Prover

Company Introduction, August 2022

Prover Facts

- Privately owned, founded in 1989
  - Formal Methods for mission critical embedded/software systems
  - For the last 15 years focus has been on rail control systems
  - The leading supplier of design automation and formal verification solutions for rail signalling systems
- HQ in Stockholm, Sweden
  - Sales and engineering in France, China and US
- 30+ employees
  - Combining expertise within software development, formal methods and rail control systems
  - 10+ mathematics and computer science PhDs

Business Focus

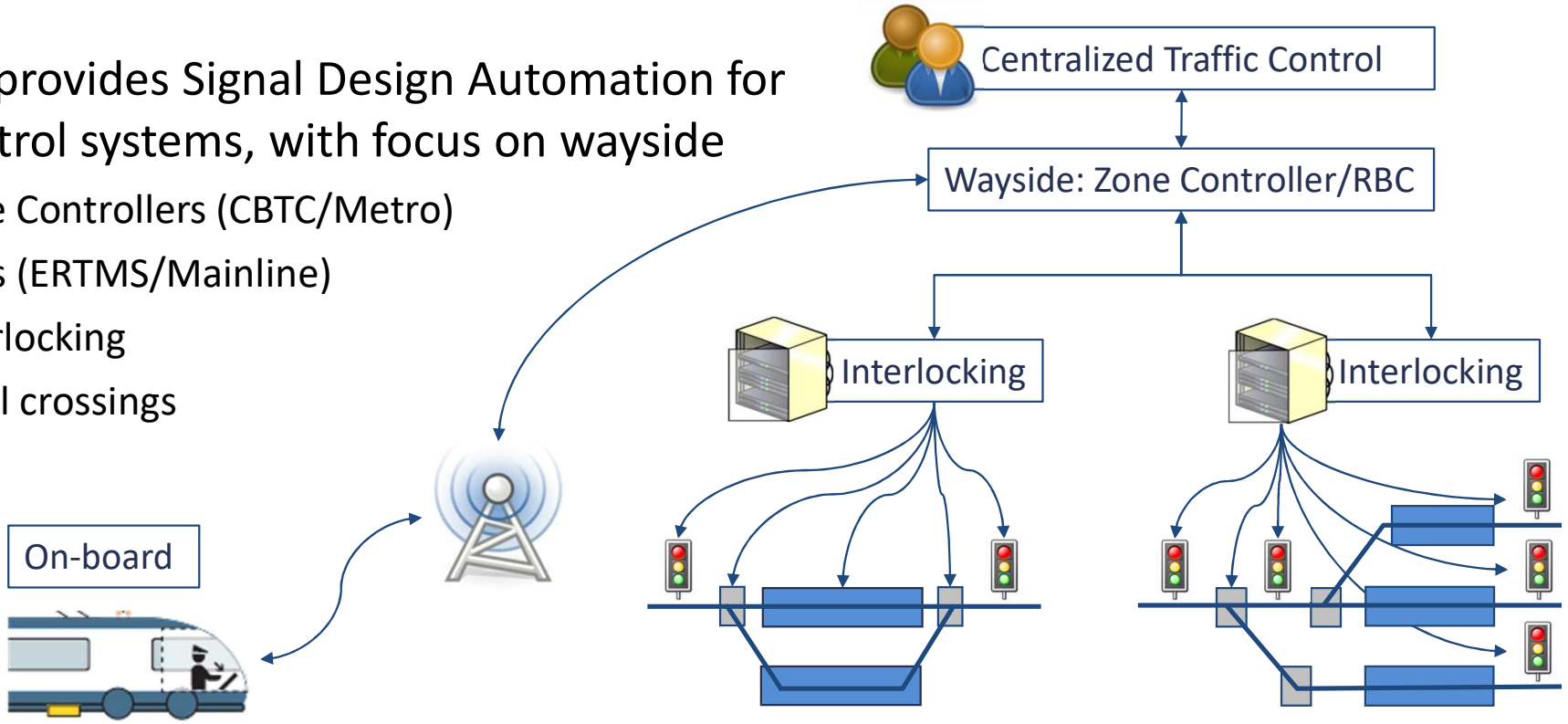
- Design Automation for rail control systems, helping customers to:
  - Formally verify safety
  - Define and maintain requirement specifications
  - Increase safety and capacity
  - Decrease costs and project delays
- Customers
  - Rail infrastructure managers
  - Suppliers of rail control systems
  - Mainline, light rail, metro, freight, …

- Products and Solutions:
  - Prover Trident
  - PiSPEC, HLL & LCF
  - Prover iLock
  - Prover Certifier
  - Prover Extractor
- Professional Services:
  - Safety analysis and assessment
  - Requirement specification and formalization
  - Turnkey verification projects
  - Turnkey design projects

Software-based rail control systems

Prover provides Signal Design Automation for rail control systems, with focus on wayside

- Zone Controllers (CBTC/Metro)
- RBCs (ERTMS/Mainline)
- Interlocking
- Level crossings



Signal Design Automation – Benefits

- Develop Application Specific Software in days
  - Including CENELEC EN 50128 compliant safety evidence
  - From Generic Application capturing signaling requirements
- Experiences of Signal Design Automation show:
  - Effort in man hours reduced by 50%
  - Overall cost savings of 50%
  - Calendar time reduced by 50%
  - Simplified maintenance
  - Improved consistency and fewer issues
  - Increased end-customer satisfaction

Key features of Signal Design Automation tools:

- Configuration of specific applications
- Automated generation of design and revenue service code
- Automated functional test
- Safety verification based on formal proof, providing 100% coverage
- CENELEC EN 50128 compliance

Formal Verification - benefits

Formal Verification: mathematical proof of the system's safety, providing 100% coverage

- Manage increased system complexity: testing is not enough!
- Reduce effort and time-to-market, can be fully automated

Required by Infrastructure Managers as the only cost-efficient way of assuring safety

- Metros of New York, Stockholm and Paris; national railways of Sweden and France. With more following…
- A Working group within the European initiative Shift2Rail is working on Formal Methods and Verification

In demand from suppliers to drive down verification costs while maintaining quality

- Proving safety is key to be able to quickly respond to requirement changes and change requests
- Verification process from **months to days**

Formal Verification key Benefits:

- Increased confidence in safety, with 100% coverage
- Reduced on-site testing
- Automation, reduces effort and cost
- Repeatable, supporting the maintenance phase
- Helps find, and resolve, issues earlier in the process

Formal Specifications – Benefits for IMs

- Allows Infrastructure Managers to get control of their systems
  - Clear specifications are key to successful procurements
- Cost savings of up to 40%
  - Automation reduces the time and effort to develop the software (with ~50%)
  - Effort is focused on clearly defined requirement specifications
  - Testing, verification and safety assessment is simplified
- Reduced on-site testing
  - High quality software generated from the specifications and configuration data
  - Test and verification of the software completed on the desktop
  - Correct functionality at first installation
- Enabler for COTS and standard interfaces, reducing vendor lock-in

Business Models

- Rail Control Software Delivery
  - We develop formally verified and simulated code ready for revenue service, with safety case
- Safety Verification Projects
  - We perform formal safety verification, delivering a safety report
  - We perform safety assessments, delivering safety evidence and recommendations
- Joint bids
  - We provide turnkey services or license products in joint bids prepared together with you

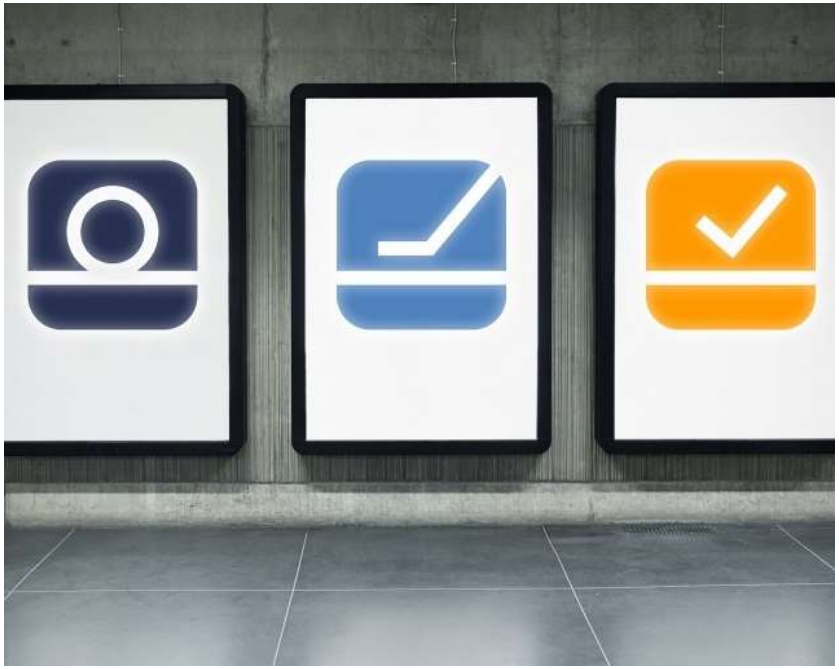
- Product Licensing, Project-Based or Time-Based
  - **PiSPEC IP**, with standard signaling principles for different end-customers
  - **Prover iLock**, for coding, simulation-based testing and/or formal safety verification in your development process
  - **Prover Certifier** for formal verification-based safety evidence, compatible with CENELEC EN50128 (SIL 4)
  - **Prover Extractor** for analysis of relay-based systems

