and two minor variations on the second version that they developed for utilization by the Swedish Railways (SJ). The size in terms of number of procedures, lines of assembly code and number of memory bytes are as follows.

Version	Number of Procedures	Number of Instructions	Number of Bytes
ATC1	157	4116	10365*
ATC2	308	10281	26284**
ATC2.1	313	10523	27029**
ATC2.2	339	11178	29522**

* Motorola 6800 microprocessors
** Motorola 68HC11 microprocessors

The small size, clear structure, and simplicity of the software solution have led to many advantages in respect to verification as well as further development and maintenance as described below. We should note that even the Ada programming language solution developed by Ansaldo subsidiary Union Switch and Signal in Pittsburgh, Pennsylvania is very compact by Ada standards as reported by Alan Swiss, one of the developers of this version.

5.1 Evolution of the Architectural Concepts

In 1975, Standard Radio contracted the consultant services of Harold Lawson to assist Roger Andersson, project leader, and Sivert Wallin, chief designer, in the conceptualization of the architecture. Following a review of the work done to date on the software, Harold Lawson and Sivert Wallin re-examined the fundamental requirements of the ATC function and developed the problem oriented architecture concepts that has successfully provided product stability as well as a sound basis for further development under the entire life cycle of the ATC onboard system product.

The following three core concepts were developed and have been driving factors during the product life cycle.

Time Driven: The major conceptual aspect of the design is the treatment of the system as being continuous in time as opposed to being discrete event driven. Motivation - Given the fact that a 250 millisecond resolution (*dT*) of the state of the train in respect to its environment was determined to be sufficient to maintain stability, it became clear that the simplest approach was to simply execute all relevant processes (procedures) during this period of time.

Software Circuit [1] : As a result of the time driven concept a cyclic time driven approach became the basis for the solution where short well-defined software procedures behave like circuits.

Black-Board Memory: In order for Software Circuits to have access to key information, variables are retained in a black-board where both reading and writing are permitted.

This simplification of concepts led to the fact that the processors only needed to be interrupted by two events. One interrupt to keep track of time (1 millisecond) and one interrupt when information from a transponder is available. The time in the 250ms *dT* is more than adequate to perform all processing. Adding more structure to the problem, for example, via the use of an event driven operating system approach would have had negative consequences in terms of complexity, cost as well as reliability and risk thus affecting safety. In 1975,

[1] The naming of this concept was developed later when the concepts of the architecture were applied in a Swedish research and development project for local area networks in vehicles [2] and [3]. In the later Ada programming language solutions they are called objects.

Lawson documented the fundamentals of the approach [4]. Figure 3 illustrates the operating system.

The "circuit like" structure of software led to highly simplified coding of processes (procedures). While it would have been useful to deploy a higher-level language in the solution, we deemed it unnecessary due to the low volume of code that was expected. Experience has indicated that this was a reasonable decision at that time. On the other hand, we decided to comment the code in a higher-level language. In earlier versions of the product, we employed the Motorola MPL language, a PL/I derivative. In later versions, we consistently employed a more Pascal-like annotation. In system tests, MPL, respective Pascal versions where executed in parallel with the execution of the assembly language version in order to achieve system verification.

As the concepts evolved, the more global implications of the concepts became evident as documented in a comprehensive software plan [5].

> *"A comprehensive plan for the specification, development, testing, verification, production and maintenance of the software components of the ATC project is presented. The goal is to produce reliable software parts to complement the three processor Motorola 6800 system so that a trustworthy total system is provided. A further goal is to assure that the software constituent remains reliable under the lifetime of the product. That is, that future modifications to the software will not affect the reliability due to oversights concerning design features and software component interrelationships."*
>
> ...
>
> *"The key to a successful software product lies in the ability to decompose the system to be implemented into well defined units such as processes, procedures, blocks, etc. Further, the operation, inputs, and outputs of these units must be well specified and the specification must serve as a control over the implementation, testing, production, and maintenance."*
>
> ...
>
> *"In the ATC project, the process is the unit to which the system structure has been decomposed. A process should be viewed as a testable component, precisely as a hardware component (integrated circuit). It must have a clear specification and have a well defined component test procedures."*
>
> ...
>
> *"A system can never be more reliable than its components and their interconnections. Assuming that each software component has been tested, the interconnections of subsystems of components and finally the total system must be developed, tested, and verified systematically."*

Thus, it is clear that even at this early point in the product history conceptualization, we clearly identified the importance of architecture as a controlling factor for the life cycle of the product. Even though the owners of the product and development and maintenance has changed management, the fundamental concepts established in the mid-1970s are still in place and have led to a successful solution for train safety not only in Sweden, but in other countries.

