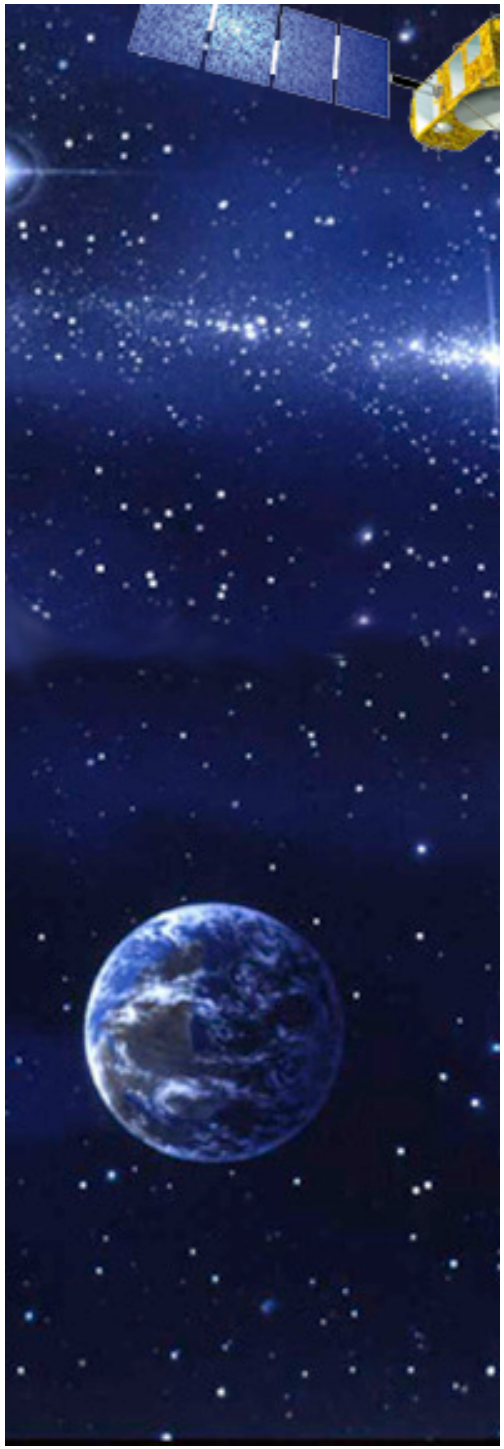
CAR'07 2nd National Workshop

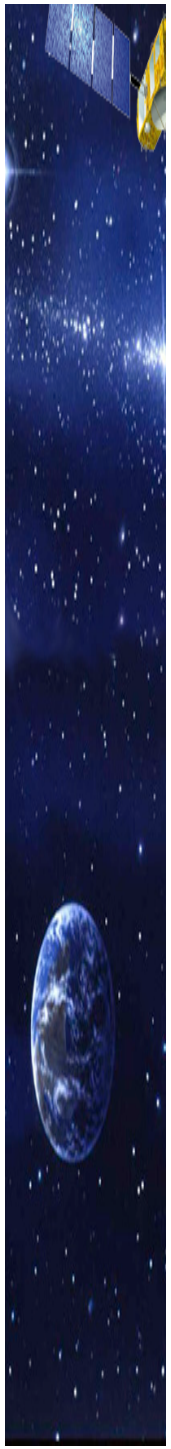
Z and ProCoSA based specification of a distributed FDIR in a satellite formation

Charles CASTEL, Jean-François GABARD, Catherine TESSIER / ONERA-DCSD
Jean-Charles CHAUDEMAR / SUPAERO