Prover Trident: Formal Development Tool Suite

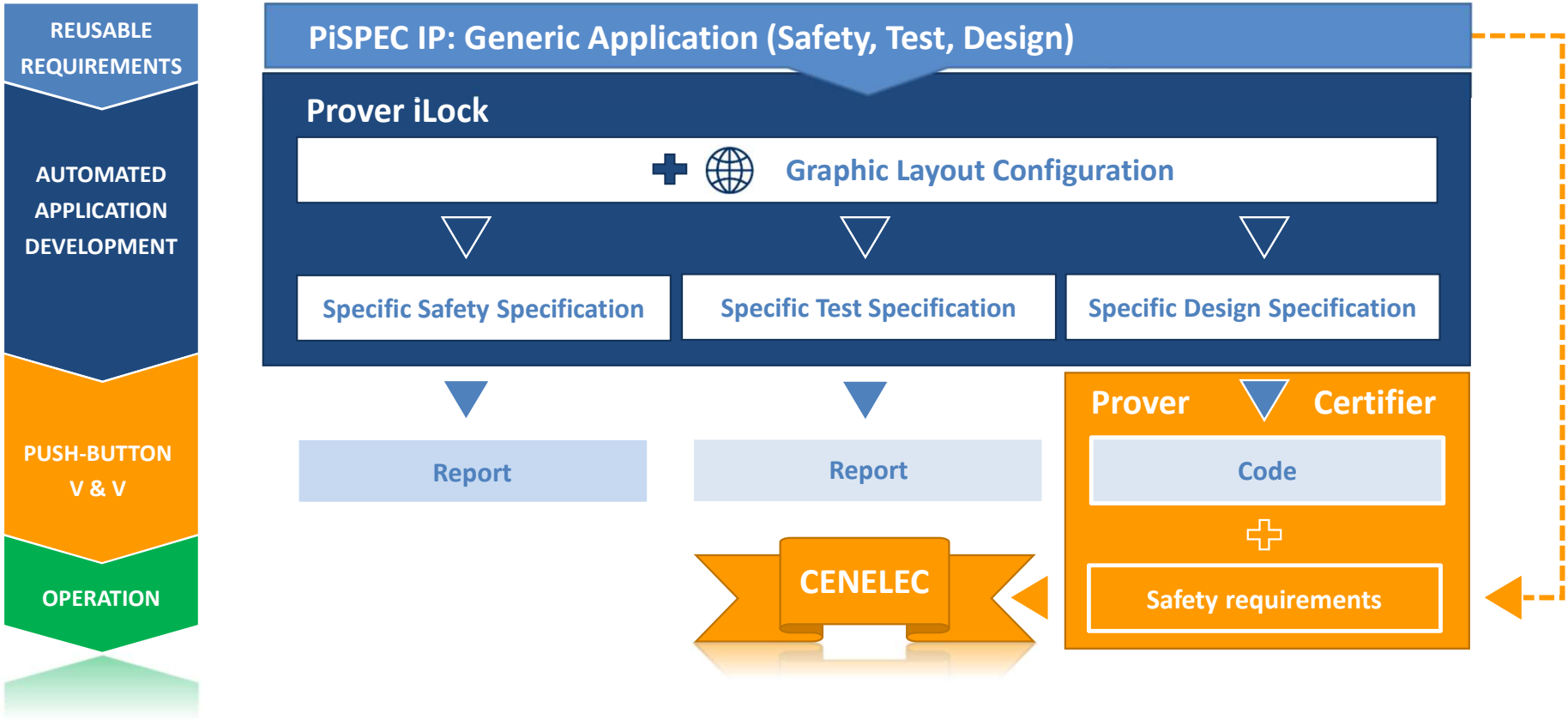
Prover Studio for formal specifications
Capture signal requirements in Generic Application Specifications in the PiSPEC language.

Prover iLock for formal development
Generate, test and verify application software from configuration and formal specifications.

Prover Certifier for formal sign-off verification
Generate CENELEC EN 50128 SIL 4 compliant safety evidence for the application software.

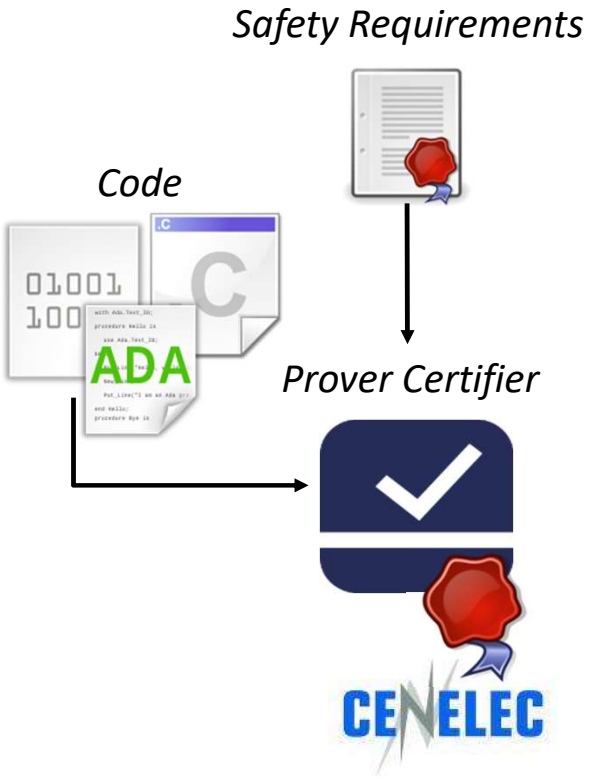


Prover Trident



Formal Verification with Prover Certifier

- Automated safety verification with mathematical proof
  - 100 % coverage
  - Highly recommend by CENELEC EN50128 for SIL 4
- Prover Certifier
  - CENELEC EN50128 SIL 4 compliant formal verification tool
  - Generates safety evidence for use in safety cases, the correctness of all steps is validated by independent tools (proofs are logged and checked)
- Can be used to verify safety of embedded software
  - Source code, and sometimes binary code, is translated into HLL
  - Translators exists for proprietary languages for rail control, general purpose programming languages (e.g. subsets of C and ADA) and model-based development tools such as Ansys SCADE



Open, Published Formal Languages

- Languages developed to meet the high demands of SDA
  - Precision, performance, certifiability, configurability
  - No built-in domain knowledge

Layout Configuration Format (LCF 2.0)

- Declare generic configuration data
- Define specific configuration data (for a system)
- Minimize compact data for manual review
- Certifiable translation to HLL (for V&V)

High-Level Language (HLL 3.0)

- Define safety requirements
- Define model of system under verification (general-purpose and vendor-specific programming languages)

- LCF Slogan: ”Readable by both humans and computers” (see blog post)

- HLL Forum develops language
  - Open language, “de facto standard”
  - Community (end users, suppliers, tool vendors)

