Control-in-the-loop Model Based Safety Analysis

Tuesday, 16th September 2014

Pierre-Yves Piriou

Jean-Marc Faure

Jean-Jacques Lesage

Control-in-the-loop Model Based Safety Analysis

- Background and objective
- Modeling switching mechanisms in critical systems with BDMP formalism
- Comparison study: qualitative MBSA with/without considering failures of the control system

Industrial Context

Connexion
Contrôle-commande numérique pour le nucléaire

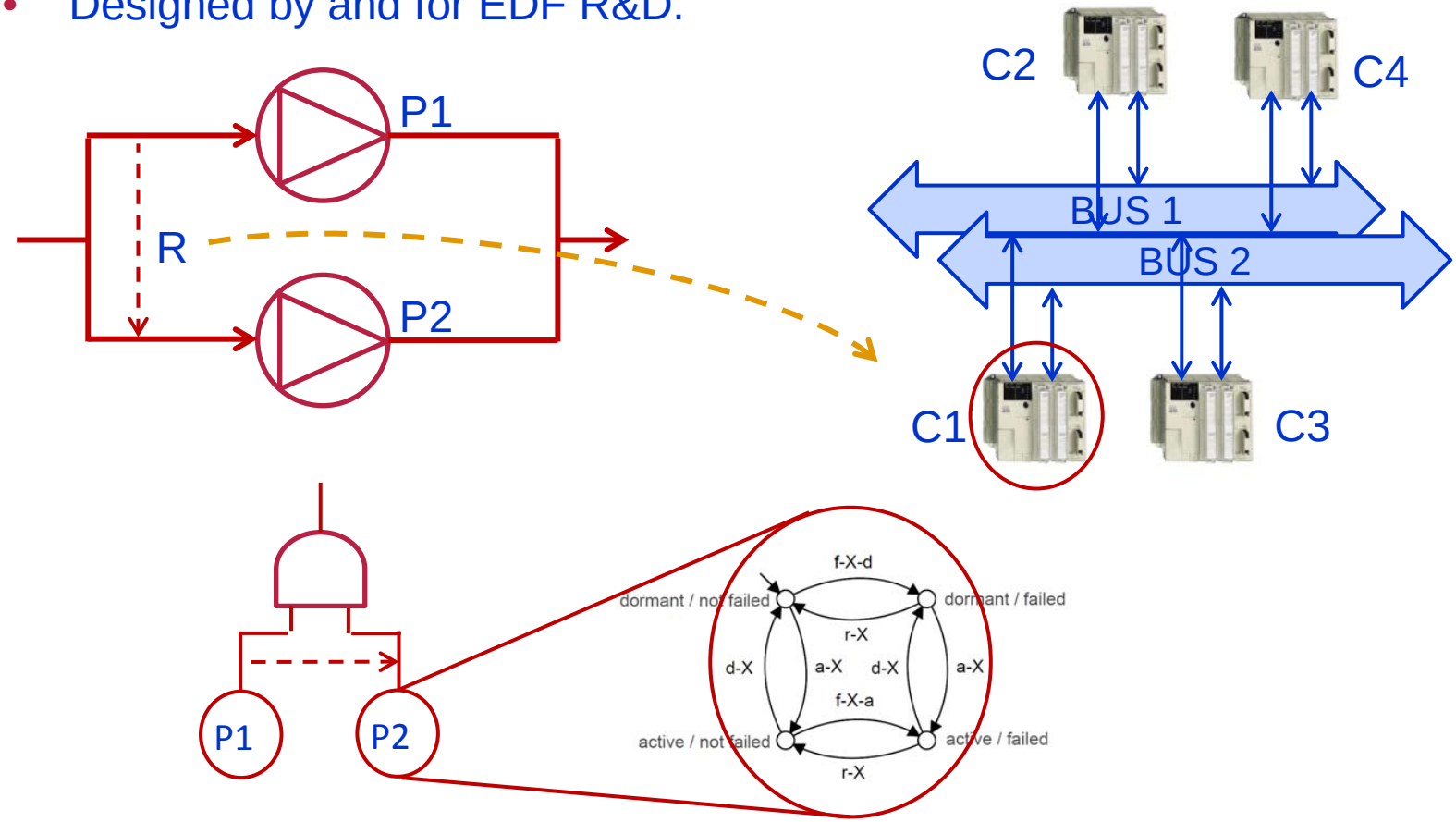
- **Project Connexion: control systems for nuclear power plant**

EDF AREVA ALSTOM
ESTEREL Technologies
ROLLS ROYCE Rolls-Royce
informatiques mathématiques
cea
energie atomique • energies alternatives
ALL4TEC ETUDES & CONSEIL

- **Safety assessment of closed loop systems.**
- **Technological constraints:**
  - Repairable components
  - Phased mission systems
  - Components can fail on demand