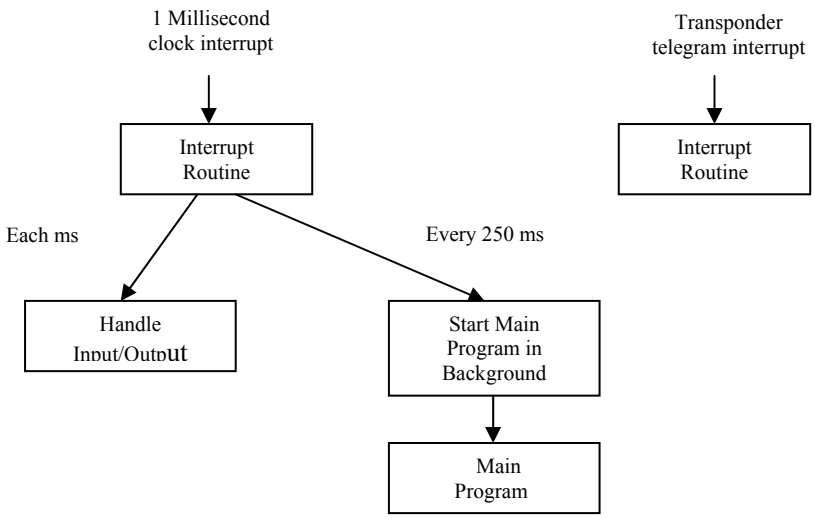

Figure 3. Operating System Structure

5.2 Development and Maintenance Principles

The early development work was based upon using a PDP-15 computer both for simulation as well as for assembly language translation. The target system based upon Motorola 6800 processors was connected to the PDP-15 so that both procedure and system testing could be well controlled.

Due to the simplicity of the architecture, we discovered many advantages and principles that guided both development and maintenance. We established them as follows.

Utilize the clear points of built-in controls provided in the short procedures as an aid in the instrumentation of testing and in fault isolation.

As a general control of proper cycle execution, the stack pointer must be returned to the same point in each execution cycle.

By following code discipline, no wild loops can occur.

No backward jumps are permitted other than in well controlled loops in procedures.

By keeping the solution simple, quick reliable changes can be made and verified thus reducing costs.

The operating system core can easily be reused by removing procedures and incorporating new procedures for new functionality (recorder, simulator).

Following these principles has led both a reliable and stable onboard system product as well as a basis for the reuse of code.

5.3 Verification Perspective

We carried out verification via module testing, code inspection, and system test. Early verifications of ATC1 where carried out by the Foundation for Scientific and Industrial Research (in Norwegian: *Stiftelsen for industriell og teknisk forskning*, or SINTEF) at the Technical University in Trondheim, Norway. Bertil Friman was involved in verification of ATC2 as reported in [1]. The report describes the verification of the ATC2.2 version that is used for trains crossing the Öresunds Bridge.

5.3.1 Module Testing

Since the beginning of the ATC project, we tested the software circuit-like procedures of the ATC system by running them in parallel with equivalent software circuits written in a high-level language, and comparing the results. Back in 1975-76 when the original ATC was developed, we did this by connecting the target system (6800-based) directly to the bus of a minicomputer (PDP-15). We then ran the high-level version on a minicomputer that we also used to control the execution of the target system and to compare the results. The same principle, although more refined, is also in use today. The high-level version is now written in Pascal and runs on a PC computer. The PC computer has direct read/write access to the 64k byte memory space of the target system based upon 68HC11. This configuration makes it possible to test approximately 1000 value combinations per second. They can test two million combinations in roughly half an hour. If a software circuit has a small number of input variables, then they can test it exhaustively. If the number of input variables is large, then the value ranges are limited to values around min, max and close to the decision points in the code.