Digital Twin

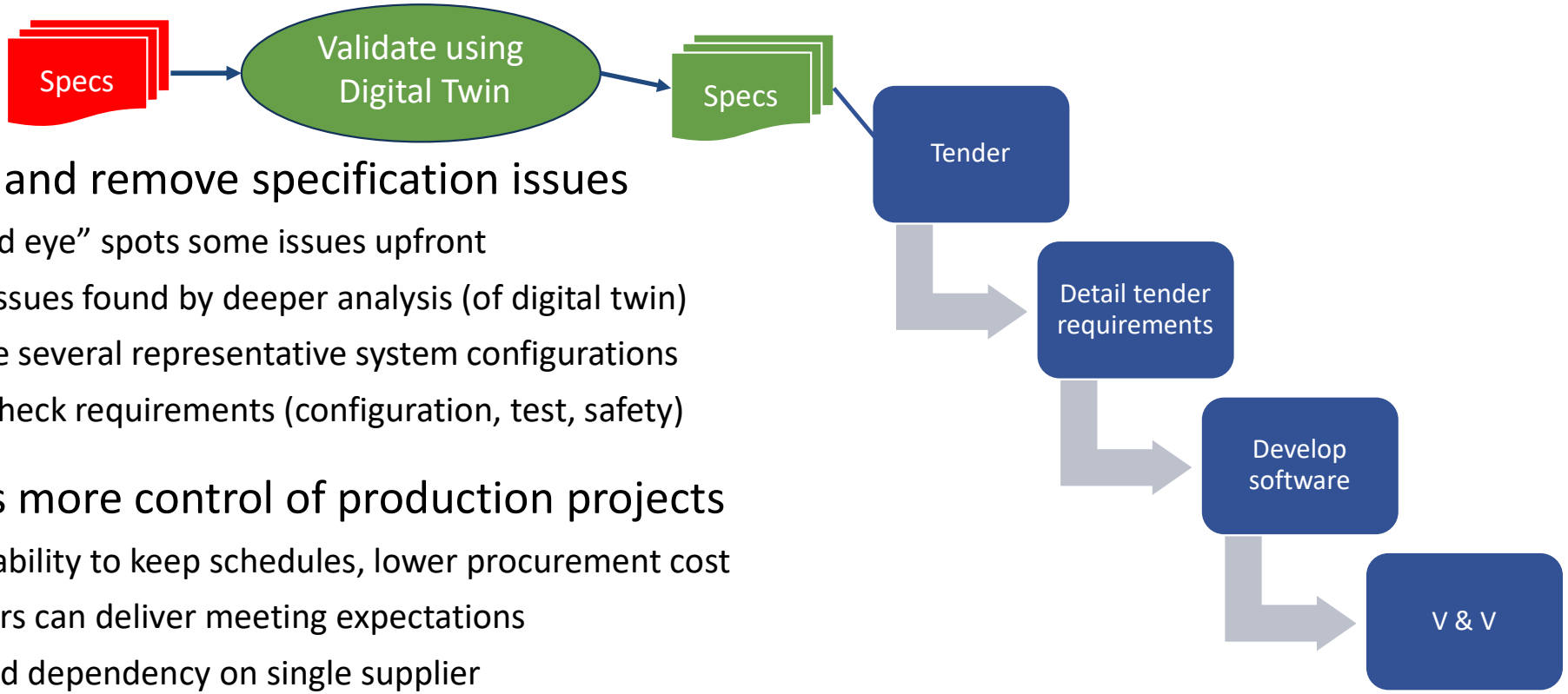
Benefits

Process

Digital twins to improve tender requirements

- End customer
  - Fewer errors in requirements, reducing cost
  - Enable different suppliers to interpret requirements the same way
  - Reduce risk for “vendor lock-in”
  - Reduce onsite testing, and surprises in projects delivering on tenders
- Supplier
  - Makes it easier to interpret requirements
  - Deliver high quality systems using less resources
- Can judge if systems comply with requirements, improved quality / safety
  - V&V can be automated with re-usable specifications
  - Reduced dependency on manual expertise and judgement

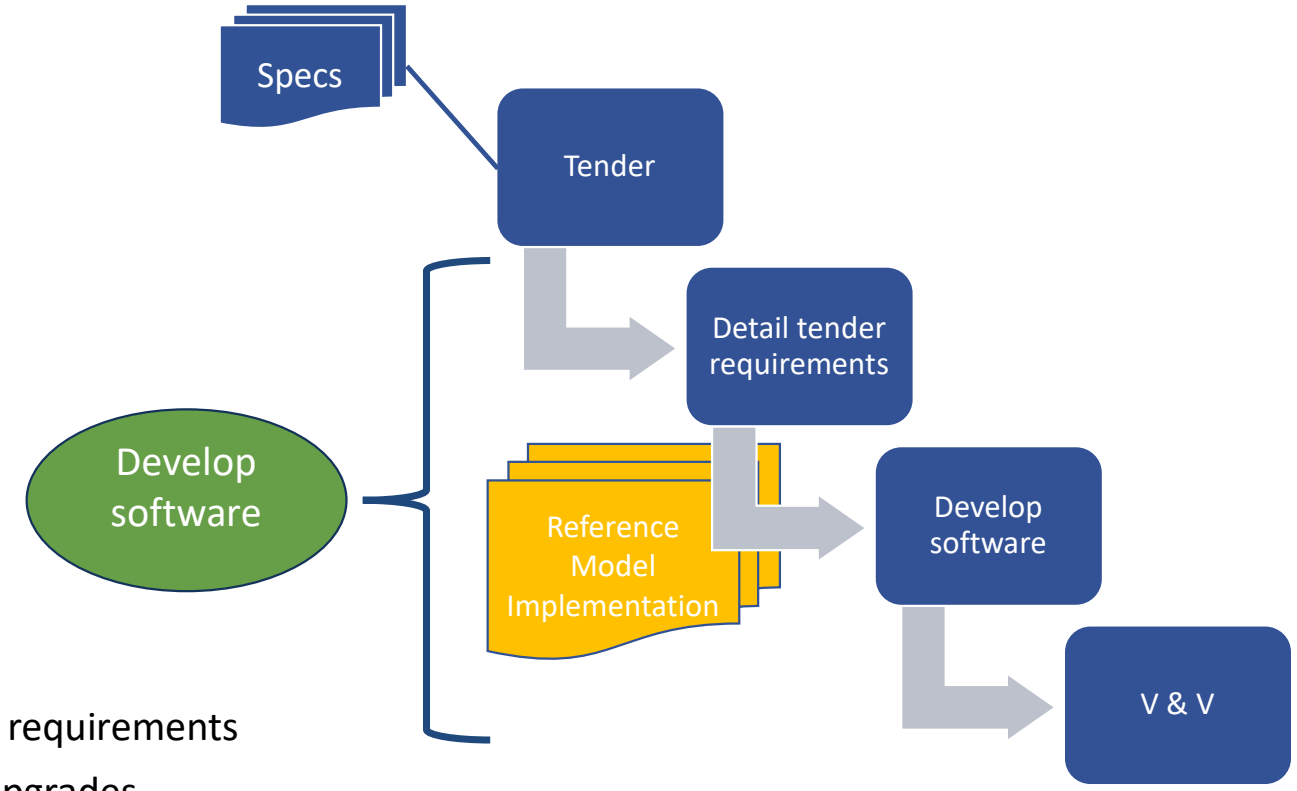
1. Digital Twin to validate tender requirements



- Identify and remove specification issues
  - ”Trained eye” spots some issues upfront
  - Other issues found by deeper analysis (of digital twin)
  - Exercise several representative system configurations
  - Cross-check requirements (configuration, test, safety)
- IM gains more control of production projects
  - Better ability to keep schedules, lower procurement cost
  - Suppliers can deliver meeting expectations
  - Reduced dependency on single supplier
  - IM can verify requirements are fulfilled