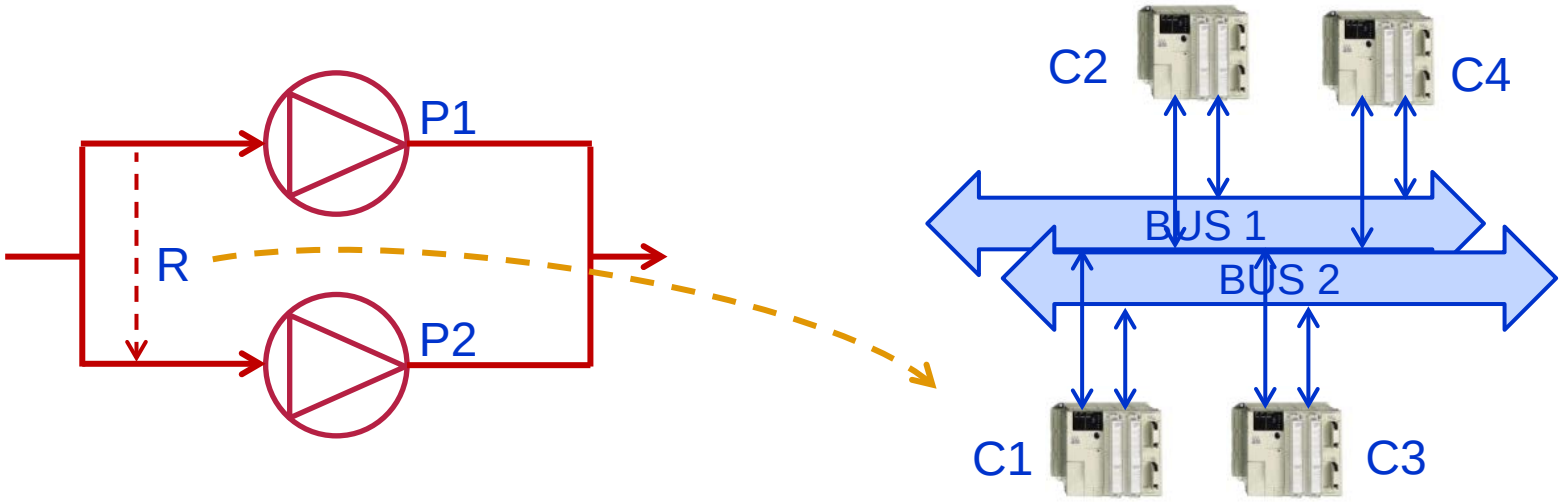
Modeling safety of critical systems

- **Boolean logic Driven Markov Process (BDMP) [Bou03]**
  - Unique formalism that natively deals with repairable components.
  - Designed by and for EDF R&D.



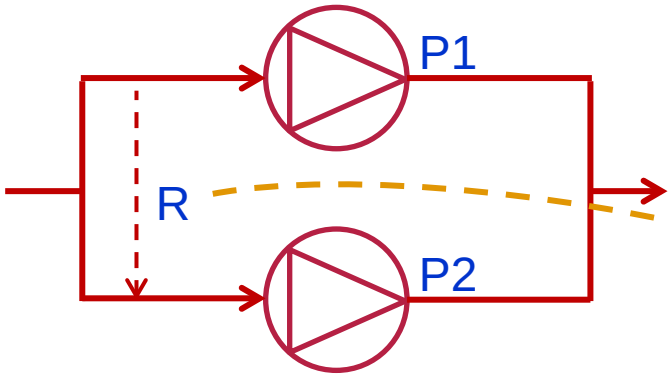
Main claim

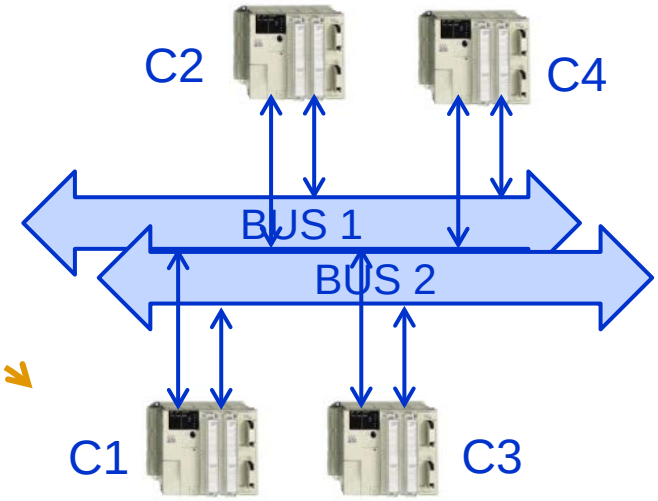
- **Control hardware failures must be considered in safety dynamic analysis.**
  - Digital components in critical systems are increasing.
  - External causes failures consideration…
  - Rq: only hardware failures are considered. Software failures can be avoided using formal verification methods.
- **Switching mechanisms are control-dependent.**

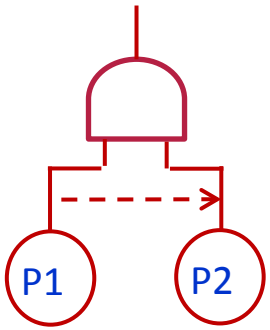


Modeling the loss of a trigger

- How to model the influence of control on switching achievement?