May 31, 2007



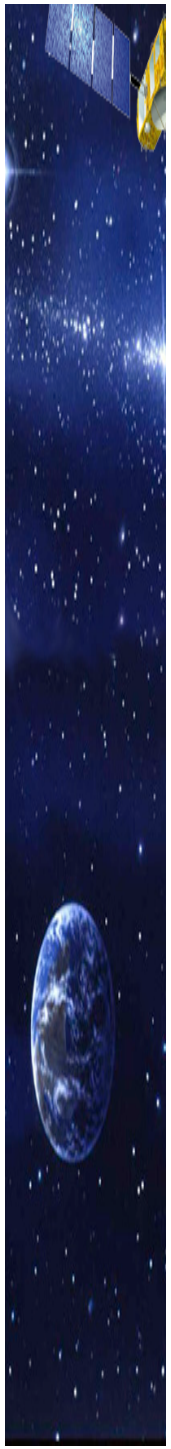
CONTENTS



Autonomy in space missions

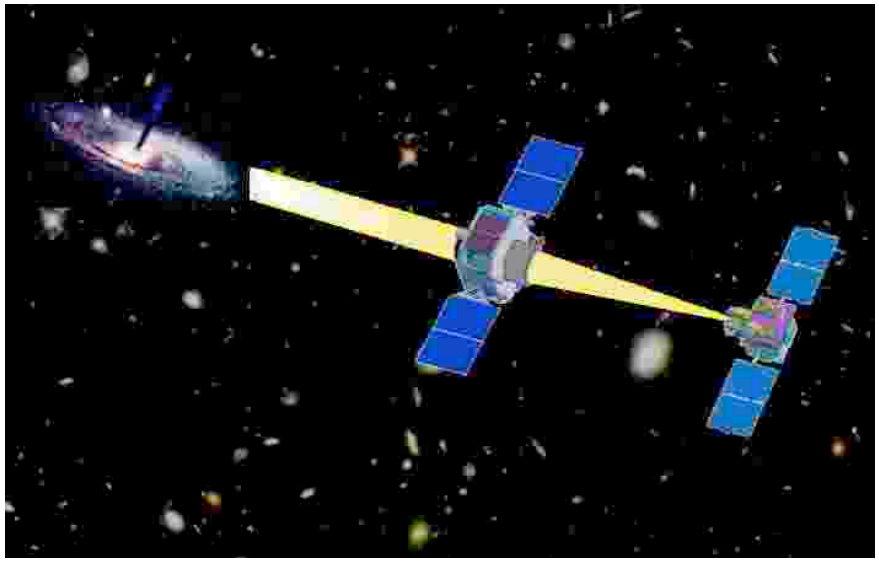
- Reduction of ground operations, reduction of service interruptions, improvement of reactivity of the system.
- On-board planning related to satellite command-control issues
- Organisation of reliable software components in a hierarchical closed loop architecture

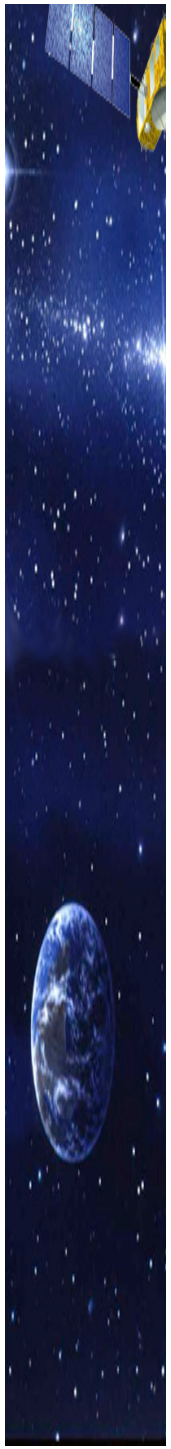
  {perception, situation assessment, decision, and action}
- Concurrent control of distributed components



Autonomous satellite formation

- Formation flying of satellites: a virtual large satellite
- Functions distributed among multiple satellite
- Very precise autonomous coordination and control of satellites: common scientific goal



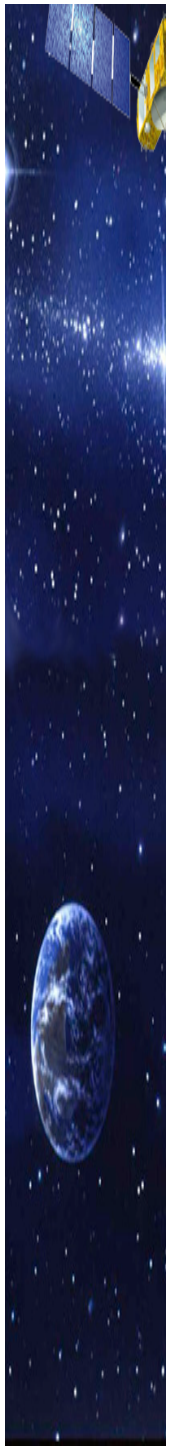


Anomalies in operational use

¬ Three classes :