5.3.2 Code Inspection

Back in 1988, when they started the major revision of ATC that resulted in ATC2, they decided that because of the increased complexity of the program, it would be subject to a thorough and detailed inspection. They contracted Friman Datakonsult AB to do the inspection, which they mainly did by the use of informal proof techniques. They defined a goal, and then they built up an informal proof to see if they satisfied the goal.

They soon noticed that most goals were associated with variables and their contents. A (simplified) goal could for instance be that the variable HS (main signal speed) should always be zero after the passage of a stop signal transponder. Since most goals were associated with variables, the goal-proof-technique was successively replaced by a systematic analysis of individual variables. They did this analysis by tracing all places where a variable could be assigned a new value, and for each such place, finding out the real world conditions that were associated with the variable change. They could often check directly these real world conditions against sentences in the requirement specification.

Associating real world conditions to places in the code where a variable changes value requires an incremental analysis of variables. First variables that only depend on hardware inputs must be analyzed. Then variables that depend on these variables can be analyzed and so on. Sometimes two or more variables can be dependent on each other in a circular fashion. Analyzing such a loop requires more effort because they have to analyze all involved variables together. The variable based inspection method has been very successful both for ironing out special case errors and for enhancing the confidence in the ATC system.

Johan Fredrik Lindeberg and Øystein Skogstad at SINTEF in Norway encouraged at an early stage the development of CASE tools to support the code inspection. They developed several such tools. The most important was VTR (Variable TRacer) which is directly associated with the variable based inspection method.

5.3.3 System Testing

They did the bulk of the system testing of ATC with the use of a simulator. They tested the ATC system by simulating the train start-up and travel on the rails that are equipped with transponders. The simulator has handles, buttons and indicators that correspond to handles, and buttons and indicators in the locomotive cabin. They simulated the transponders with a file that contains their positions (from the starting point) and telegrams. They tested a new scenario (use case) by editing a track file and executing the new version on the simulator. After they changed a track file, they ran it on the simulator instantly. On some occasions, an interesting scenario has been discussed on the phone and at the same time been tested on the simulator. This was a superb trouble shooting mechanism. Many parties have contributed track files including Teknogram, ATSS, Banverket and Adtranz. Each track file is accompanied by a specification of how the ATC system shall react at each place on the route. ATSS has an archive containing hundreds of track files that can be used for the validation of new versions of the ATC system.

Quick cycle-time simulation has been a key ingredient in the ATC project since its beginning. The first simulator was a program that ran on the same PDP-15 mini computer that they used to assemble the code. It was directly, over the PDP-15-bus, connected to the development version of the ATC system. Today, the simulator uses a 68HC11 CPU with essentially the same operating system and program structure as the ATC program itself. They used a PC for storing the track files and for controlling the parameters of the simulation through the screen and keyboard.

6. Lessons Learned

We can learn several lessons from the Standard Radio ATC onboard system product experience. We could well apply these lessons in other products, particularly safety critical computer-based systems. Some of the most significant lessons are as follows.

6.1 Architecture is a Key Aspect

The definition and consequent deployment of a problem relevant architecture is a key factor for success. While it is important to have well defined work processes for all life cycle stages of a product, a good architecture reduces the need for heavy processes with multiple activities and tasks. One can simplify decision-making when we bound decisions by the architectural concepts as described by Lawson [11].

6.2 An Engineering Viewpoint Is Superior to a Software Viewpoint

Instead of creating significant quantities of software, an engineering view of the functions to be performed was taken. The analogy between hardware circuits and the logic of the software, later identified as software circuits provides a strong, simplifying solution. We can conclude that software, especially in large quantities, is dangerous, but we can control it with the proper engineering viewpoint.

6.3 Do Not Add More Structure Than Is Necessary

Adding more structure to a solution than necessary for achieving desired behaviors leads to unnecessary complexity that adds to costs and risks. This pitfall is very common, even for safety critical systems. Operating systems and programming languages that provide elaborate structures such as for interrupt handling and multitasking could complicate verification, further development, and especially maintenance. In addition, they can deploy complex methods and tools. All of these supporting methods and tools implicitly become a part of the product. Together they often are an overkill solution leading to increased cost and risk.