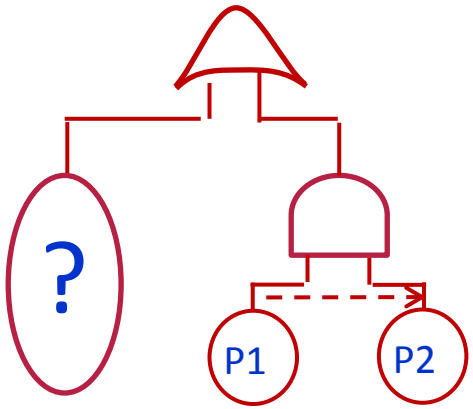




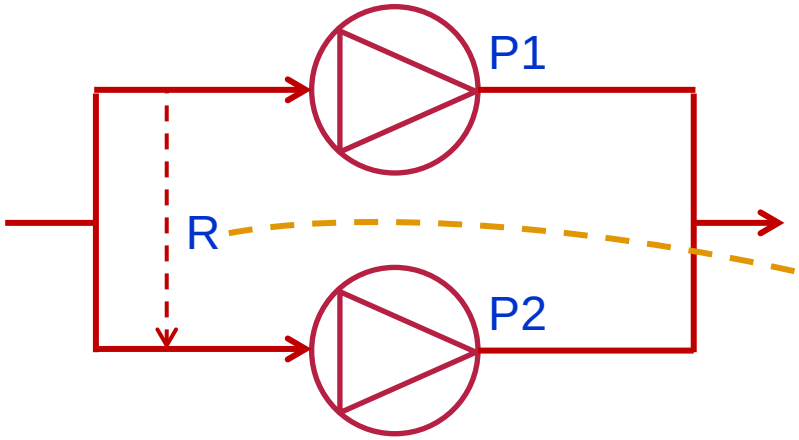


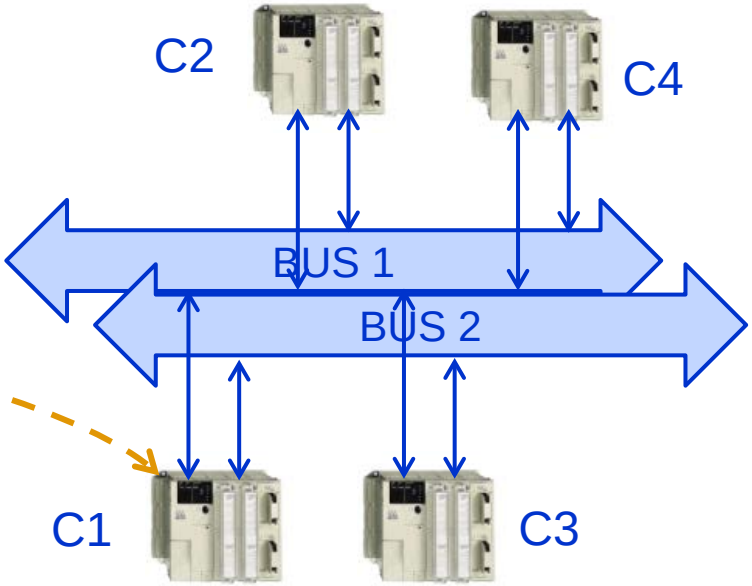
A trigger holds two switching mechanisms