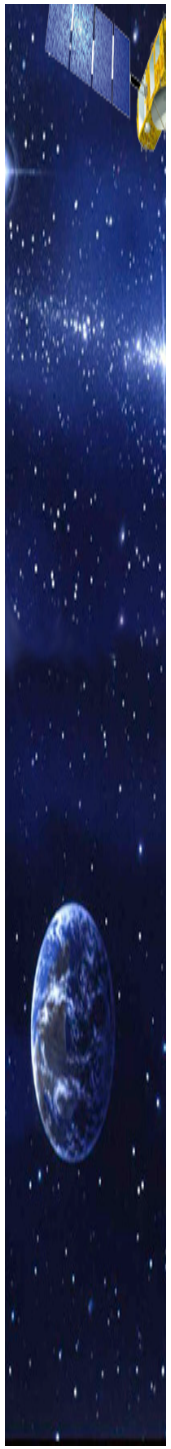
- formation geometry anomalies: Keep Out Zone (KOZ) violation, altered relative positions, altered orientations;
- degradation or loss of parts of instruments
- degradation or loss of communication within the formation, or between the formation and ground stations

◊ KOZ violation



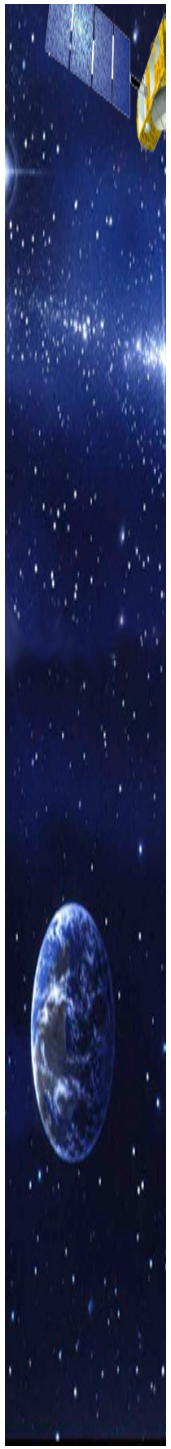
FDIR basic concepts

- FDIR : Fault Detection, Isolation and Recovery
- The formation = a decision agent for FDIR
- FDIR embedded in the global autonomy architecture: part of various autonomy functions
- FDIR strategy designing in accordance with the type of formation: master-slave formation, homogeneous formation, etc



Z-ProCoSA based specification

- Z specification: static aspects
- ProCoSA Petri nets: behavioural aspects
- Link: global formal specification
- Combining Z-Petri nets (Heiner, Heisel, 99) (Xudong, 01) (Peschanski, Julien, 03)



Z basic features

- Z formal specification notation based on set theory and first-order predicate logic