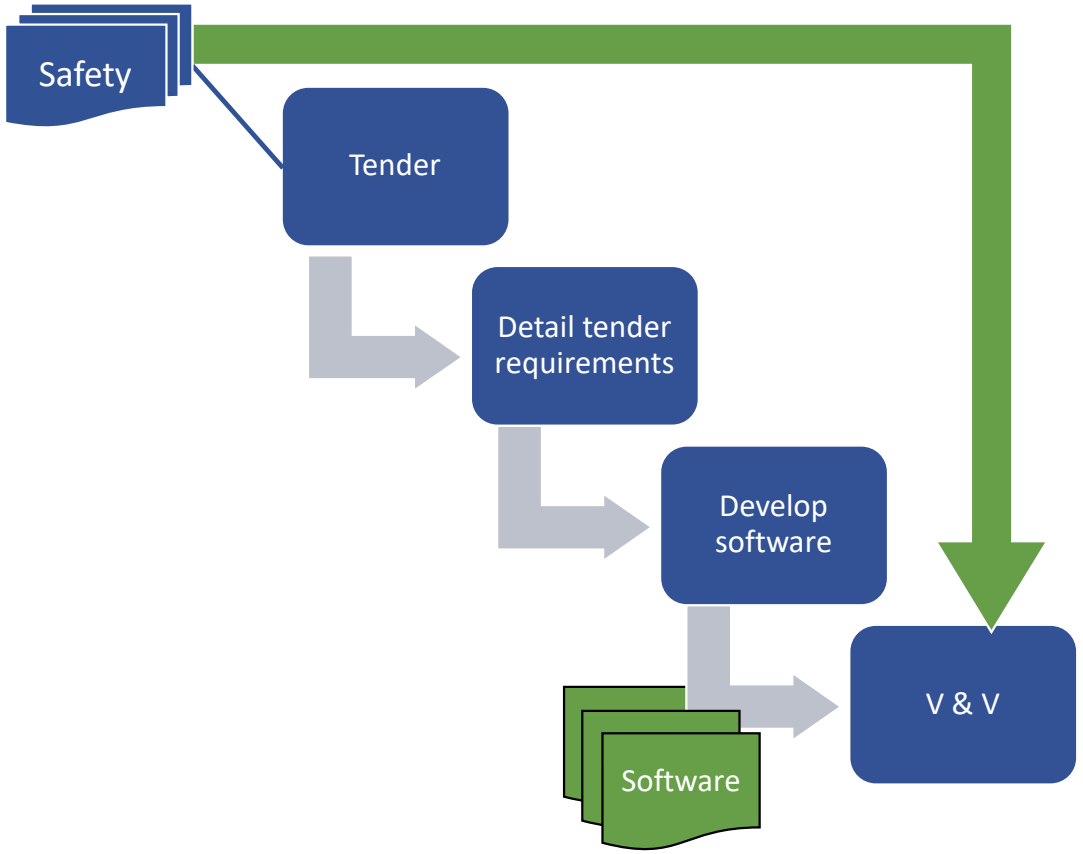
2. Create high quality software, using less resources

- Use SDA to develop software
  - Future production process
  - More automation
  - Stronger V&V
- Benefits
  - Save resources
  - Gain predictability
  - Ship high quality for less
  - Minimize risk for project delays
  - Efficiently handle change requests
  - Ensure software developed meets its requirements
  - Simplify maintenance and software upgrades



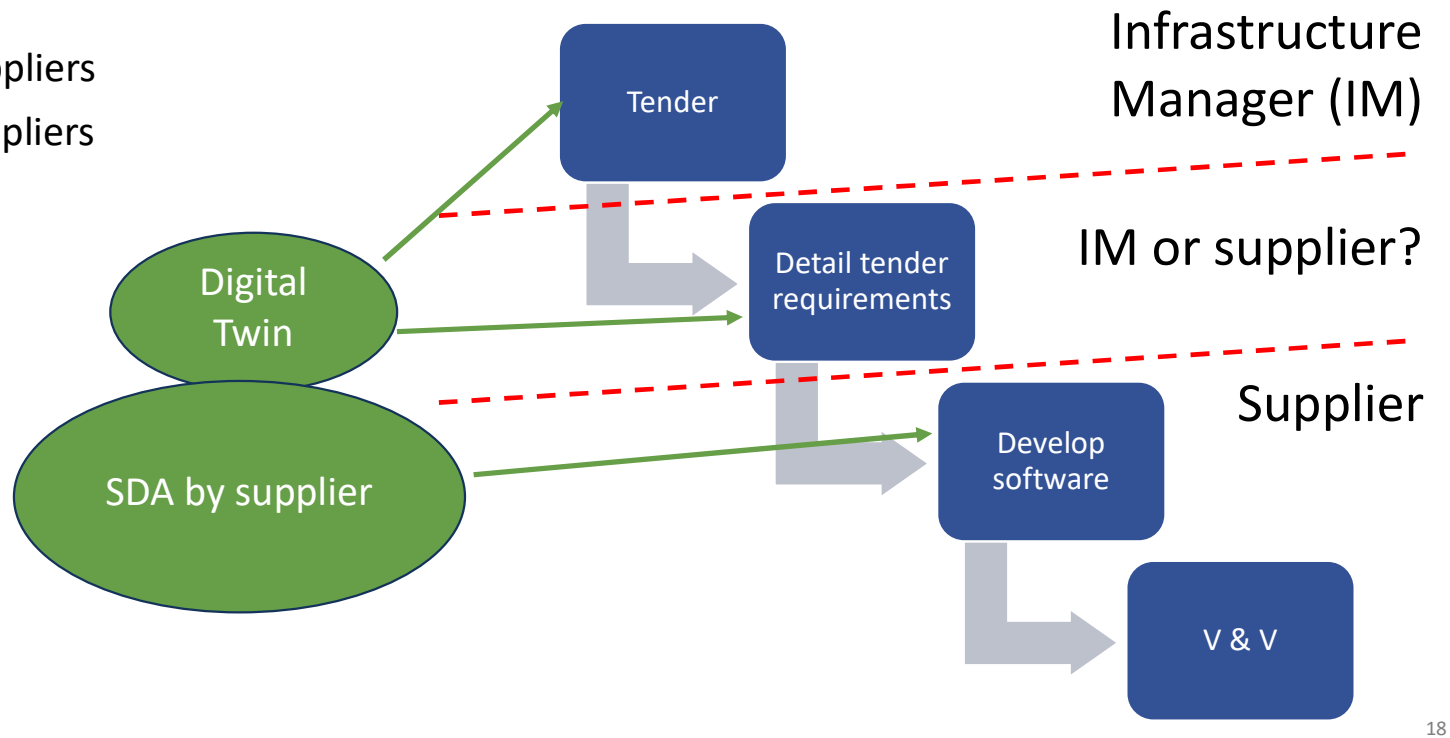
3. Verify and validate before revenue service

- Basic idea
  - Tender specifies safety requirements
  - Verify against supplier software
- Benefits
  - 100% coverage in safety verification
- Challenges addressed by digital twin (before tender)
  - Ensuring safety requirements are correct and complete
  - Save cost due to reuse of mature requirements



Future aspects: interface between customer and supplier

- Where should interface between customer and supplier be?
- Possibilities
  - Publish Digital Twin to suppliers
  - Publish SDA toolset to suppliers



Formal Verification

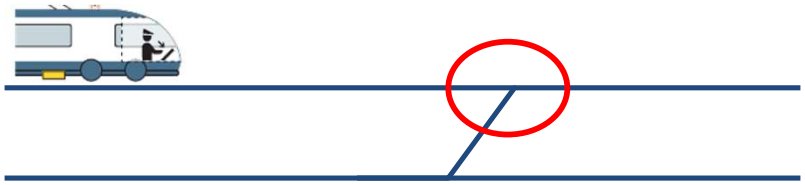
Limitations of test and simulation

- Test and simulation
  - Apply certain values to system inputs and check that values of system outputs are as expected
  - Such tests sample system responses, but cannot verify properties related to safety or security
- Safety and security properties
  - Forbidden system outputs that must never be produced, no matter what sequence of input value combinations received
  - To verify such properties exhaustively, we need mathematical analysis methods, especially **formal verification**

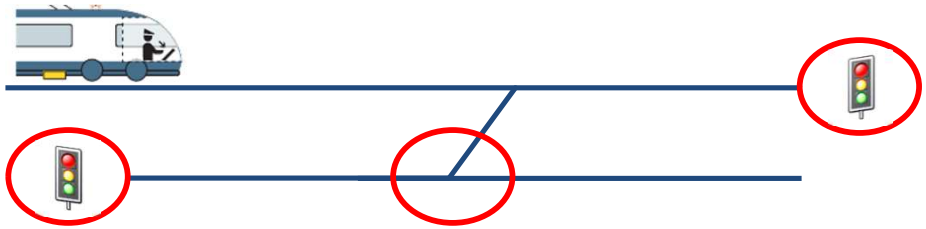
Safety requirements

Requirements state *what* must be fulfilled rather than *how*:

