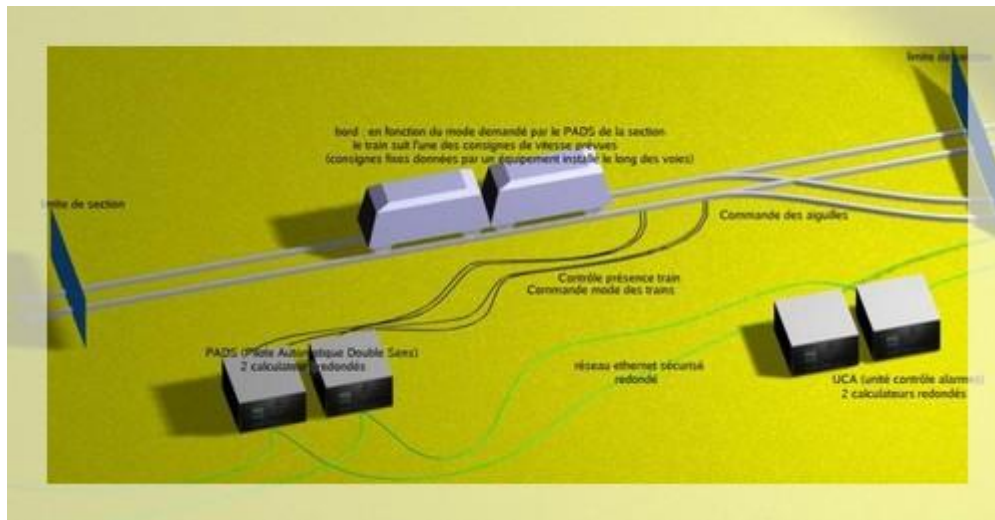


VAL DE ROISSY

ENTWICKLUNG DER SICHERHEITSSOFTWARE SIL4 FÜR FESTE AUTOMATEN DES ZUKÜNFTIGEN VAL DE ROISSY

Das vereinfachte System



Ausführung der Sicherheitssoftware mit Methode B

Siemens Transportation Systems (STS) gestaltet als Subunternehmer mit ClearSy die Ausführung B der Sicherheitssoftware für Automaten des zukünftigen VAL de ROISSY: Alarmsteuereinheit (UCA) und Sektionsautopiloten (PADS) auf Rechnung von Siemens. Diese Software vertritt letztlich etwa 150.000 ADA-Linien.

Diese Software entspricht SIL4 nach der Norm IEC61508: EN50126, EN50128, EN50129

Einige Zahlen...

Auf der VAL-Linie L1, die am 4. April 2007 eingeweiht wurde, wurden 2 Rechner installiert: UCA und PADS (so viele PADS wie nötig – S für Sektion).

Für die PADS-Software:

- 186.440 Linien für den Ada-Sicherheitscode der AS (Sicherheitsanwendung)
- 30.632 Linien für den nicht sicheren Ada-Code der AS
- Zahl der mathematischen Beweise: 62.056
- Zahl der B-Linien: 256.653 Linien



Für die UCA-Software:

- 50.085 Linien für den Ada-Sicherheitscode der AS (Sicherheitsanwendung)
- 11.662 Linien für den nicht sicheren Ada-Code der AS
- Zahl der mathematischen Beweise: 12.811
- Zahl der B-Linien: 65.722 Linien

Die effektive Zahl der B-Linien ist kleiner als die angegebene, da Kommentare berücksichtigt werden, darunter Kommentare, die zu Verfeinerungen führen.

Eine zweite Linie zum Flughafen Charles de Gaulle hätte im Juni 2007 eingeweiht werden sollen.

Veröffentlichungen und Erfahrungsberichte

- Einführungsdokument: Entwicklung der Sicherheitssoftware SIL4 von Val de Roissy: [herunterladen](#)
- Konferenz ZB2005: Artikel "Using B as a High Level Programming Language in an Industrial Project": [herunterladen](#)
- Konferenz ZB2005: Präsentation (Folien) "Using B as a High Level Programming Language in an Industrial Project": [herunterladen](#)
- Meteor: a Successful Application of B in a Large Project", FM'99, Toulouse, Frankreich, 1999 - Behm P., Benoît P., Faivre A., Meynadier J.-M. [SpringerLink.com](#)
- Vital software: Formal method and coded processor - ERTS 2006 - 25-27 January 2006 - Toulouse - Dollé D. [Artikel herunterladen](#)
- Formal Methods in Industry: Achievements, Problems, Future - JeanRaymond Abrial Swiss Federal Institute of Technology Zurich : [Portal.acm.org](#)
- MetroPole : [ein Artikel über Val de Roissy](#)