  to specify data-oriented aspects of a system

FORMATION

ACTEUR

$satellites : \mathbb{F}_1\ SATELLITE$

$distance : SATELLITE \times SATELLITE \pfun \mathbb{N}_1$

$dispose\_de\_fop : \mathbb{F}_1\ FONCTION\_OP$

$dispose\_de\_fdir : FDIR$

$status\_vkoz : ETAT\_V\_KOZ$

$\mathrm{dom}\ distance \subseteq satellites \times satellites$

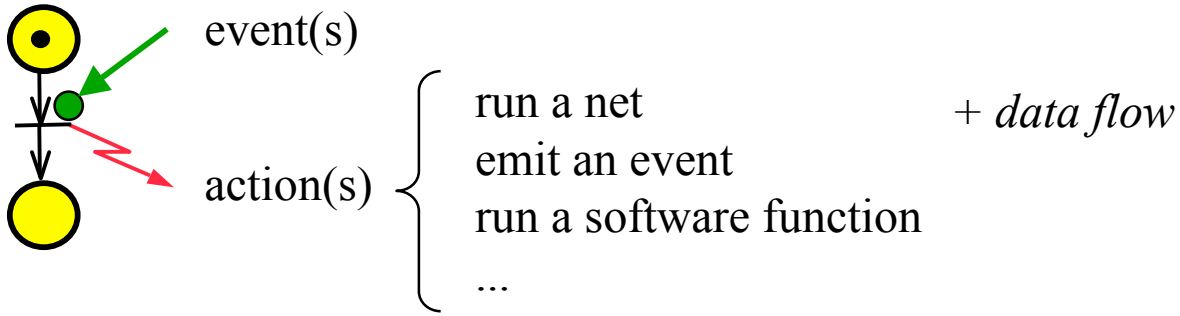
$status\_vkoz = normal \Leftrightarrow$

$(\forall\ sat1, sat2 : SATELLITE \mid (sat1, sat2) \in \mathrm{dom}\ distance$

$\bullet\ distance(sat1, sat2) > sat1.koz + sat2.koz)$

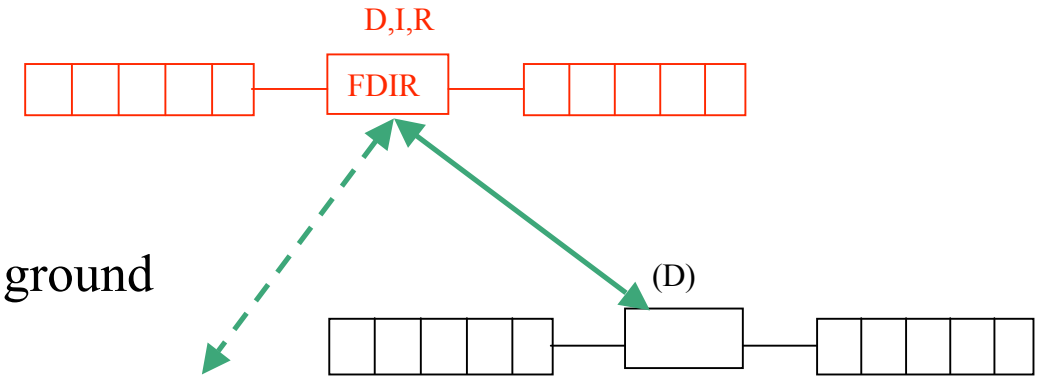
ProCoSA

- "Programmation et Contrôle de Systèmes à forte Autonomie" ® 1999
- Integrated package
  puts together and synchronises functions achieving system autonomy
  aims at developing an embedded decisional software architecture
- Interpreted nets