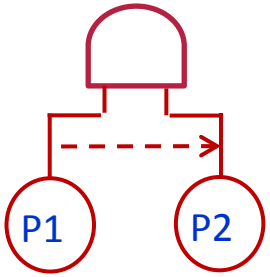
- Replacement
- Recovery

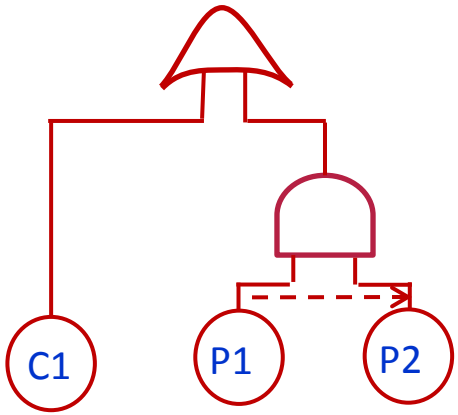


Integrating the loss of a switching function in a BDMP model

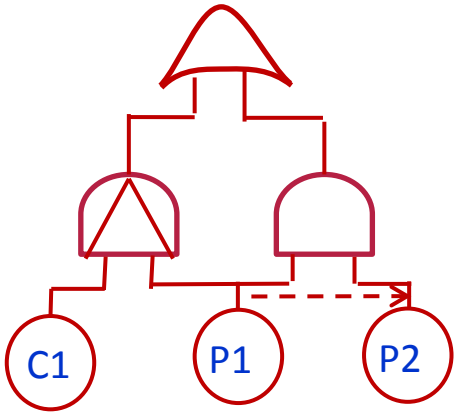






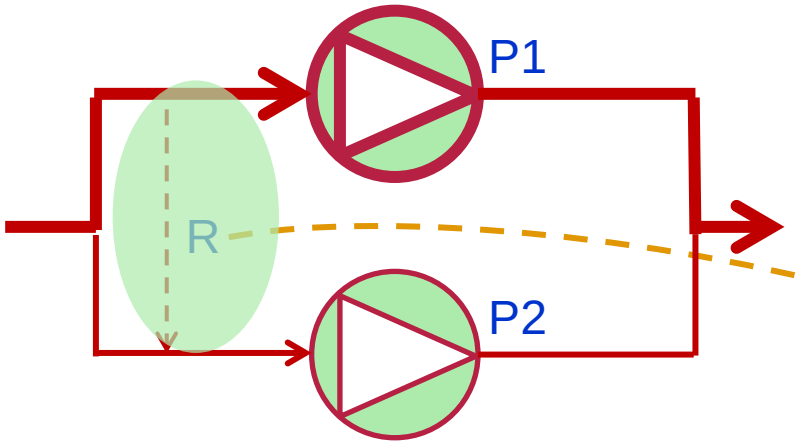


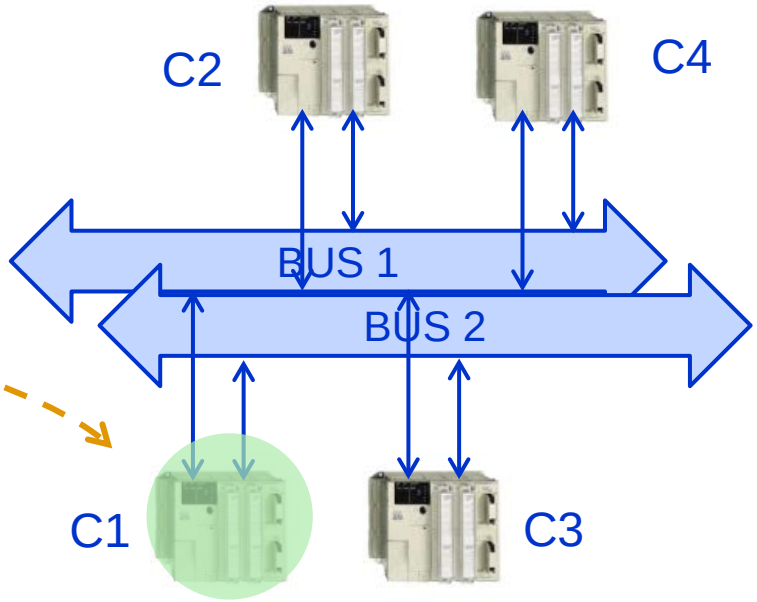
Model 1



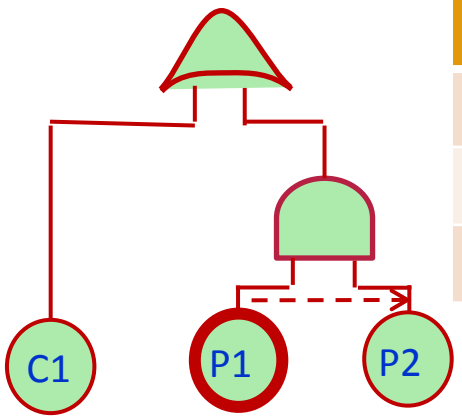
Model 2

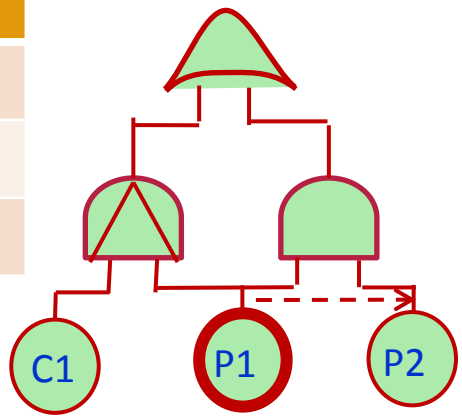
Initialisation



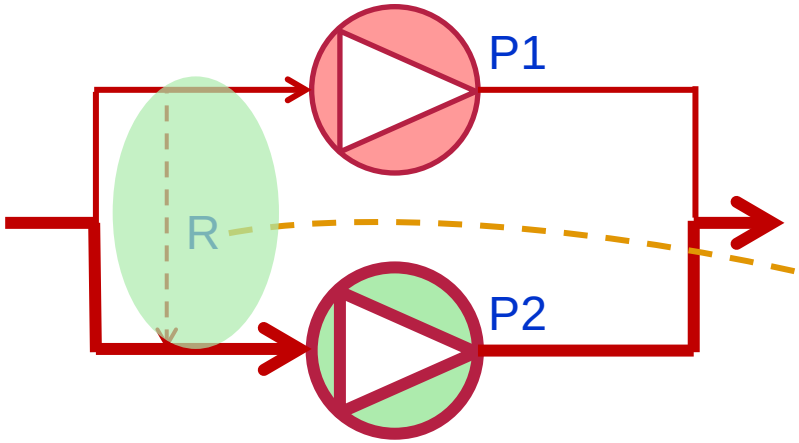


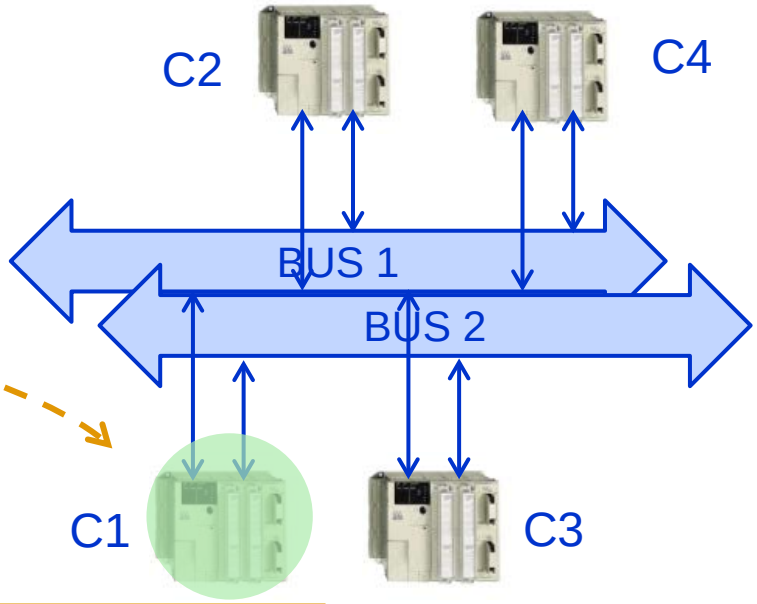
Sequence	$0 \xrightarrow{f-P1} 1 \xrightarrow{f-C1} 2 \xrightarrow{r-P1} 3 \xrightarrow{f-P2} 4$				
Expected	P1				
Model 1	P1				
Model 2	P1				