6.4 Verification Is a Vital Aspect of Safety Critical Systems

One must verify all safety critical systems with respect to their specifications and safe behavior in various situations. The combination of module testing, code inspection, and system test via simulation has proven to be an adequate approach for ATC. Simplicity in the architecture and code structure simplifies verification and contributes significantly to safety verification.

6.5 A Good Technical Solution Is Essential But Does Not In and Of Itself Guarantee Safety

The technical solution is only one component of the total system. There are many other factors, including investment decisions, human factors, operation management, and so on, that can and have affected the utilization of the ATC safety system.

7. Train Control in Other Nordic Countries

The Swedish ATC computer-based solution was the first in the world. Norway was also quick to see the benefits of the Swedish ATC solution. Ericsson Signal originally provided the track-to-train transmission system solution in Norway, which was the same as in Sweden. Due to a perceived need to have one supplier, Ericsson Signal also delivered the onboard system solution based upon their product delivered for Stockholm's Local Traffic commuter trains. In the past few years however, due to problems arising in that onboard system now supplied by Bombardier, Norway is partially converting its onboard solution to the ATC2 system now supplied by Ansaldo. Further, in later years Ansaldo has also installed their track to train transmission system product in parts of Norway.

In Finland in the mid-1990s, Bombardier delivered a modified version of the original Ericsson Signal track-to-train transmission system and the onboard system. As a coincidence, when Harold Lawson delivered his keynote speech at HINC2 in Turku, Finland, the day before there had been significant failures in this system and the local press interviewed him about ATC and its implementation.

Siemens supplied both infrastructure and onboard systems solutions for the Danish railways beginning in 1993. The Öresunds Bridge project led to a mixed solution for the new Öresund trains plus some X2000 train sets running between Sweden and Denmark. Since 2002, the first fully automatic (unmanned) trains in the Copenhagen underground where delivered by Ansaldo's subsidiary Union Switch and Signal of Pittsburgh, Pennsylvania. However, they did not base the solution utilized in this application upon the Swedish ATC system.

8. The Need for a Holistic System Perspective

As mentioned above, the technical product is only one part of the system. One must take a holistic systems engineering perspective to achieve the safety function to be provided in Automatic Train Control. These non-technical factors become evident by examining the following two accidents.

8.1 Borlänge, Sweden Accident

On 9 April 2000, six freight cars filled with Liquefied Petroleum Gas derailed and tipped over at 70 km/h in the Borlänge station. The speed limit in the area was 40 km/h. The authorities declared the station and central Borlänge off-limits to the public. As a result, 650 people evacuated for a week while they emptied the train of its contents.

The ATC braked the train three times in the 30 kilometers before the train crashed in Borlänge station. Unfortunately, the ATC infrastructure with balises does not cover the Borlänge station itself. They believe the driver had passed a restrictive optical signal just ahead of the turnout at which the train derailed. It

turned out that the driver was drunk and tests showed that he had 1.0 per mille of alcohol in his blood.

Thus, ATC functioned exactly as it was programmed to behave. However, two non-technical factors were at work. Firstly, the earlier decision not to invest in placing ATC balises in the Borlänge station area. Secondly, the human factors aspect of a drunken train driver.

8.2 Aasta, Norway Accident

On January 4, 2000, nineteen people were killed and several more injured when an express train from Trondheim to Oslo carrying 83 passengers collided head-on with a local train carrying 17 passengers heading from Hamar to Rena about 150km North of Oslo.

The Norwegian National Rail Administration stated that the probable cause of the accident was the northbound train passing the main exit signal at Rudstad station while it was showing red. The trains were equipped with ATC, but the permanent infrastructure along this stretch of track on the Røros line was not equipped with this system. The *total* system was therefore not equipped with ATC.

Safe train control involves many aspects (technical and non-technical) including strategic planning, finance, resource allocation, human factors, management, administration, maintenance, training and education, catastrophe procedures, laws and regulations and more.