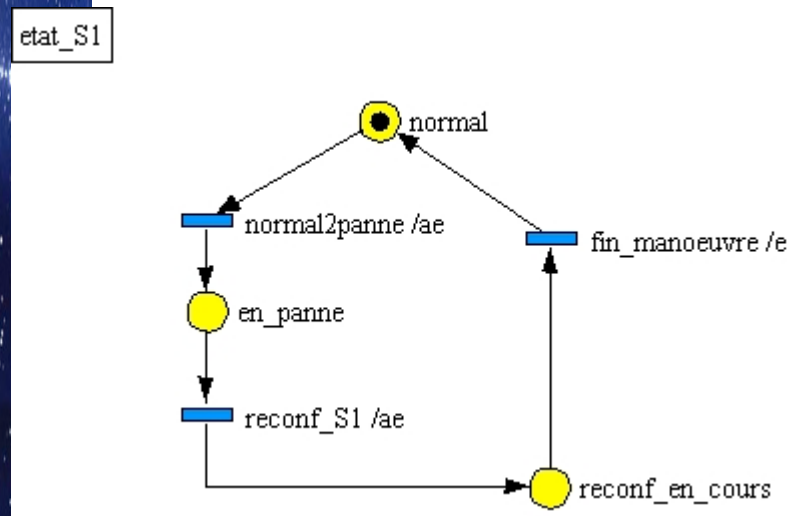


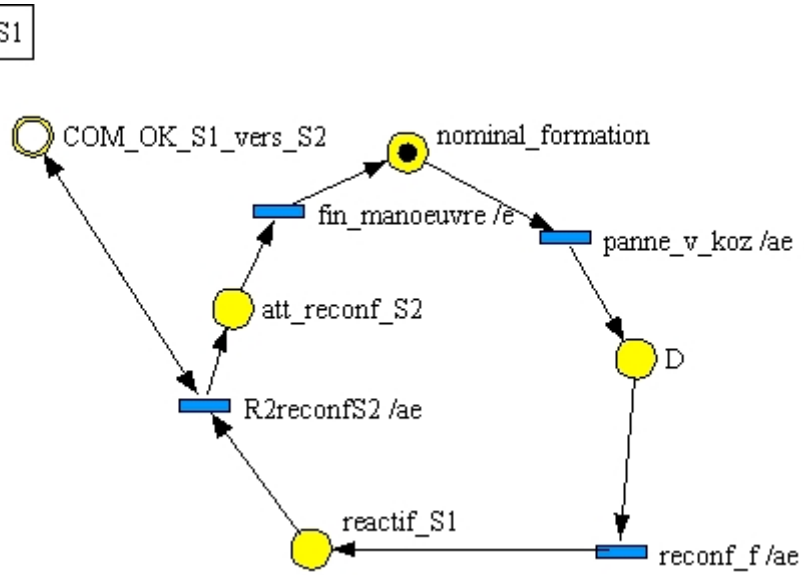
Example: FDIR centralised strategy

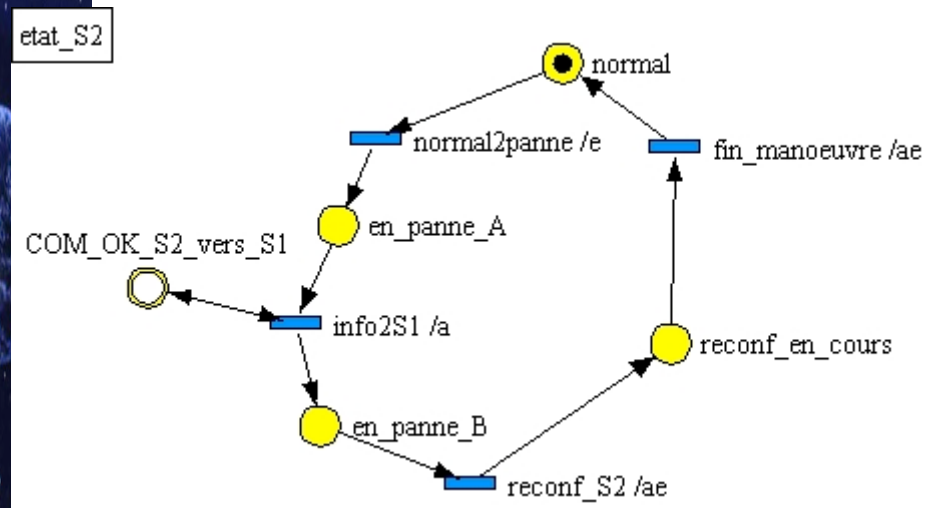
- One satellite performs FDIR for the whole formation
- S_{FDIR} communicates with ground stations