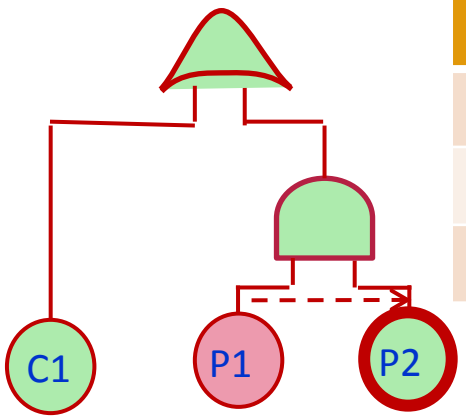




Sequence f-P1

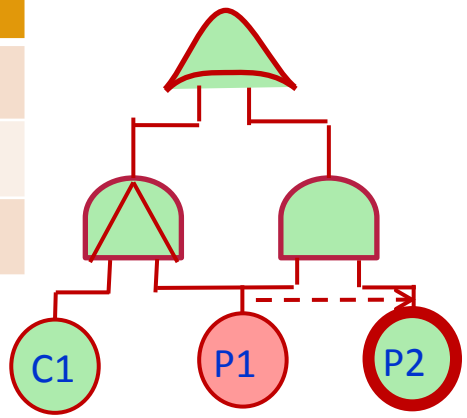




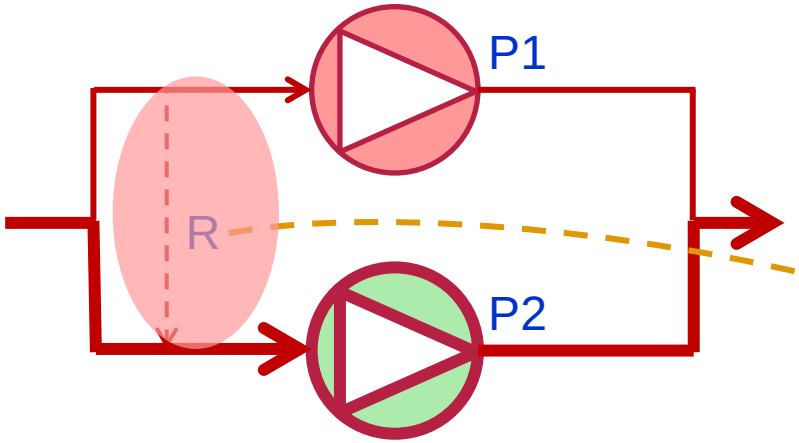


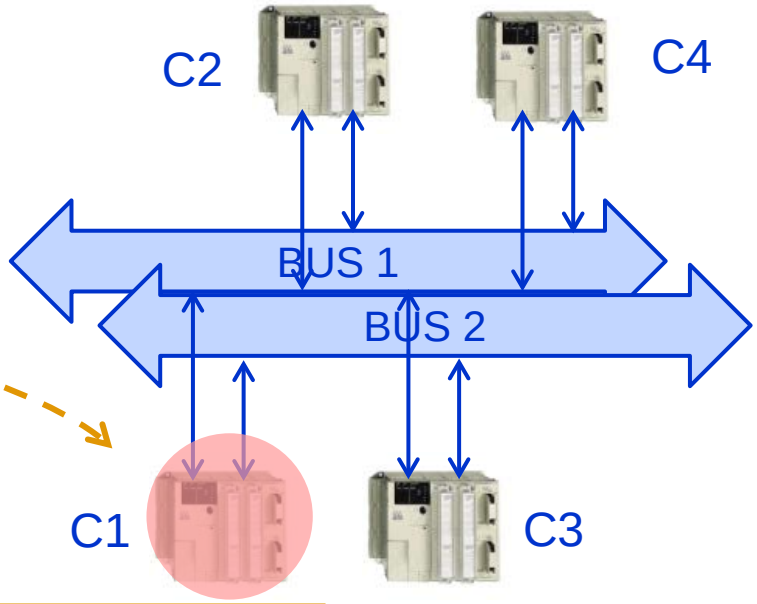
Sequence	$0 \xrightarrow{f-P1} 1 \xrightarrow{f-C1} 2 \xrightarrow{r-P1} 3 \xrightarrow{f-P2} 4$				
Expected	P1	P2			
Model 1	P1	P2			
Model 2	P1	P2			

