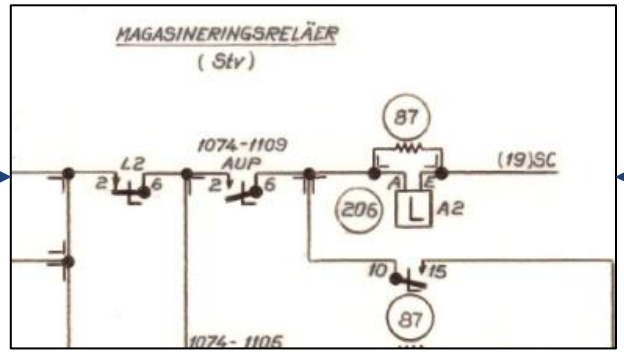
A Digital Twin for Rail Control and Traffic Management at Stockholm Metro

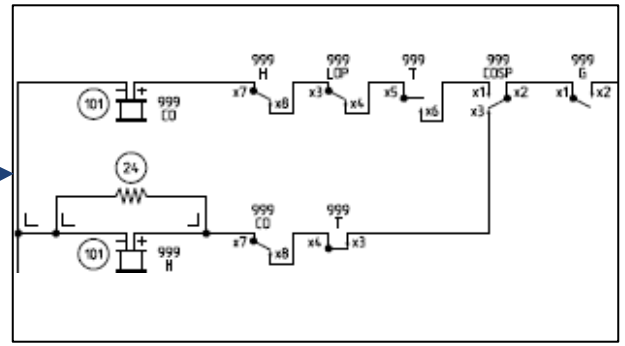
Gunnar Smith, 2023-01-24

Project background

- Procurement of a new Traffic Management System for the red and blue lines of Stockholm Metro
- Interfacing with existing signalling system
- Digital twin for validation and requirement specification for tender

Current Architecture





Physical maneuver panel

Operator interface. Push/pull buttons and switches for controls, lamps for indications

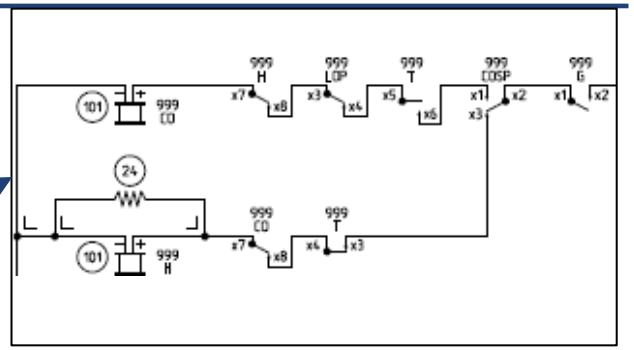
Non-vital relays

Interface between panel and interlocking, additional logic for automation

Vital interlocking relays

Safety critical signalling logic, locking of routes and points, signal aspects

Future Architecture



Computerized Traffic Management System

Operator interface

PLC

Same functionality as the current non-vital relays

Vital interlocking relays

Untouched

Digital Twin: Goals

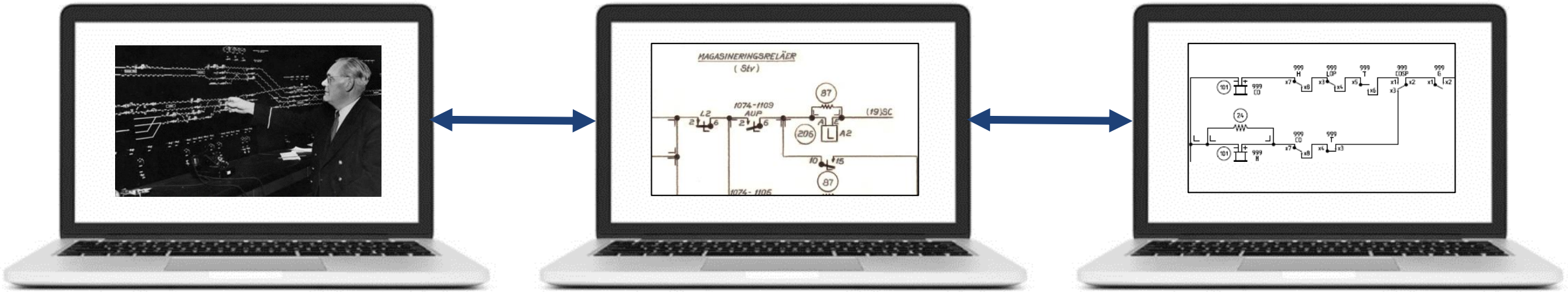
- Discover any unexpected dependencies
- Identify any safety critical functions that are dependent on the existing design
- Try out the concept
- Produce specifications for the tender
- Use it in the development of the new system