Simbol-X specification using Z and ProCoSA



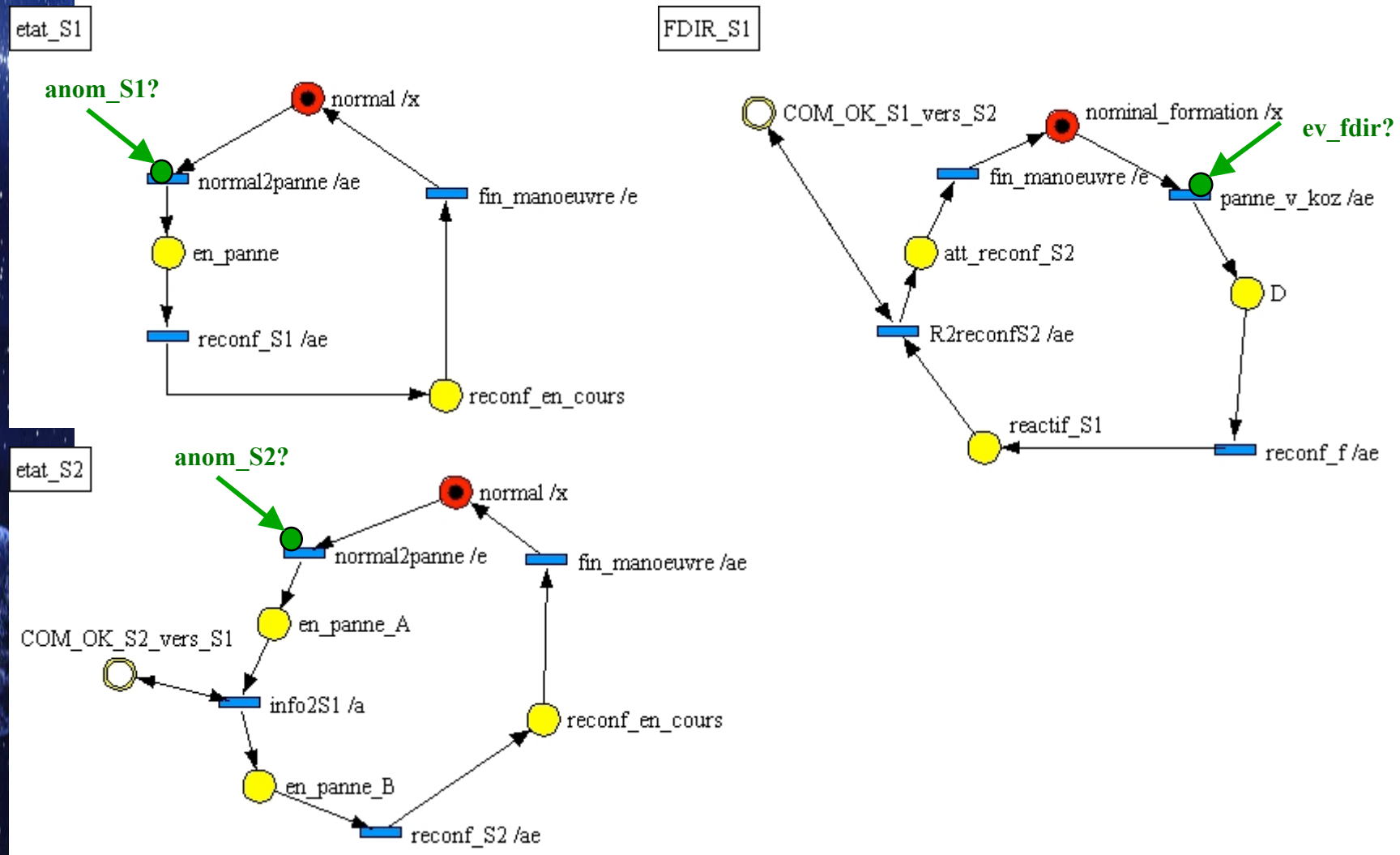




Init_FORMATION
FORMATION
$\Xi SIMBOLX$

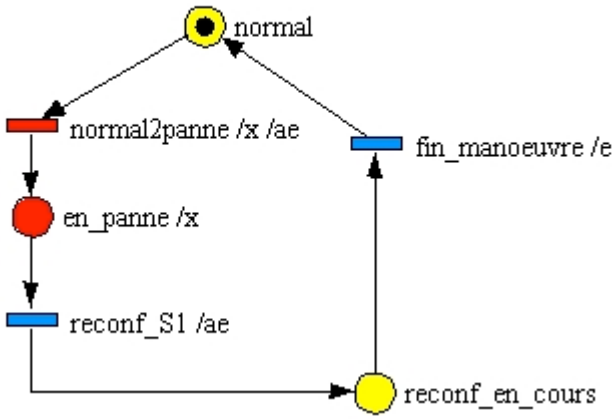
$status\_vkoz = normal$
$sat1.type = detecteur \land sat1.koz = 18$
$sat2.type = miroir \land sat2.koz = 15$