Replacement switching

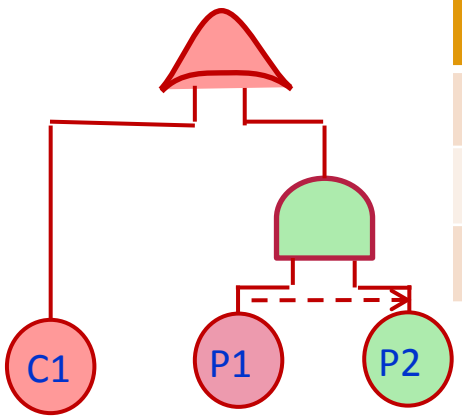


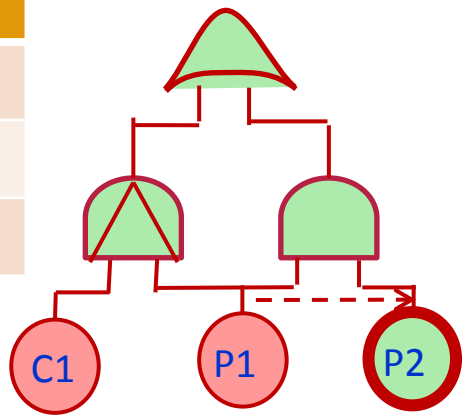
Sequence f-P1→f-C1



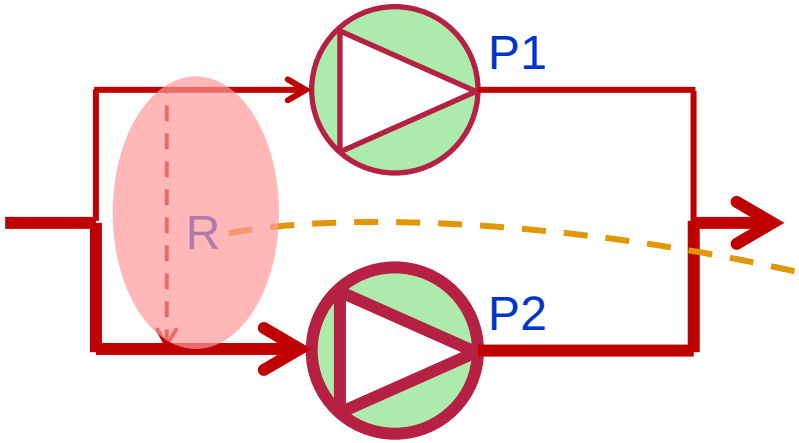


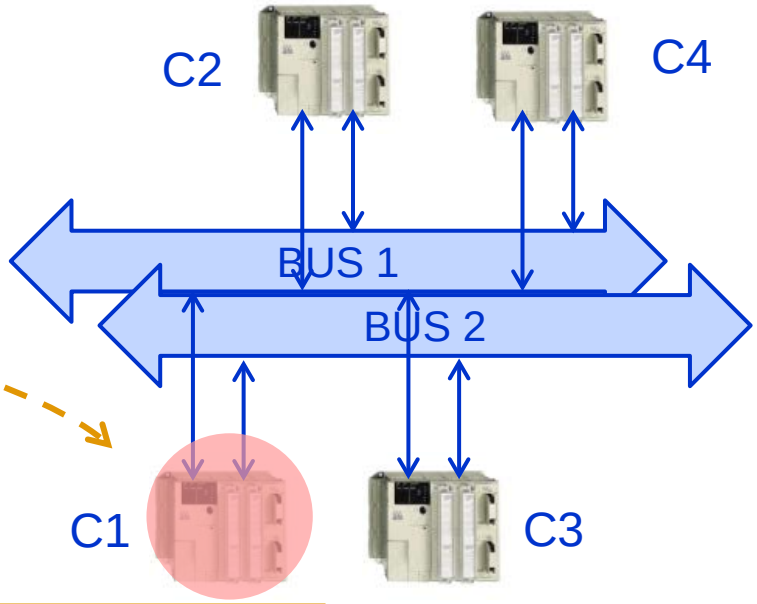
Sequence	$0 \xrightarrow{f-P1} 1 \xrightarrow{f-C1} 2 \xrightarrow{r-P1} 3 \xrightarrow{f-P2} 4$				
Expected	P1	P2	P2		
Model 1	P1	P2	Ø		
Model 2	P1	P2	P2		



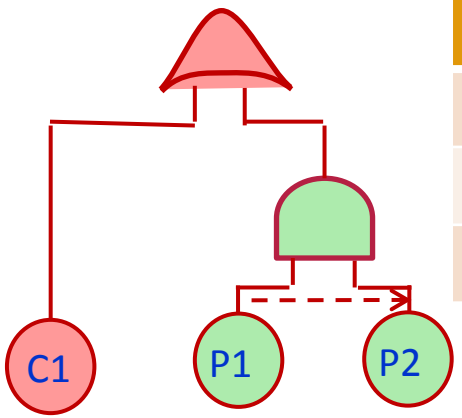


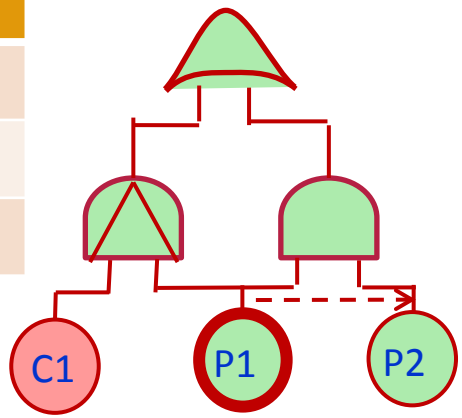
Sequence f-P1→f-C1 →r-P1





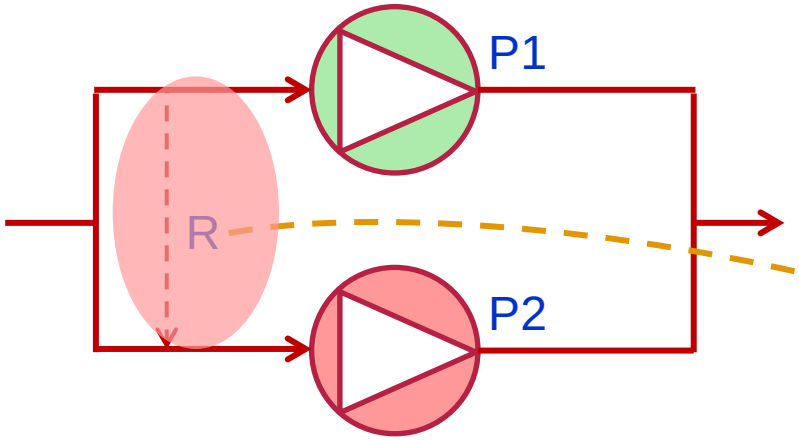
Sequence	$0 \xrightarrow{f-P1} 1 \xrightarrow{f-C1} 2 \xrightarrow{r-P1} 3 \xrightarrow{f-P2} 4$				
Expected	P1	P2	P2	P2	
Model 1	P1	P2	Ø	Ø	
Model 2	P1	P2	P2	P1	

