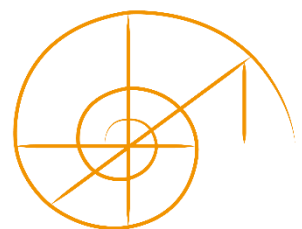


WHITE PAPER

FORMAL METHODS IN ACTION IN THE RAILWAYS

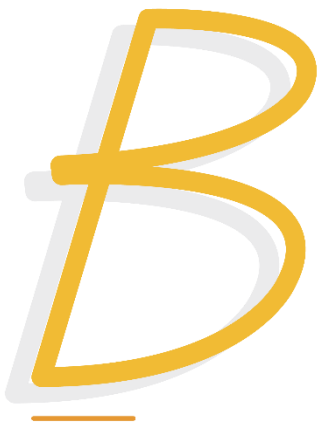
When safety is not an option



CLEAR SY
SYSTEMS ENGINEERING

Formal methods and industry are not so often associated in the same sentence as the former are not seen as an enabling technology but rather as difficult to apply and linked with increased costs. In the 1990s, the introduction of the B method and the Event-B language into several industrial development processes was witnessed with more or less success, even if new tools and new practices were available to ease acceptance in industry. At that time, a number of research projects and non-trivial industrial applications had backed these two formal methods. Almost 10 years later, after several real size experiments in diverse application domains, the situation has slightly evolved and this white paper intends to make clear how the B method, the Event-B language and the Formal Data Validation have contributed to a safer world.

The B Method



The B Method was introduced in the late 80's to correctly design safe software. It is a formal method to develop software mathematically proved to comply with its specification. It relies on a mathematical model of the software, containing both what the software is expected to do and its algorithm.

The software model is decomposed into smaller models in order to manage the complexity ("divide and conquer").

The model is proved: the algorithm doesn't contradict its specification.

The software code is generated from the implementation model. Code is readable, very close to the model and is easily checked. The final software application is made of parts developed with B and parts not developed formally.

The main idea was to avoid introducing errors by proving the software while being built, instead of trying to find errors with testing after the software was produced. Promoted and supported by RATP¹, B and Atelier B have been successfully applied to the industry of transportation, through metros automatic pilots installed worldwide. Paris Meteor line 14 driverless metro is the one of the main reference applications with over 110,000 lines of B models, translated into 86 000 lines of Ada. No bugs were detected after the proof was completed, neither at the functional validation, at the integration validation, and at the on-site testing, nor since the beginning of the metro line operation (October 1998). For years, Alstom Transportation Systems and Siemens Transportation Systems (representing a major part of the worldwide metro market) have been the two main actors in the development of B safety-critical software. Both companies have a product based strategy and reuse as much as possible existing B models for future metros. As an example, the Alstom Urbalis 400 CBTC (Radio communication based train control) equips more than 100 metros in the world, representing 1250 km of lines and 25 %² of the CBTC market.

¹ Paris metro authority

² Source : <http://www.alstom.com/products-services/product-catalogue/rail-systems/signalling/products/urbalis-400/>

For such applications including driverless metros, B modeling is used for safety critical functions for both track-side (zone controller, interlocking) and on-board (automatic train pilot or ATP) software. The interlocking part has to avoid having two trains on the same track section. It computes Boolean equations that represent the tracks status as seen from diverse sensors. The automatic pilot is mainly in charge of triggering the emergency brake in case of over-speed. It requires several functions such as the localization that involve several graph-based algorithms, and the energy control which computes the braking curve of the train, based on the geometry of the tracks. Data types used are integer for the energy control, Booleans for the interlocking and tables of integer for the tracks.



Figure 1: automatic driving metro subsystems, based on the B method, installed worldwide (Alstom Urbalis, Siemens Mobility Trainguard)

To date, the biggest B software is a XML compiler enabling the execution of safety critical embedded applications by an interpreter. The B models generate more than 300,000 lines of Ada code, for this SIL4 T3-compliant (EN50128) program. The method is not limited to 300,000-line software and has not met any bottleneck until now. Therefore, the method is likely to scale up to larger, non-threaded software.

