CLEARSY SYSTEMS ENGINEERING

FRANCE

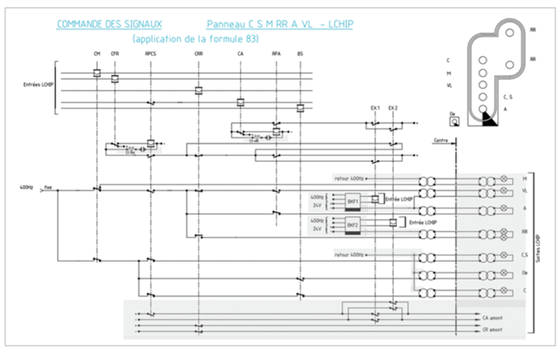
SNCF RÉSEAU

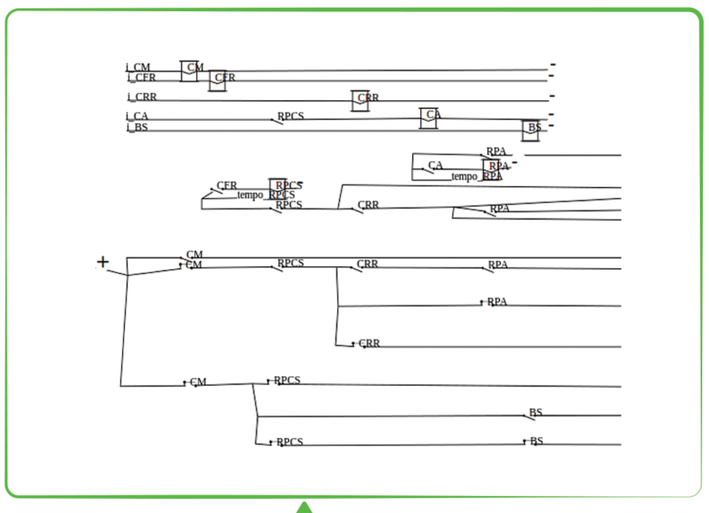
RELAY-BASED SCHEMAS ON A **SIL4 PROGRAMMABLE** CONTROL PLATFORM

SAFETY PROPERTIES

Énoncé
Il ne peut pas y avoir plus de 3 ampoules (hors oeilleton) d'allumées en même temps
Si l'ampoule 'C' est allumée alors l'oeilleton 'Oe' est éteint
Si l'ampoule 'C' est allumée alors l'ampoule 'C,S' est allumée ou l'oeilleton 'Oe' est éteint
Si l'ampoule 'M' est allumée alors l'oeilleton 'Oe' est éteint
Si l'ampoule 'VL' est allumée alors le relais 'RPA' est à l'état travail
Si l'ampoule 'VL' est allumée alors le relais 'RPCS' est à l'état travail
Si le relais 'CA' est à l'état repos alors le relais 'RPA' est à l'état repos
Si le relais 'RPCS' est à l'état repos alors le relais 'RPA' est à l'état repos

RELAY-BASED SCHEMA





i Formalize properties

Formalisation
card({M_bool, VL_bool, A_bool, RR_bool, RR_bool, CS_bool, C_bool} |> {TRUE}) <= 3
(C_bool = TRUE) => (Oe_bool = FALSE)
(C_bool = TRUE) => (CS_bool = TRUE or Oe_bool = FALSE)
(M_bool = TRUE) => (Oe_bool = FALSE)
(VL_bool = TRUE) => (RPA = STRUE)
(VL_bool = TRUE) => (RPCS = STRUE)
(CA = SFALSE) => (RPA = SFALSE)
(RPCS = SFALSE) => (RPA = SFALSE)