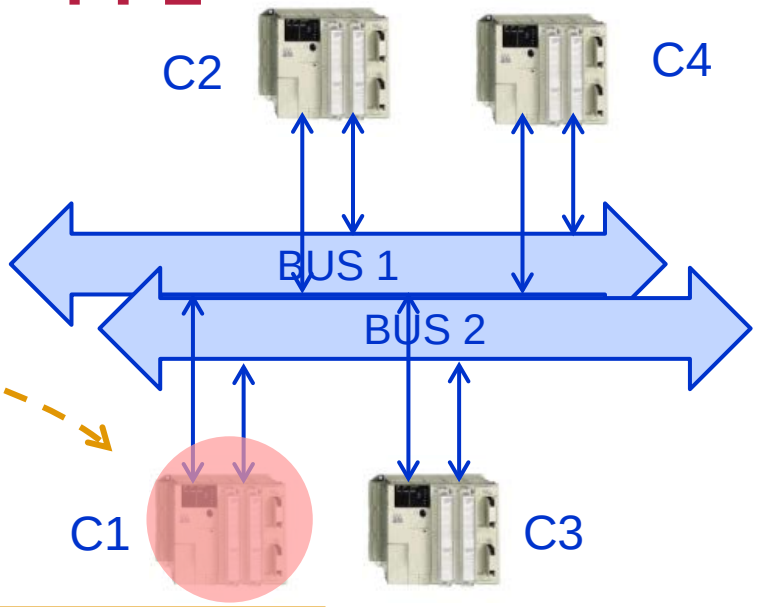




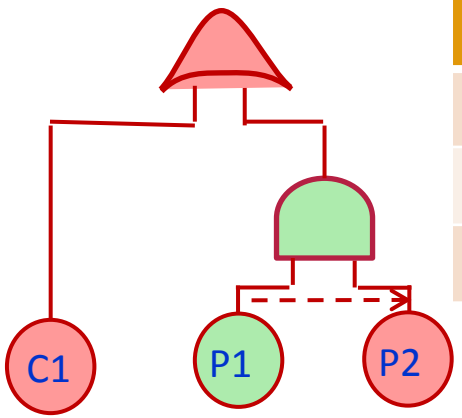
Recovery switching

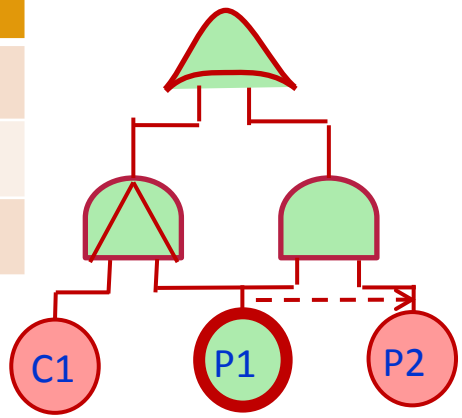
Sequence f-P1→f-C1 →r-P1 →f-P2





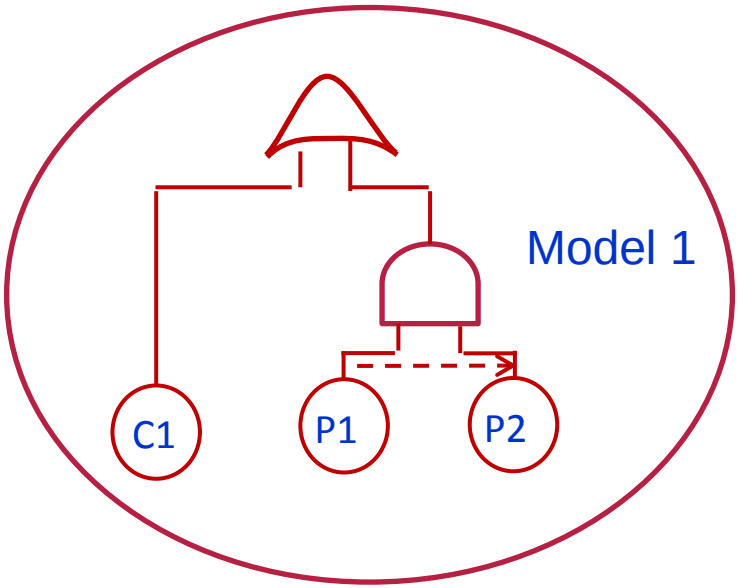
Sequence	$0 \xrightarrow{f-P1} 1 \xrightarrow{f-C1} 2 \xrightarrow{r-P1} 3 \xrightarrow{f-P2} 4$				
Expected	P1	P2	P2	P2	Ø
Model 1	P1	P2	Ø	Ø	Ø
Model 2	P1	P2	P2	P1	P1

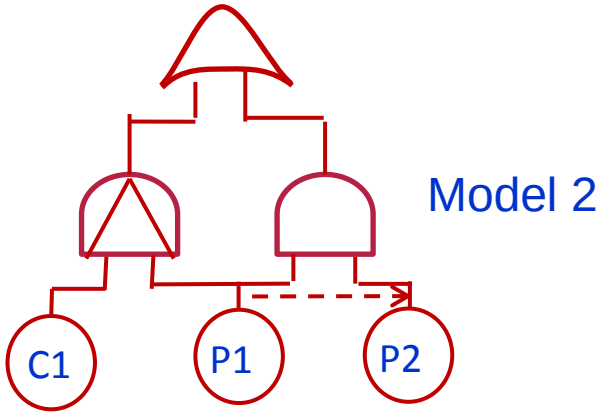




Decision

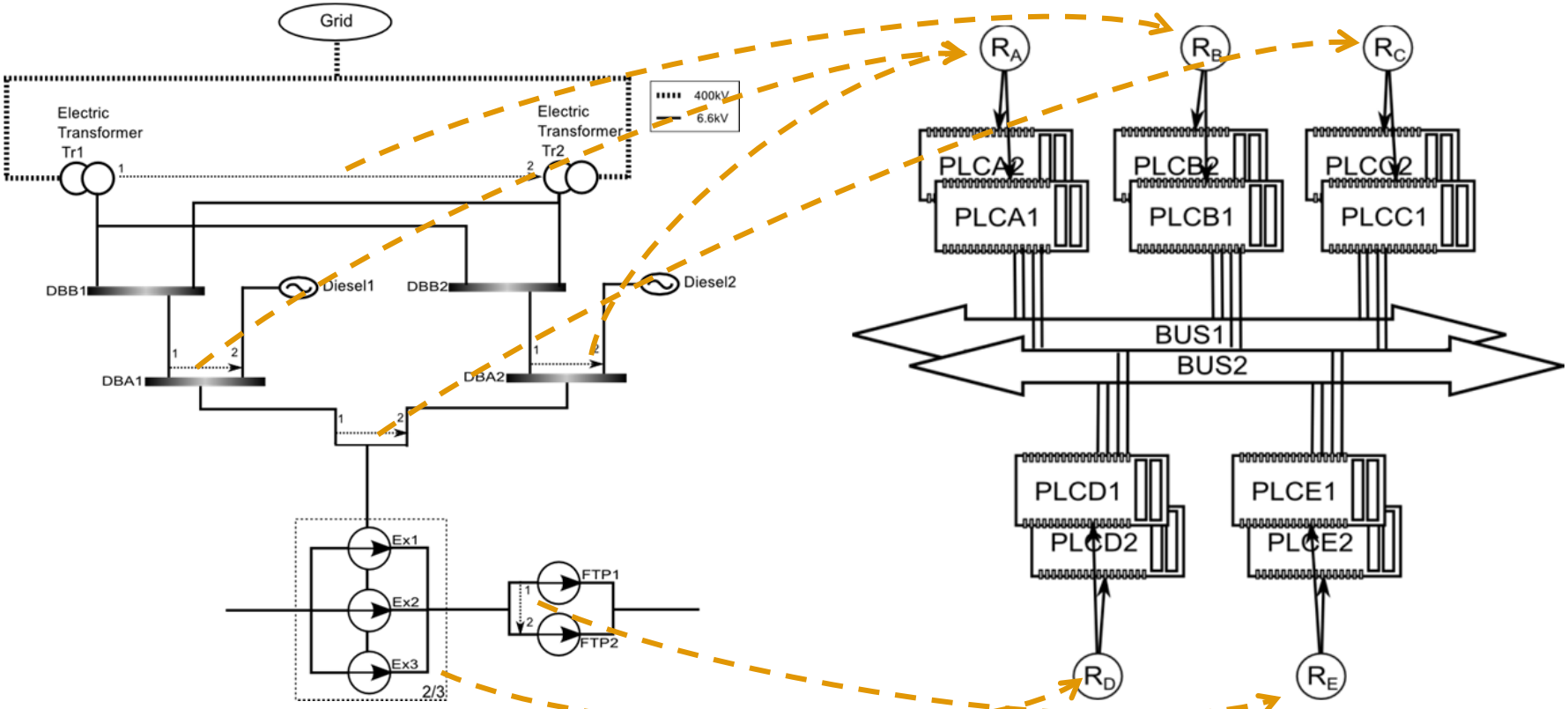
- **The loss of a switching function will be modeled by the first construction.**
- **The model 2 is not conservative**