Switches must be in the correct position

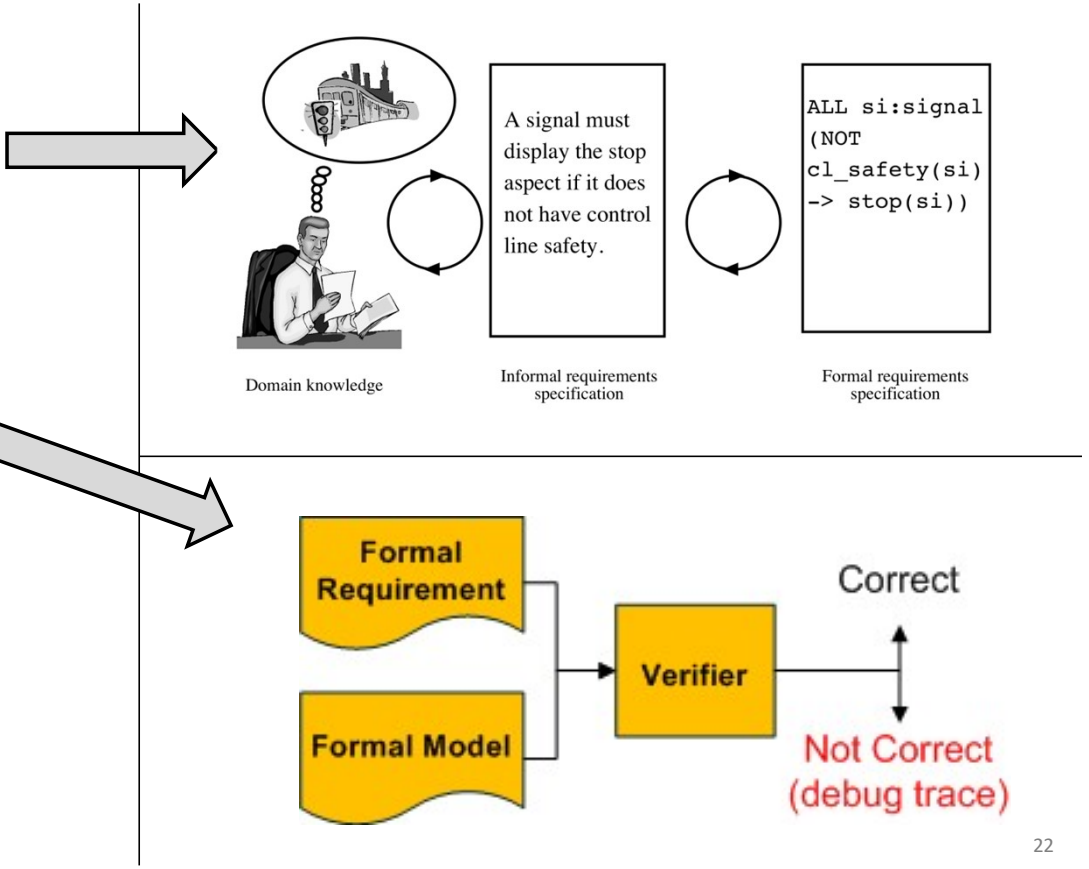


Flank protection and front protection must be established



Formal Verification

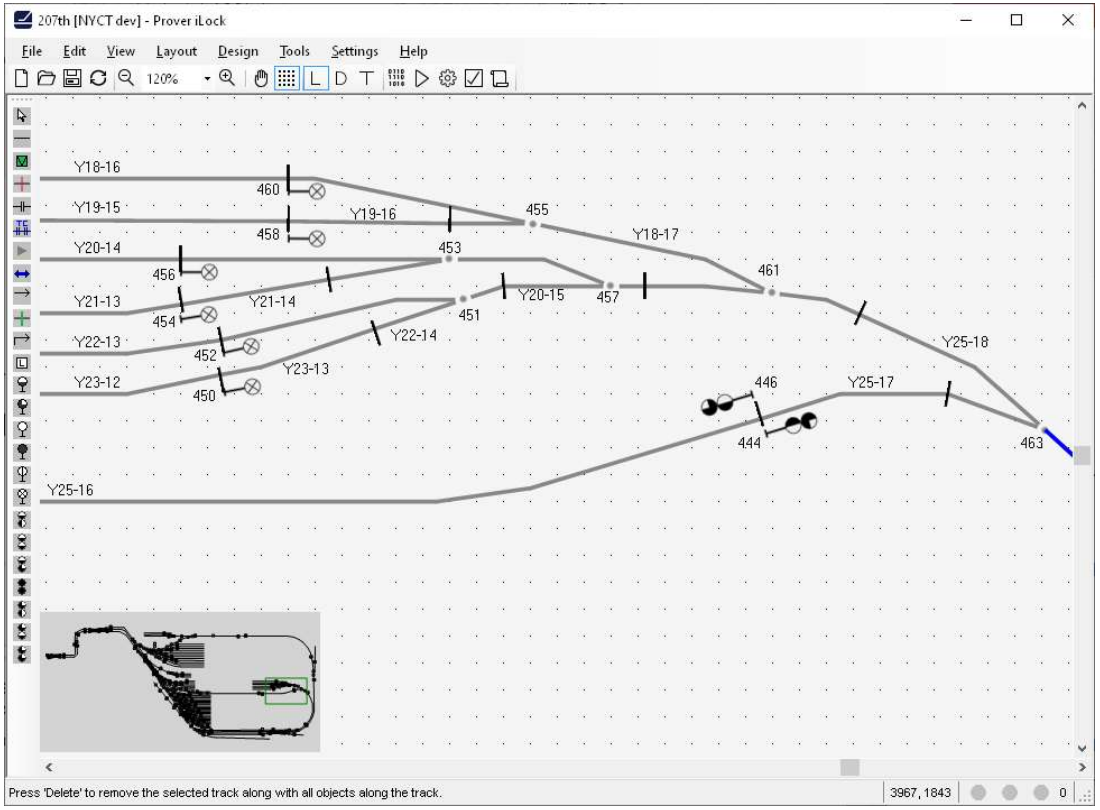
- Automated verification of requirement
  - Requirement expressed in formal logic, verified against formal system model
  - Software program proves the model satisfies the requirement, or finds counterexample for debug
- Benefits
  - Identify all meaningful errors
  - Exhaustiveness: 100% coverage in analysis
  - Soundness: results (proof) can be trusted
  - Automated: quick, repeatable



Prover iLock

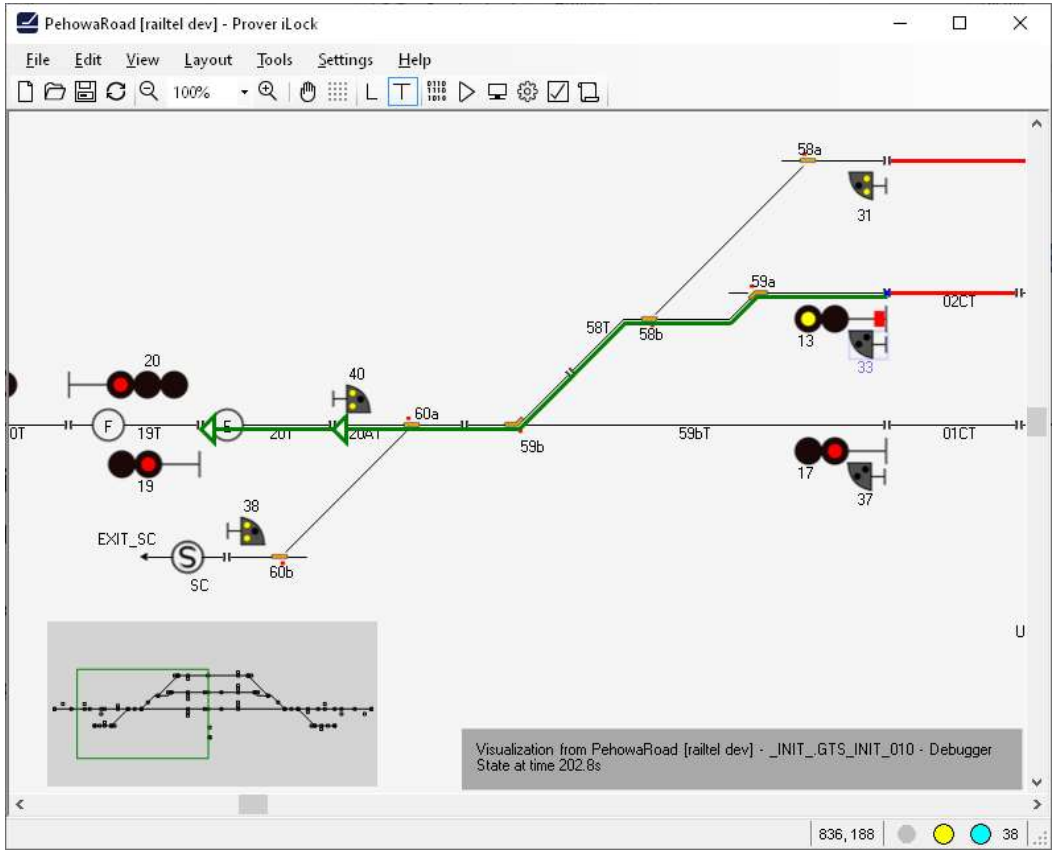
Prover iLock

- Application Engineering tool for Rail Control Software
  - Application software can be generated or imported for V&V
- Based on Generic Application defined in PiSPEC and configuration data
  - Graphical editor for e.g. track lauyout
  - Code generation/import for multiple targets, including PLC platforms, C-code and platforms from major signalling vendors (Microlok II, iVPI, Westrace Mk II, ElectroLogIXS…)
  - Functional testing with simulation
  - Formal Safety Verification
  - Support Sign-Off Verification with Prover Certifier