1 Import circuit diagram

2 Highlight wires

CLEARSY highlighter

On-the-fly automatic model extraction

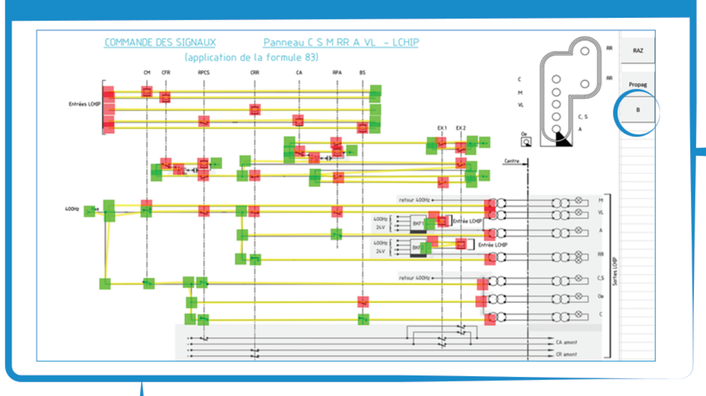


Diagram tracer

	A	B	C	D
1	Type	Left	Top	Objet
2	Entrée Plus	188,501	125,417	i_CM
3	Bobine monosta	257,593	125,417	CM
4	Alim Moins	663,884	123,915	
5	Entrée Plus	190,754	135,931	i_CFR
6	Bobine monosta	289,135	135,931	CFR
7	Alim Moins	661,631	135,931	
8	Entrée Plus	190,754	156,959	i_CRR
9	Bobine monosta	449,098	157,71	CRR
10	Alim Moins	663,133	157,71	

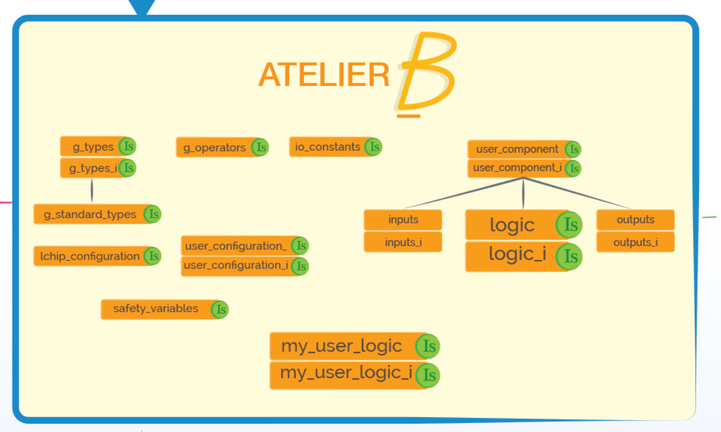
	B	C	D	E
Elements				
	2	3	4	
	5	6	7	
	8	9	10	
	11	12	13	14
	15	16	17	
	18	19		
	20	21	22	19
	23	24	25	19

	A	B	C
	Nom	Initial	Etat
	CM	Inactive	Inactive
	CFR	Inactive	Inactive
	CRR	Inactive	Inactive
	RPCS	Inactive	Inactive
	CA	Inactive	Inactive
	BS	Inactive	Inactive
	EX1	Inactive	Inactive
	EX2	Inactive	Inactive
	RPA	Inactive	Inactive

1 Visual
2 comparison

	B	C	D	E
Elements				
	2	3	4	
	5	6	7	
	8	9	10	
	11	12	13	14
	15	16	17	
	18	19		
	20	21	22	19
	23	24	25	19

3 Generate control software



Reverse translator

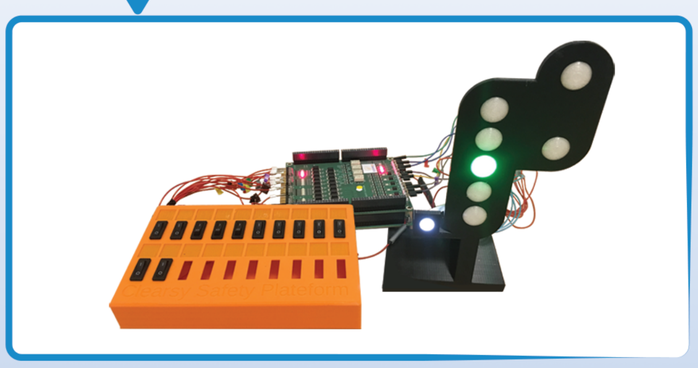
3 Automatic comparison

ii Verify properties

Pro B

Model Checking

4 Load control software



CLEARSY SAFETY PLATFORM

4
- Sil 4
- B method
- Double compilation
- Dual execution
- Automatic

David Déharbe | Clearsy
Paulin Fournier | Clearsy
Denis Sabatier | Clearsy

Damien Ledoux | SNCF

FORMAL VERIFICATION (Behaviour)

IMPLEMENTATION

VÉRIFICATION (Structure)

SIL4 CERTIFIED

TOOL

TO BE IMPLEMENTED