A case study: the Coolant Feeding Water System

- **A power plant case study: steam generator input**
  - Plant: 2 groups of pumps + a power supply
  - Control: 5 pairs of redundant PLC + a pair of redundant BUS
- **Many standby redundancies**



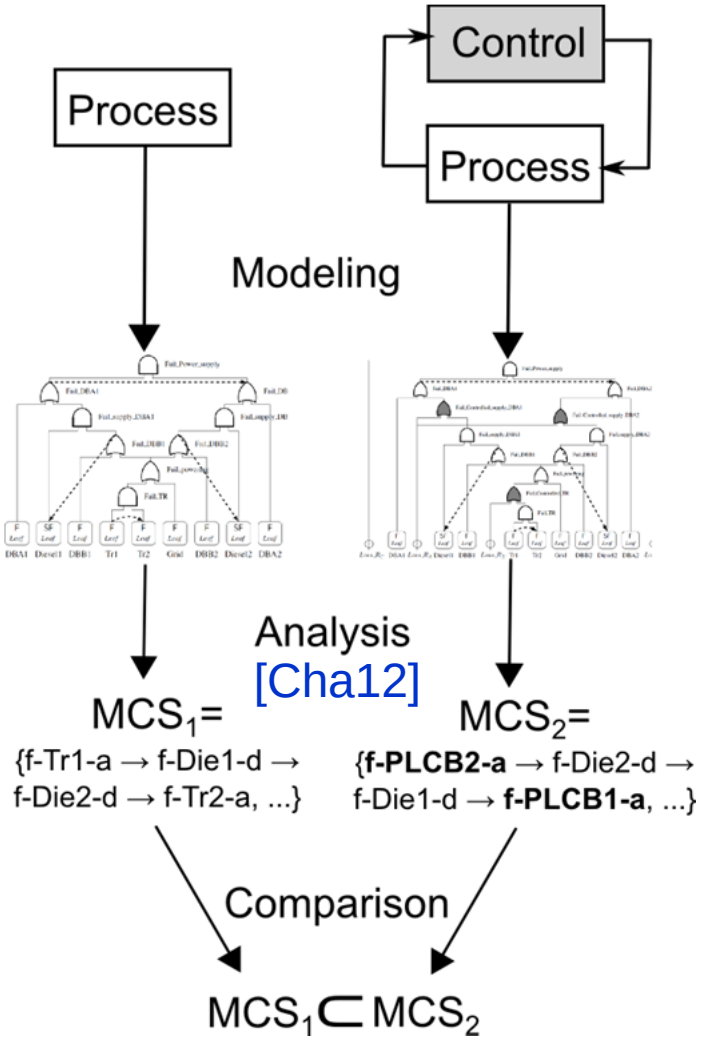
Comparing results

- **Conservative modification**
  - any minimal cut sequence for the process alone, is a minimal cut sequence for the closed loop system.

- **Control has a significant influence on system failure**
  - Include short sequences **(length 4)** that mix failures of both plant and control components.

f-PLCB2-a→f-Die2-d → f-PLCB1-a → f-DBA1-a

- **Then control hardware failures must be considered in safety dynamic analysis.**



Conclusion and outlooks

- Necessity to integrate failures of the control components in safety models has been shown.
- Limitations of BDMP for addressing this issue have been highlighted.

- Definition of an extension of BDMP to overcome these limitations.
- Formalization and systematization of the approach.

Thank you for your attention

Control-in-the-loop
Model Based Safety Analysis

Monday, 15th September 2014

Pierre-Yves Piriou

Jean-Marc Faure

Jean-Jacques Lesage

References

- [Bou03]: Bouissou, M. & Bon J.-L. 2003. A new formalism that combines advantages of fault trees and Markov models: Boolean logic driven Markov processes. *Reliability Engineering and Systems Safety* 82(2), pp. 149–163.
- [Cha11]: Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou, M. September 2011. Qualitative analysis of a BDMP by finite automaton. In *20th European Safety & Reliability Conference,* Troyes (France), pp. 2055–2057.
- [cha12]: Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou, M. June 2012. Systematic extraction of minimal cut sequences from a BDMP model. In *21th European Safety & Reliability Conference*, Helsinki (Finland). Session 16B, 8 pages.
- [Cha13]: Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G. & Bouissou M. September 2013. Towards a unified definition of minimal cut sequences. In *4th IFAC DCDS*, Volume 4, York (UK). 6 pages.