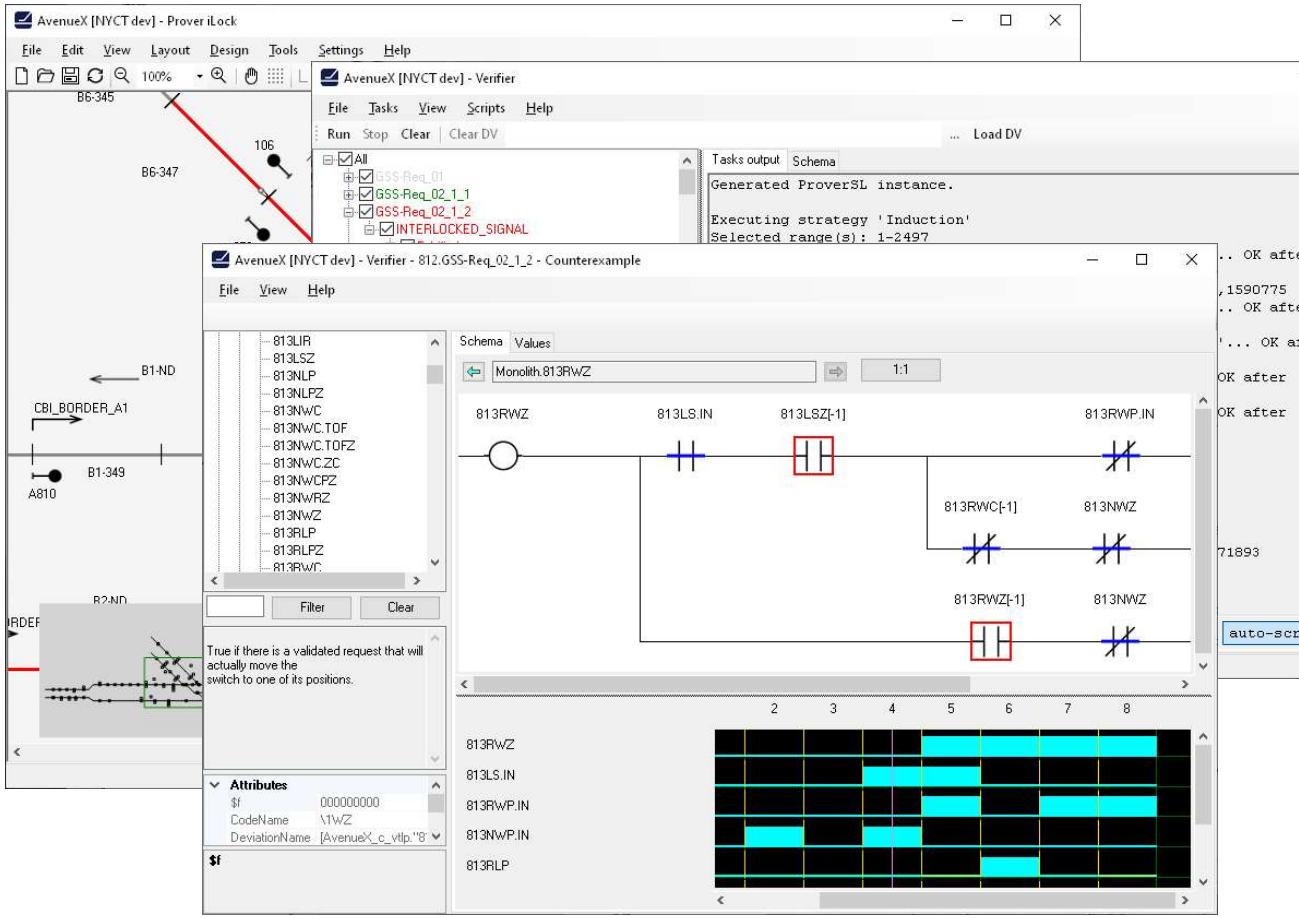
Prover iLock **Simulator**

- Test Cases defined in PiSPEC are automatically simulated
  - Test Cases are specified on generic level, specific test are cases automatically generated from the application configuration
  - States can be examined in the built-in debugger and are annotated in the track layout
  - Detailed test reports can be configured and generated
- Also supports manual, interactive, testing
  - Commands are given in the GUI
- Improved performance compared to testing on the hardware
  - Time compression
  - Multi threading
- Multiple instances can be connected over TCP/IP



Prover iLock **Verifier**

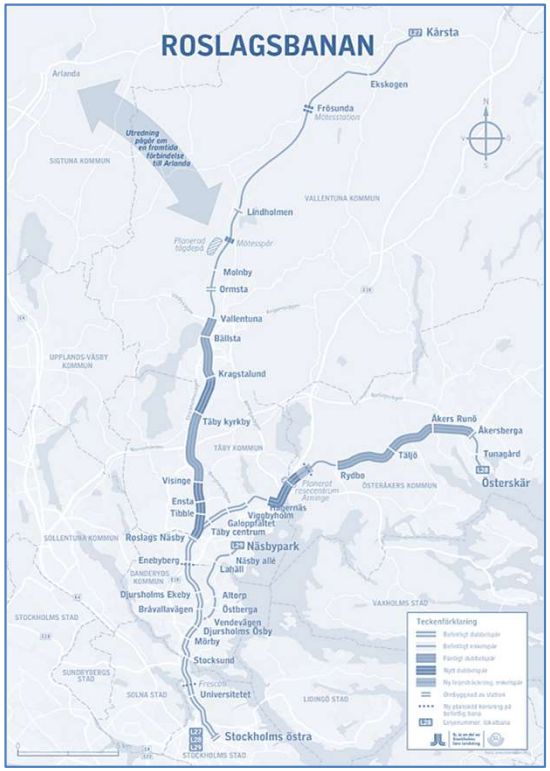
- Generic Safety requirements defined in PiSPEC
  - Specific requirements are automatically created from the application configuration
- Fully automated verification
  - 100 % coverage, with mathematical methods
- Built-in debugger
  - To analyze failing requirements
  - Examine states and variables, annotated in the track layout
- Generate Verification Reports



Prover References

SL, Stockholm Metro: Roslagsbanan

- Roslagsbanan is a mainline rail with an interlocking system from Hitachi
  - Software generated, tested and formally verified with the Prover Trident process
  - Prover developed formal specifications
  - Application engineering with Prover iLock by Hitachi
  - The high level of automation has been key to achieve project goals and schedules
  - The quality of the software resulting from the formal process as well as the automated testing and verification meant that the amount of on-site testing needed was significantly reduced
  - 20+ interlockings commissioned
- No software issues after installation thanks to
  - Clear requirement specifications
  - Formal Verification
  - Simulation-based testing
- The process also made it easier for SL to get exactly the functionality needed
  - Enables more complex functionality to be implemented in the interlocking system