At the other end of the scale, with platform screen doors (PSD) or remote inputs/outputs controllers, less demanding in term of computation, smaller applications are generated for both programmable logic controllers (PLC) and PIC32 microcontrollers, with a maximum of 64 KB in memory per software. SIL3 and SIL4 controllers, in charge of opening and closing platform screen doors have been (or will be) installed in Paris (L1, L4, L13), Stockholm (Citybanan) and Sao Paulo (L2, L3, L15 Monorail).

This modelling approach is slightly specific but comes along many interesting features. The “specification before code” motto imposes a top-down approach (or by-decomposition). Software developers are encouraged to specify first, from natural language requirements. It does not prevent to reuse existing software but avoids asking the dangerous question “what do I get if I gather all these software components together?”

The target software is cyclic and single-threaded. No interrupt should modify the state variables. Full integer arithmetic is supported (non-trivial floating-point arithmetic is practically not provable) as well as Boolean predicates and equations (and arrays of integers and Booleans).

The models are text-based. The same mathematical language (B) is used for the specification model and the implementation model, based on set theory (ex: $A \subseteq B$) and predicate logic (ex: $P \Rightarrow Q$). The model contains both the software properties (the static aspect) and its behavior (the dynamic aspect). A proved model means that the specification is consistent (no contradiction) and the implementation complies with its specification. *A minima*, the software is proved to be programming error-free.

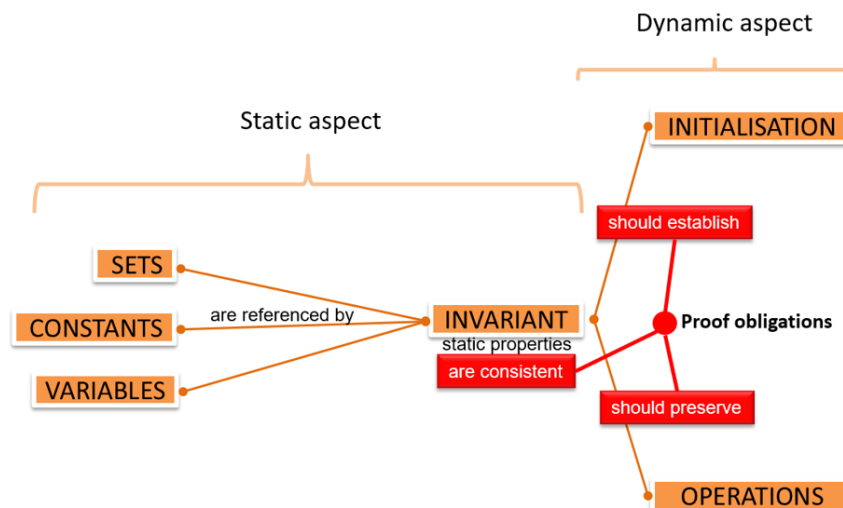


Figure 2: the relations between the B modelling elements

There are many reasons to use B for safety critical software development:

- Improved level of confidence, brought by the mathematical formalism and the proof. The use of B removes ambiguities as the mathematical model captures the meaning of the software.
- Early error detection. Errors are discovered by proof during modelling and not by test once the software is built.
- Most testing is useless. Proof replaces testing. Mathematical proof is exhaustive while testing is not.
- Avoid redundant software development. For highest safety integrity level, only one B model required, compared with two software developed more traditionally by two independent teams.
- Accepted for certification. Several industrial standards recommend or strongly recommend the use of formal methods (EN50128, IEC61508).