Thus, a holistic development and deployment of this critical train safety function involves the use of system thinking to build and analyze models for identifying and relating important multiple technical and non-technical aspects (problems and opportunities). This also relates to prudent decision-making in all aspects and the use of system engineering in respect to the life-cycle management of the system assets. Hence, the stakeholders must develop the capability to "think" and "act" in terms of systems as described by Lawson [11]

8.3 European Rail Traffic Management System

Many different train solutions have evolved in European countries starting in the 1800s resulting in incompatibilities, expensive maintenance, and traffic limitations. To improve upon this situation the European Rail Traffic Management System (ERTMS) standard sponsored by the European Union came into existence with the goal to achieve interoperability and more effectively develop and operate trains in Europe.

The European Train Control System (ETCS) is that part of ERTMS specifying control system standards for train to track communication and onboard system protocols. It also specifies the levels of equipment configurations including the use of radio communication. Six major suppliers both compete and cooperate to develop ERTMS and ETCS, namely Alstom, Alcatel, Ansaldo, Bombardier, Invensys and Siemens.

While these steps should help in treating more system related aspects, there is much, much more to do to achieve the holistic system safety perspective that is needed for this vital societal function.

9. Further Development of the Onboard System Concepts

The architectural concepts developed for ATC onboard system product is used in other projects in Sweden. During the early 1990s, Harold Lawson, the ATC architect, participated in the Swedish Nutek research funding agency sponsored Prometheus project for the automotive industry. They again proposed the engineering view of software as a means of developing the logic for safety critical functions in vehicles in the BASEMENT system [2 and 3]). A methodology based upon the use of "software circuits" evolved during this project.

The work on BASEMENT also led to the development, by Arcticus AB of an operating system concept called Rubus [12]. Rubus identifies the performance of two types of tasks: time driven (called Red) and event driven (called Blue). In relationship to the ATC solution, execution is carried out in time intervals (*dT*) where the Red tasks are always executed first and time remaining in *dT* is available for Blue task execution. They have successfully applied Rubus in developing several embedded system products including the Limited Slip Coupling device developed by Haldex Traction AB and now incorporated in all new Volkswagen automobiles as well as for medical equipment at Siemens-Elema AB. Arcticus has also produced supporting development tools and has utilized them by providing embedded systems solutions for Volvo Construction Equipment AB and for military vehicles produced by BAE Systems (Hägglunds).

Lawson reported [6 and 8] on the importance of architectural philosophy as a key to the engineering of computer-based systems. The articles cited ATC as one of the case studies in these articles. Lawson has reported on a further development related to ways of evolving the concepts into a complete resource adequate model called CY-CLONE [7]. Lawson together with Svensson further development of the CY-CLONE model for distributed and parallel execution [9].

10. Conclusions

The Automatic Train Control onboard system product developed by Standard Radio in the late 1970s has proven to be a highly successful product. It is based upon an engineering view of the problem domain that led to a straightforward architecture. The architectural concepts have been a key factor in relation to further development, maintenance, and verification of the product. The concepts used in this ATC product have been further developed in other real-time environments. Given the success of the approach, it is surprising that more safety critical systems were not constructed in a similar manner.

Acknowledgements

Several people have had important roles related to ATC and in particular the onboard system originally developed by Standard Radio. In this regard, the author gratefully acknowledges the contributions of the following people.

- Sivert Wallin for his pioneering work at Standard Radio in developing the first onboard system. Founder and president of Teknogram AB, Hedemora, Sweden.
- Bengt Sterner at SJ/Banverket for his vision of need for as well as the feasibility of providing ATC in Sweden.
- Bengt Wenning at SJ for his vision on usability and ergonomics of ATC.
- Johann F. Lindeberg and Øystein Skogstad of Norways Technical University for providing insights in the programming of ATC.
- Berit Bryntse and others at Teknogram for their continued further development of the onboard system products.
- Bertil Friman now employed at Ansaldo Sweden for his work in developing the verification strategy for ATC2.
- Bertil Sjöbergh of Ansaldo Sweden for further development and marketing of ATC.
- Denny Pascoe and Alan Swiss of Union Switch & Signal for providing information on the New Jersey Transit system and the Copenhagen underground.