SL, Stockholm Metro

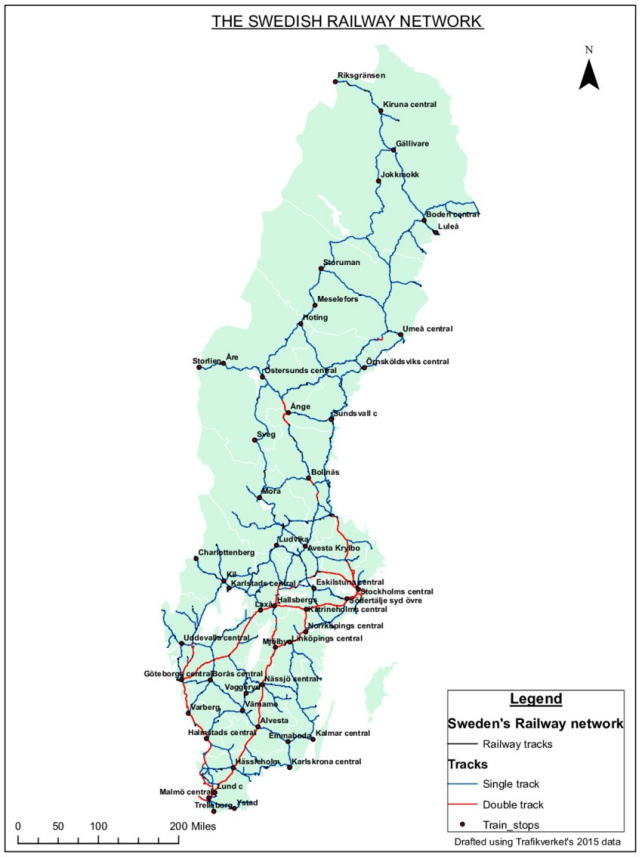
- Standardizing on formal methods for all signalling software
- Green Line: Prover has specified the safety principles of the existing system to facilitate a signaling modernization project with Siemens
  - Reduces risk in introducing new signaling technology, safety can be formally verified
- SL currently works with Prover to establish a digital twin, to prepare an upgrade of traffic management and signalling systems
  - Will help them understand and validate the requirements (current and future), and provide a way to do testing earlier in the process
  - This is also a first step towards introducing COTS components

Port Authority of New York and New Jersey

- PATH
  - System supplier: Siemens
  - CBTC: Siemens
  - Interlocking: Alstom iVPI
- Interlocking development
  - Generic Application (PiSPEC IP)
  - Design, code and V&V results created using Prover iLock
  - Some quite large and complex locations
  - Parts of FAT replaced with simulation and verification reports from Prover iLock

Trafikverket, ERTMS

- Prover supports the safety verification for the ERTMS pilot lines with
  - Formalization of requirements in the HLL language
  - Prover Certifier based tool chain
  - Verification services
- For the wide ERTMS roll-out, time consuming safety verification has been identified as a major risk
  - To be addressed with automation, structured data (LCF) and formal verification
- Shift2Rail, EU project to promote research & innovation
  - Prover is supporting Trafikverket with expert knowledge on Formal Methods



Paris Metro, RATP

- **RATP** OCTYS CBTC system
  - Pioneer within formal methods for rail control systems
  - Prover developed the CENELEC EN 50128 SIL-4 compliant formal verification solution **Prover Certifier** in collaboration with RATP, to allow them to replace traditional safety verification techniques in their safety cases
  - Savings both in the verification and development process, as well as more predictable schedules and fewer issues in commissioned systems
- **Prover** develops and maintains formal verification tools, licensed to RATP and suppliers
  - Prover Certifier, HLL Language, Translators

Line	System	Development Method	Formal Proof toolkit	Date of Operation	Usage
3	CBTC (Zone Controller)	Scade 5	Prover Certifier	2010	Safety Case
12	Computerized Interlocking	Thales PIPC/PMI	Prover Certifier	2010	Safety Case
8	Computerized Interlocking	Thales PIPC/PMI	Prover Certifier	2011	Safety Case
12	Computerized Interlocking	Thales PIPC/PMI	Prover Certifier	2012	Safety Case
4	Computerized Interlocking	Thales PIPC/PMI	Prover Certifier	2013	Safety Case
1	Computerized Interlocking	Thales PIPC/PMI	Prover Certifier	2013	Safety Case
5	CBTC (Carborne)	Scade 5	Prover Certifier	2013	Safety Assessment
13	CBTC	Scade 6	Prover Certifier	2013	Safety Assessment

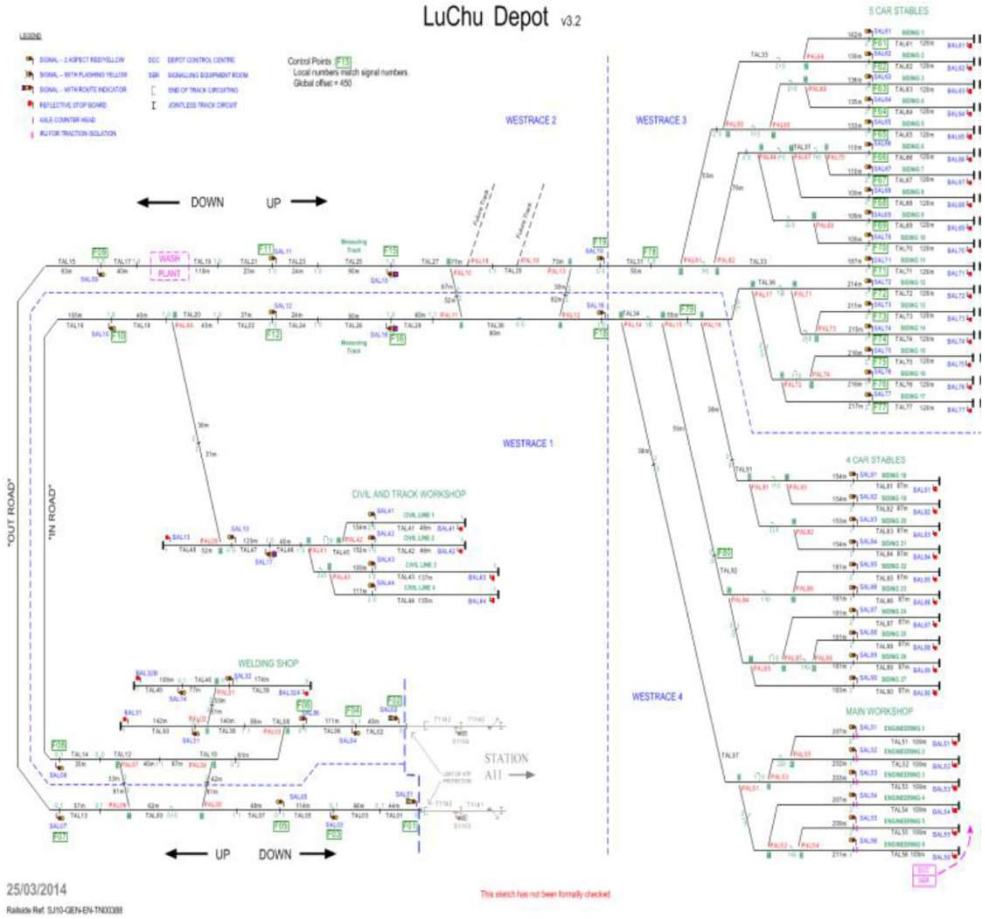
New York City Transit, NYCT

- **NYCT** has defined interoperability specifications (I2S) for CBTC
  - Three approved suppliers with full interoperability between wayside and on-board CBTC
  - Developed with formal methods, together with two suppliers
  - Formal methods and verification seen as the only cost-efficient way to ensure quality and safety
  - Formal Verification used to verify safety of interlocking systems

- **Prover**
  - Defined the Safety Specification for NYCT interlocking system, including CBTC (Zone Controller) interfaces
  - Formal verification with Prover iLock used by NYCT ISAs, for multiple interlocking vendors
  - Project with NYCT to extend I2S specifications for localization with ultra wideband (UWB), and apply formal verification to such systems

Taoyuan International Airport Access Verification

- Siemens used Prover iLock and Prover Certifier for formal safety verification of 11 Westrace interlockings on the Taoyuan International Airport Access Railway in Taiwan (2014-15)
- Turn-key project; Prover supplied tool chain, formalized Siemens' safety requirements, and performed the verification
- Prover iLock for configuration and debug verification
- Sign-off safety verification tool based on Prover Certifier, in compliance with CENELEC EN 50128:2011