Digital Twin | The Process

Digital Twin: Process

- Developed with Formal Methods and Automation:
  1. Digital model of existing system
  2. Automatic generation of the PLC application software
  3. Digital model of the future system
  4. Replace the model of the PLC with an actual PLC
  5. Connect the model with the actual relay system (field testing)

Step 1: Digital model of existing system



Maneuver panel

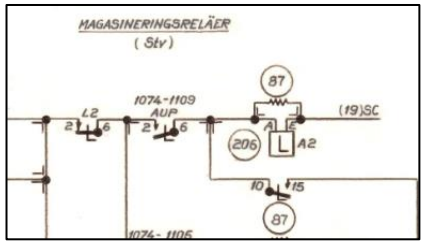
Non-vital relays

Vital interlocking relays

The three parts modelled in Prover iLock

Communication over TCP/IP

Step 2: Generation of PLC application software



Generate a PLC program from the model of the non-vital relays

Some functions are added to cater for the replacement of the maneuver panel

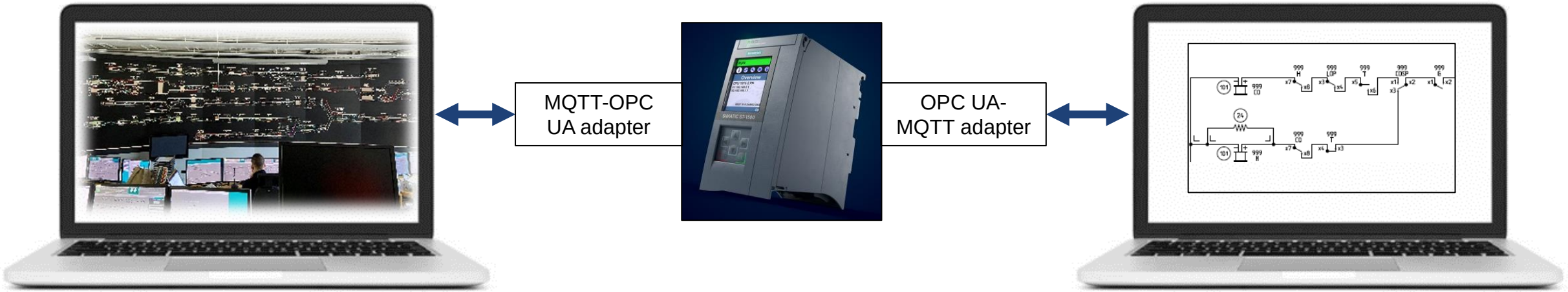
Formally verify the PLC-program

Step 3: Digital model of the future system

TMS PLC Vital interlocking

Include modeling of the PLC program execution

Step 4: Introduce an actual PLC



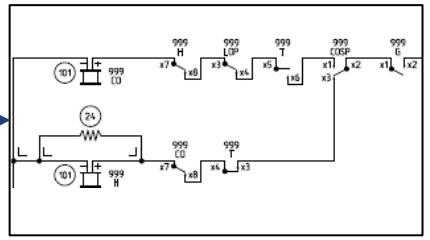
TMS PLC Vital interlocking

Load the generated PLC program on the PLC

Connect the PLC to the TMS and interlocking models

Step 5: Connect the model to the interlocking relays

MQTT-OPC
UA adapter



TMS PLC Vital interlocking relays

The PLC I/O is wired to the vital interlocking relays

Done onsite in the metro

Results

- The modularity of the proposed system has been validated
  - Interfaces defined and clearly specified
- Replacement of the non-vital relays with a PLC system validated
- New requirements identified
- Simplified transition to the physical environment
  - Field tests were done over one night
- Specification validated with formal verification and simulation
- In the future the models can be used for
  - Testing and verification of the new system during development
  - Testing together with physical components
  - Reproducing issues from field error reports/logs
  - Validation of design changes and new functionality
  - Training and documentation

PROVER

Thank You!

www.prover.com