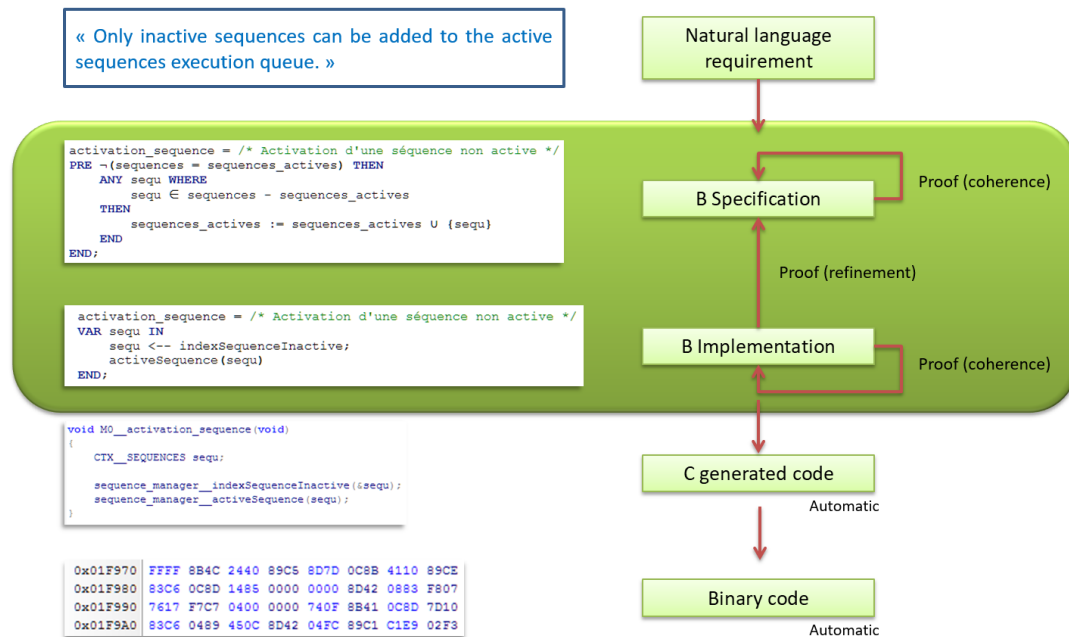


Figure 3: the complete path from requirements to binary code. The proof-by-construction principle applies to the green area (specification, implementation). Conformance crosschecks (requirements and source code) require other means.

The Event-B Language

```

File Edit View Search Help
M0.sys
1- SYSTEM
2- M0
3- CONSTANTS
4- C0, C1
5- PROPERTIES
6- C0 <: INTEGER & C1 <: C0
7- VARIABLES
8- interv
9- INVARIANT
10 3/3 interv <: C1
11- INITIALISATION
12 1/1 interv :: POW(C1)
13- EVENTS
14  add_element =
15 1/1 ANY v_ WHERE
16    v_ : C1 - interv
17  THEN
18 1/1 interv := interv \ {v_}
19  END;
20  remove_element =
21 1/1 ANY v_ WHERE
22    v_ : interv
23  THEN
24 1/1 interv := interv - {v_}
25  END
26  END

```

A broader use of B appeared in the mid '90s, called Event-B, to analyze, to study and to specify not only software, but also systems³. It extends the usage of B to systems that might contain software, hardware and equipment, environment, and also to intangible objects like process, procedure, business rule, etc. In that respect, one of the outcome of Event-B is the proved definition of systems architecture in its environment and, more generally, the proved development of, so-called, "system studies", which are performed at the beginning, before the specification and design of the software. This enlargement allows one to perform failure studies right from the beginning, even in a large system

development.

Event-B is used for formal modelling to progressively analyze and verify by proof a system-level specification. It relies on a mathematical model of the system, containing both the

³ system is here considered in its widest definition

properties of the system and its evolution rules. The evolution rules are encoded in the form of a collection of asynchronous events that may be triggered based on conditions and may modify the system state variables. The modelling is progressive as the model is made more and more detailed, and complexity is added gradually. The top-level model is simplified (abstracted) with few state variables modelled. Modelling details are added to successive models (refinements). Events and properties have to be rewritten to consider these details. For example, a train can be seen as a point moving on a line then can be refined by adding details like the numbers of cars, the length of train, its braking capability, the track slope, etc.

“The model is proved” means that the evolution rules enforce the properties of the system.

Similarly, there are many reasons to use Event-B to model systems:

- Improved level of confidence. It is brought by the mathematical formalism and the proof. It enables the assessment of complex specification (structure, behavior) in the early stages. The model may be checked against scenarios. Finally, better software specification are derived from this modelling.
- Ambiguities are removed. The mathematical model captures the meaning of the system specification.
- Easier test definition. The modelling allows defining which tests have to be performed for subcomponents acceptance and before daily operation.
- Accepted for certification. Several industrial standards either recommend or strongly recommend the use of formal methods (EN50128, IEC61508), or require the use of formal methods (Common Criteria).