Simbol-X specification using Z and ProCoSA

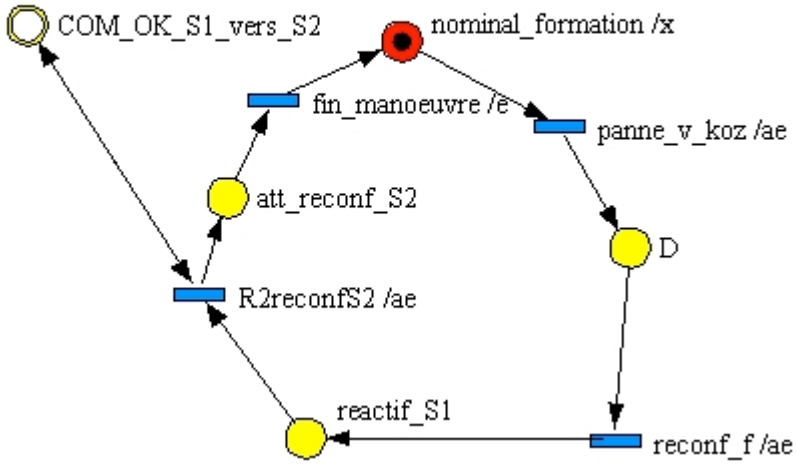


Simbol-X specification using Z and ProCoSA

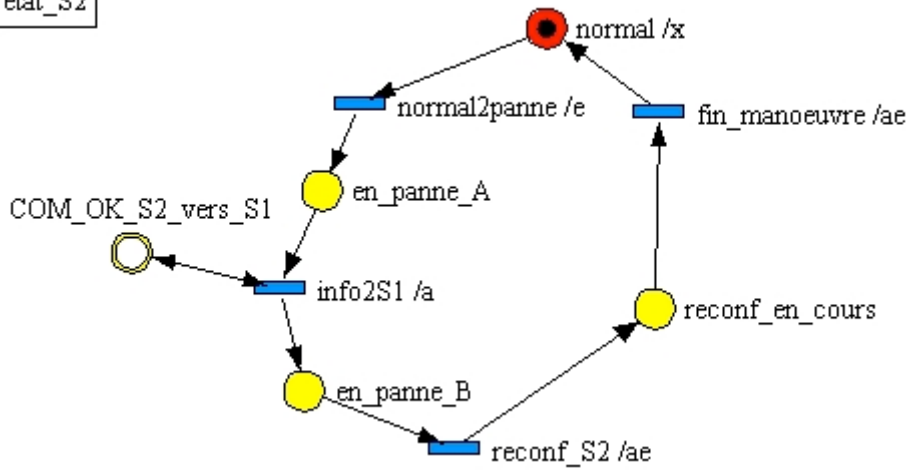
etat_S1



FDIR_S1



etat_S2



NORMAL2PANNE

$\Xi SIMBOLX$

$\Delta FDIR$

$anom\_S1? : DEFAUT$

$anom\_S2? : DEFAUT$

$anom\_S1? \in sat1.dispose\_de\_fdir.traite$

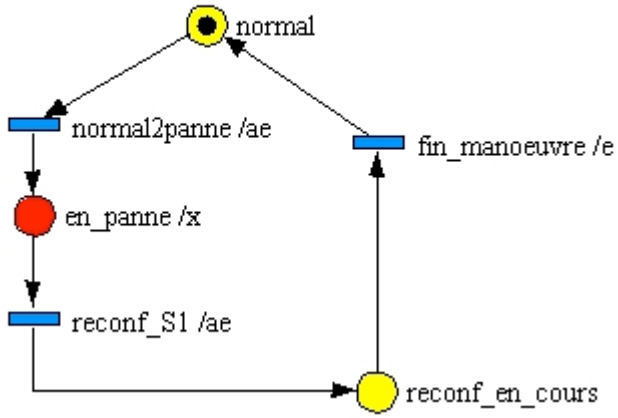
$anom\_S2? \in sat2.dispose\_de\_fdir.traite$

$sat1.dispose\_de\_fdir.detections \cap detections' \neq detections \cap sat1.dispose\_de\_fdir.detections$