References

[1] Friman, B. 1999. Software Validation Inspection Report for Combined Danish-Swedish ATC System Version 2.2, Validation report, June 4, 1999. (ATSS Company Confidential)

[2] Hansson, H., H. W. Lawson, M. Strömberg, and S. Larsson, 1996, BASEMENT: A Distributed Real-Time Architecture for Vehicle Application, Real Time Systems, The International Journal of Time-Critical Computing Systems, Vol. 11, No. 3, November, 1996.

[3] Hansson, H., H. W. Lawson, O. Bridal, C. Eriksson, S. Larsson, H. Lön, and M. Strömberg, 1997. BASEMENT: An Architecture and Methodology for Distributed Automotive Real-Time Systems, IEEE Transactions on Computers, Vol. 46, No. 9, September, 1997.

[4] Lawson, H.W., 1975. Recommendations for Software Organization and Execution Control for the MPU, Consultants Report to Standard Radio and Telefon AB, October 23, 1975

[5] Lawson, H.W., 1976. Preliminary Proposal for a Comprehensive Software Plan for ATC, Consultants Report to Standard Radio and Telefon AB, November 9, 1976

[6] Lawson, H.W., 1990. Philosophies for Engineering Computer-Based Systems, IEEE Computer, Vol. 23, No. 12, pp. 52-63, December, 1990.

[7] Lawson, H.W., 1992. CY-CLONE - An Approach to the Engineering of Resource Adequate Cyclic Real-Time Systems, Real Time Systems, The International Journal of Time-Critical Computing Systems, Vol. 4, No. 1, February, 1992.

[8] Lawson, H.W., 1992. Engineering Predictable Real-Time Systems, appearing in Real Time Computing, Springer Verlag, 1994, Lectures from a NATO Advanced Study Institute, October, 1992.

[9] Lawson H.W. and B. Svensson 1993. An Architecture for Time-Critical Distributed/Parallel Processing, Proceedings of the EUROMICRO Workshop on Parallel and Distributed Processing, IEEE Computer Society Press, January 1993.

[10] Lawson, H.W., Wallin, Sivert , Bryntse, Berit and Friman, Bertil. Twenty Years of Safe Train Control in Sweden, Proceedings of the Symposium on the Engineering of Computer-Based Systems, Washington, DC, 2000.
[11] Lawson, H.W., 2007. "A Journey Through the Systems Landscape". Version 8.0 – A book in preparation for publication.
[12] Lundbäck, K-L, C. Eriksson, and H.W. Lawson, 1995. A Real-Time Kernel Integrated with an Off-Line Scheduler, Proceedings of the 3rd IFAC/IFIP Workshop on Algorithms and Architectures for Real-Time Control, Ostend-Belgium, 1995.

Appendix A

Historical Timeline

1973	Standard Radio decides to enter the train control market place Swedish State Railways (SJ) requests proposals on a transmission system
1974	Standard Radio, Philips, Ericsson Signal develop transmission solutions
1975	SJ selects the Ericsson Signal approach for the transmission system Standard Radio starts work on an onboard system concept SJ favors the Standard Radio onboard mechanical structure Work on the software architecture concept begins
1976	A problem related architecture evolves Guidance for development, production, testing, and maintenance
1977-79	Standard Radio selected for the onboard system for SJ trains Development, testing and verification Contract to Ericsson Signal for onboard system for SL trains only[1] Integration of transmission and onboard systems followed by validation
1980	Installation of ATC1 on SJ locomotives
1980-93	ATC1 operates successfully without any changes in software
1988-92	ATC2 plan: SJ, NSB[2], EB-Signal, Standard Radio-ATSS, Teknogram Further development based upon ATC1, testing, verification, validation
1993	Installation of ATC2
1995	Radio block solution introduced Linköping-Västervik line (ATC2.1)
1997-2000	Development and installation of Öresunds bridge system solution (ATC2.2)

1. SL – Stockholm's Local Traffic. Utilizes a different onboard solution based upon N-version programming. Different program solutions deployed and output results compared. This solution was inherited by Elektrisk Byrå AB, ABB Signal AB, Adtranz AB and finally Bombardier.
2. NSB - Norwegian State Railways