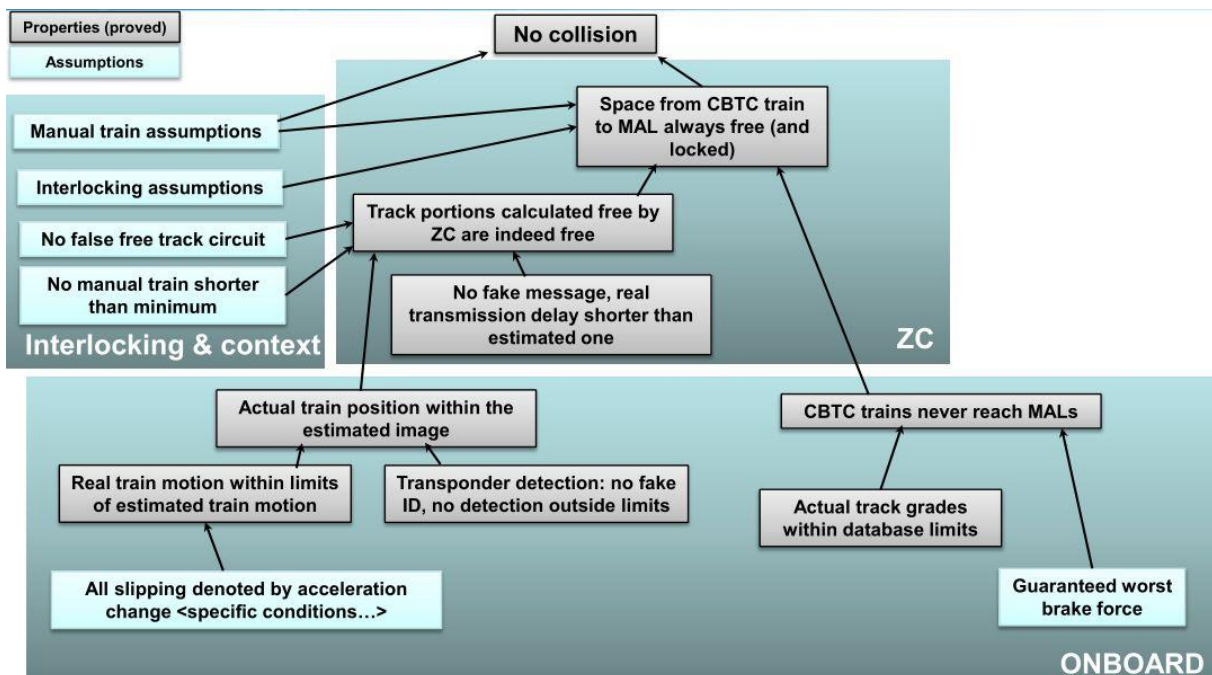


Figure 4: NYCT line 7 modernization project - the structure of the formal proof for the main safety properties of the system: no collision and no over-speeding. Event-B/Atelier B was used to support the mathematical demonstration.

Event-B is used in a number of safety cases. The fundamental goal is to extract the rigorous reasoning establishing that the considered system ensures its requested properties and is safe, and to assert that this reasoning is correct and fully expressed. At system level, this rigorous reasoning involves the properties of different kind of subsystems (from computer subsystems to operational procedures), that the formal proof shall all encompass. Event-B is used to formalize the reasoning with a collection of separate models: each model is readable and understandable by a non-expert and does not require to dig into hundreds of events and tens of refinement levels. This approach was used for the system formal verification for the CBTC of New York subway line 7 in 2012 and Flushing in 2014 (effort divided by two due to models reuse). It was also deployed by the SNCF to design a new signaling system, based on a degraded version of ERTMS, aimed at low-traffic, regional lines. At this moment, RATP is making use of it for the system formal verification for the CBTC of Paris subway line 4.

Atelier B



Atelier B is the reference tool from ClearSy, freely available and fully functional:

- for the development of (safety critical) software . It supports the B method and the B language.
- for the modelling of systems. It supports the Event-B language.

It includes several model editors, proof tools and code generators. It has been used for certified applications up to SIL4 (EN50128) in the railways and EAL6+ (Common Criteria 3.1) in the smartcard industry. A dedicated support (more frequent Atelier B releases, privileged access to beta features for evaluation, short-term bug correction) is provided for maintenance contract holders. ClearSy also proposes courses and services to help its customers.