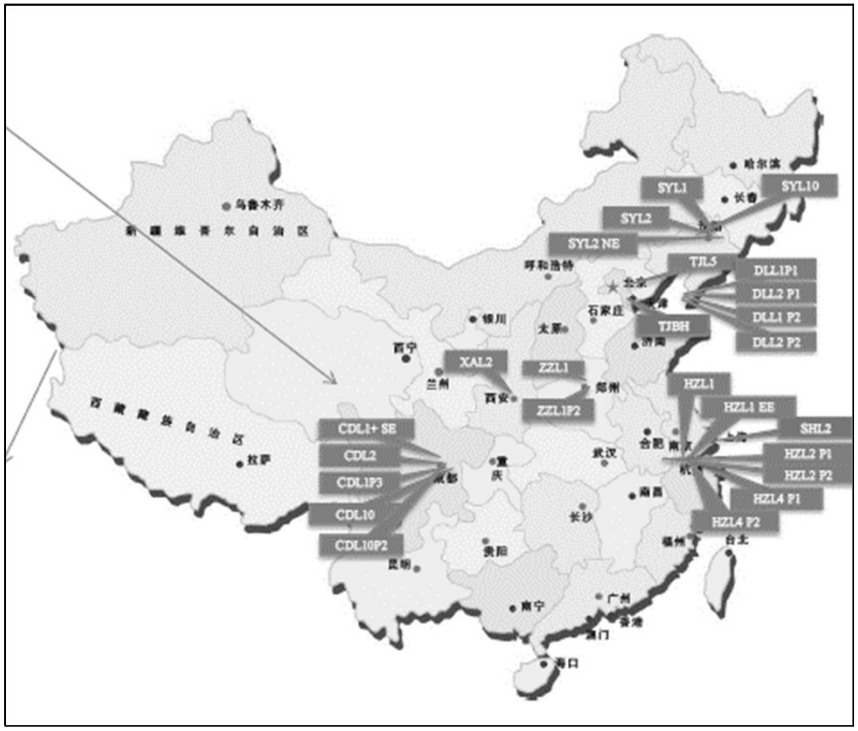


PROVER

Ansaldo STS
A Hitachi Group Company

Ansaldo STS CBTC

- Application Data Property Verification
  - Data Safety Properties for Carborne Controllers and Zone Controllers verified with Prover Certifier
- Zone Controller Software
  - Developed with SCADE
  - Safety properties verified with Prover Certfier, for both SCADE model and generated Ada code
  - Applied to 52 Zone Controllers globally
    - Ankara, Copenhagen, Paris, China, …
- Motivation: Find safety critical issues before commissioning, with minimal effort

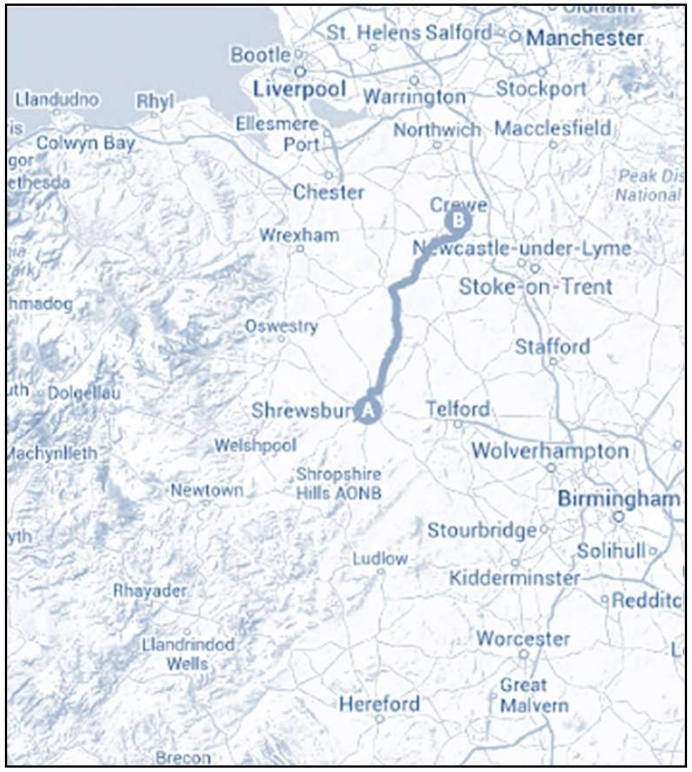


Canadian Pacific (CP)

- Class 1 Freight Railroad
  - Interlocking platforms by Alstom (GE) and Ansaldo STS, with coded track circuits (ElectroLogIXS, VHLC and Microlok II)
  - Large network in Canada and US
- Interlocking development
  - Off-the-shelf solution, code generation, simulation-based testing and formal safety verification
  - Generic Application for Class 1 railroads (PiSPEC IP)
  - Prover iLock used in-house, and by external consultants
  - Generate FAT/SAT test sheets

Network Rail's modular signaling

- Mainline railway
  - System supplier: Siemens
  - Interlocking: Westrace Mk II
  - 3 interlocking systems
- Prover Trident (formal verification currently)
  - Generic Application: PiSPEC IP
  - Generation: Prover iLock
  - Sign-off verification: Prover Certifier (source code and binary code)
- 2017
  - Update for Baseline 3 of Modular Handbook
  - 3 new interlocking systems (North Wales Coast)



Qinghai-Tibet Railway

PROVER TECHNOLOGY

May 27, 2009

To Whom It May Concern,

As part of a project for the Ministry of Railways of the People's Republic of China, GE Transportation Global Signaling (GETSGS) supplied 20+ SSIs for the Qinghai-Tibet Railway. Prover Technology joined the project in 2006. Prover formally specified the signaling rules governing test and safety principles for these systems, implemented on VHLC hardware. GETSGS used these rules (together with the Prover iLock software) to perform automated simulation and formal testing of the interlocking applications. Following the success of this project, GETSGS have proceeded to further our collaboration with Prover, and the VHLC programming tool ACE is now integrated with Prover iLock.

GETSGS believes the use of Prover iLock together with VHLC and ElectroLogIXS hardware is particularly appropriate for clients that are looking to either a) deploy state of the art safety verification, or b) reduce the recurring engineering costs for projects with many interlocking systems.

GE
Transportation
Global Signaling, LLC

Derald J. Herinckx
Wayside Product Leader

Swedish Rail

Standardized on Prover's tools for formal verification of safety for the largest and most complex interlocking system type in Sweden (Stockholm area)

- Automated checking of relay schematics
- Generate formal verification model
- Formal verification of control table and signaling plan requirements

PROVER TECHNOLOGY

To whomever it may concern

Prover Technology has delivered a variety of software solutions and services to Banverket (Swedish National Rail) over the last ten years, including formal safety verification of a large number of interlocking systems using Prover iLock. Prover iLock has, among other things, been used to verify two of Scandinavia's largest and most complex interlocking systems - Stockholm Central and Karlberg stations. These systems are owned and operated by Swedish National Rail. The stations are implemented with a total of more than 10 000 free-wired vital relays. The relay logic was formally verified to comply with the customer's control tables and signaling diagrams, that expresses safety requirements, during both normal and fault mode operation.

We are pleased with the support and expertise demonstrated by Prover Technology team. Please feel free to contact me in case you have any questions.

Yours truly

/Staffan Wiklund/

Director
Swedish National Rail (Banverket)

TRAFIKVERKET

Jernbaneverket
(NORWEGIAN RAIL)

PROVER TECHNOLOGY

Jernbaneverket

Prover Technology delivers formal safety verification services for 17 new installations of ABB's computer-based Merkur interlocking system. The systems are part of the Nordlandsbanen line, the Ganddal freight terminal, and the double track Sandnes-Stavanger. Jernbaneverket (Norwegian National Rail Administration) owns, operates and maintains these systems. Previously, Prover Technology has verified the functional safety of many interlockings in Norway (including Sand/Roven, Gulsvik, Harran, Heggedal, Spikkestad, Namskogan, Majavatn, Svenningdal, Trofors, Vinstra and Rena). The functional safety has been verified using a formal method supported by Prover Technology's software tool Prover iLock Verifier.

The interlockings were implemented using a variety of relay-based and computerized solutions (ABB Merkur, NSB-87, NSB-94, and NSI-63). In all above projects Prover Technology delivers software safety verification reports, which play a central role in the Technical Safety Report as a part of the CENELEC Safety Cases for these interlocking systems. The safety verification of all interlocking systems in Norway is performed against generic formal specifications of the Norwegian safety requirements. Prover Technology has played a central role in the development of these specifications, which are maintained in cooperation with Jernbaneverket and ABB.

We are pleased with the support and expertise demonstrated by Prover Technology team. Please feel free to contact me in case you have any questions.

Yours truly

Terje Sivertsen
Head of signalling
Jernbaneverket