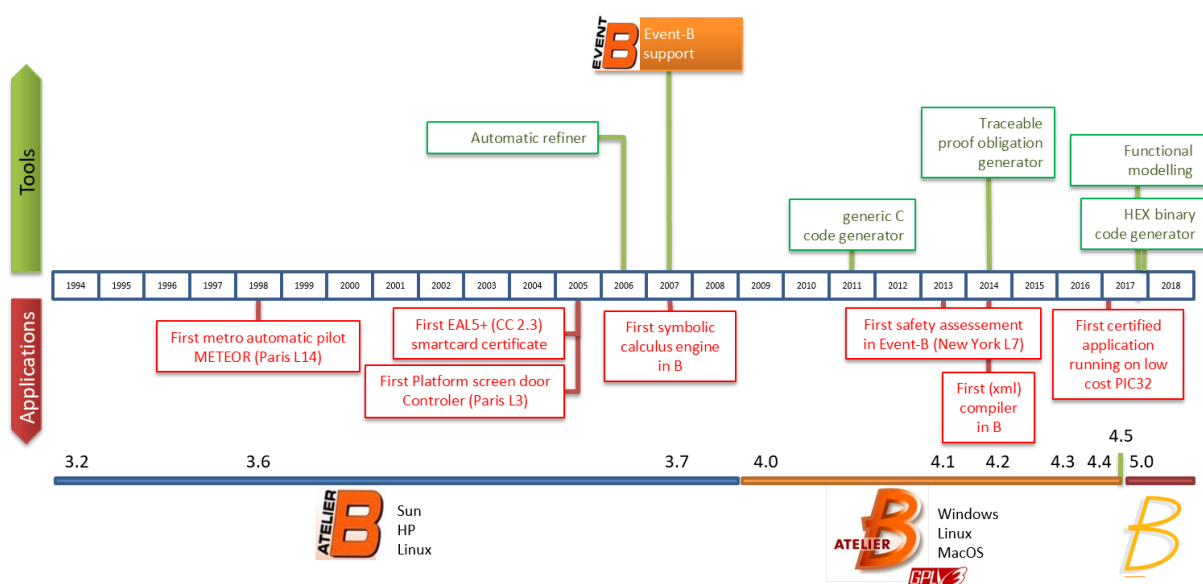


Figure 5: Atelier B timeline showing the major improvements (in green) and the first new kinds of applications (in red), since its infancy.

Formal Data Validation

In the railways, software are usually developed and validated independently from the parameters or constant data that fine-tune its behavior. For example, the track topology, signal and switch positions, kilometer points, etc. are constant data used by an automatic pilot to compute breaking curves and to determine when to trigger the emergency braking. In order to avoid a new compilation if the data are modified but not the software, two different processes define the software and the data validations.

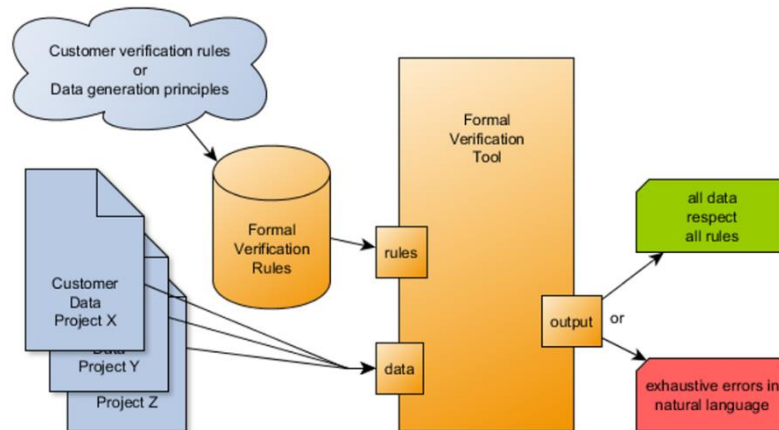
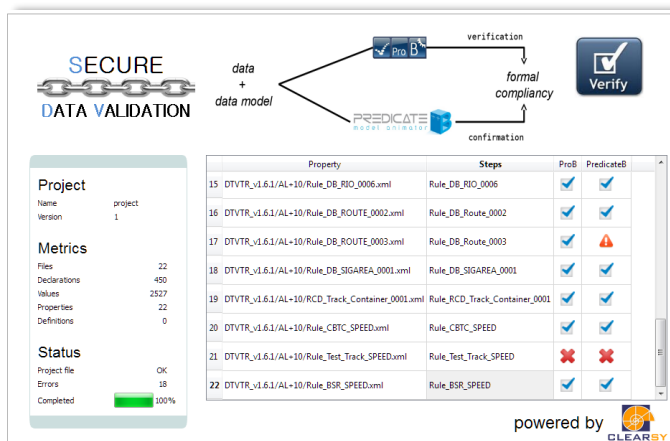


Figure 6: Formal data validation scheme

Data validation consists in checking a heterogeneous data collection⁴ against a set of properties / rules⁵ issued from regulation, exploitation constraints, train manufacturer product design, etc. Manual data validation used to be entirely human, leading to painful, error-prone, long-term activities (requiring several months to check manually up to 100,000 items of data against 1,000 properties / rules).



Formal data validation is the natural evolution of this human-based process into a more secure one where:

- the properties / rules are formalized, to constitute a formal data model (mathematical, based on the B language). It is built from natural language inputs.
- the verification of conformance between the data collection and the formal data model is performed by a formal tool (or by a combination of redundant formal tool if required)

⁴ CBTC or ETCS configuration data, IXL or RBC parameters, etc.

⁵ For example, “successive track circuits should have continuously increasing kilometer points”, “there exists a path between two distinct track circuits”, “signals should be positioned a minima 100 meters before the switch they protect”, etc.

This approach has been invented by ClearSy, thanks to its deep knowledge and skills on formal method technology and associated tools.

The benefit of this formal approach is diverse:

- It is fast: up to 10x faster than a pure human verification, a couple of hours is enough for validating a complete railway project
- It is automatic, push-button and repeatable at will
- It removes human errors, as it makes use of certified formal techniques
- It allows a strong reuse from one project to another (capitalization of the knowledge)

Formal data validation is industry ready. Several major players currently have deployed it, such as:

- Alstom – more than 20 metros (Urbalis) and tramways
- General electric – for the Singapore metro
- RATP (Paris metro authority)
- SNCF (French Railways) – for checking the interlocking tables on the main lines (Mistral NG)
- Siemens Mobility – for metros (Trainguard)
- Thales

Bibliography

- Benveniste, M.V.: [On using B in the design of secure micro-controllers: An experience report](#). Electr. Notes Theor. Comput. Sci. 280 (2011)
- Hansen, D., Schneider, D., Leuschel, M.: [Using B and prob for data validation projects](#). In: Abstract State Machines, Alloy, B, TLA, VDM, and Z - 5th Int'l Conf., ABZ 2016, Linz, Austria, May 23-27, 2016
- Lecomte, T.: [Safe and reliable metro platform screen doors control/command systems](#). In: FM 2008: Formal Methods, 15th Int'l Symposium on Formal Methods, Turku, Finland, May 26-30, 2008
- Lecomte, T.: [Applying a formal method in industry: A 15-year trajectory](#). In: Formal Methods for Industrial Critical Systems, 14th Int'l Workshop, FMICS 2009, Eindhoven, The Netherlands, November 2-3, 2009
- Lecomte, T.: [Double cœur et preuve formelle pour automatismes sil4](#). 8E-Modèles formels/preuves formelles-sûreté du logiciel (2016)
- Lecomte, T., Burdy, L., Leuschel, M.: [Formally checking large data sets in the railways](#). CoRR abs/1210.6815 (2012)
- Sabatier, D.: [Using formal proof and B method at system level for industrial projects](#). In: Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - 1st Int'l Conf., RSSRail 2016, Paris, France, June 28-30, 2016

Executive Summary

Formal methods are now industry ready, able to scale up to real size railway projects and to provide a real support for successfully completing safety demonstrations.

In this white paper, we show that several formal methods (B, Event-B, formal data validation) directly contribute to safety critical software development, system-level specification analysis and constant parameters validation, with the help of mathematical proof.

Based in Aix en Provence, Lyon, Paris and in Strasbourg, ClearSy is a French SME company, which specializes in developing SIL1 to SIL4 level safety systems and software. It develops complex systems, from their design to putting them into service, and undertakes the interim stages of validation, checking and safety testing. ClearSy is particularly active in the development of systems and software in the railway, car, military, nuclear energy and space industries.

<http://www.clearsy.com/en/>

<http://www.fersil-railway.com/en/>

<http://www.atelierb.eu/en/>