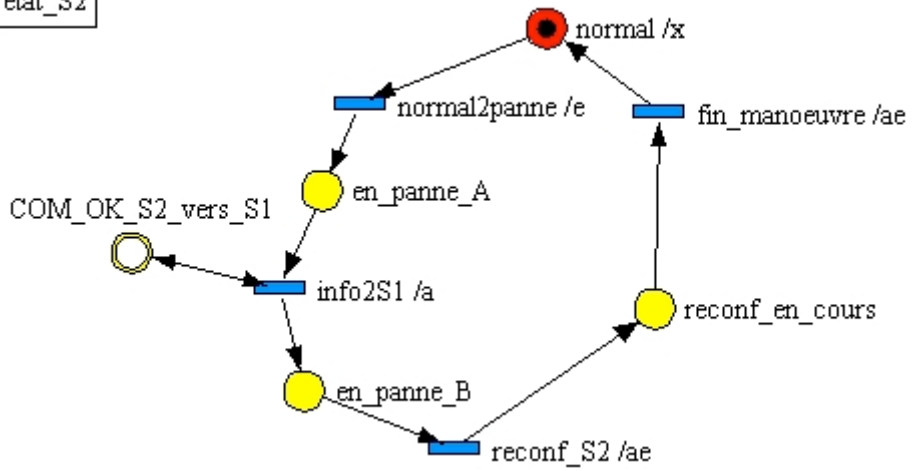
$sat2.dispose\_de\_fdir.detections \cap detections' \neq detections \cap sat2.dispose\_de\_fdir.detections$

Simbol-X specification using Z and ProCoSA

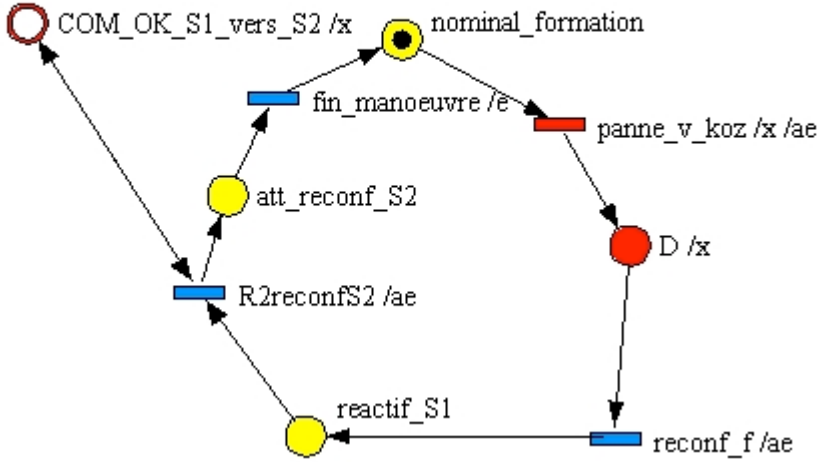
etat_S1



etat_S2



FDIR_S1



PANNE_V_KOZ

$\Xi SIMBOLX$

$\Delta FORMATION$

$ev\_fdir? : DEFAUT$

$ev\_fdir? \in formation.dispose\_de\_fdir.traite$

$status\_vkoz = normal$

$(sat1, sat2) \in \mathrm{dom}\, distance$

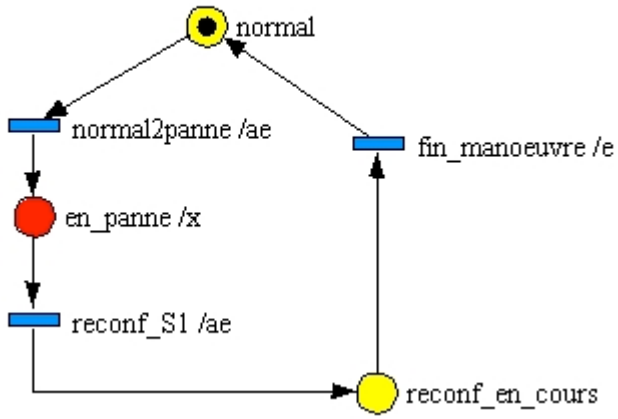
$distance(sat1, sat2) > sat1.koz + sat2.koz$

$status\_vkoz' = en\_panne$

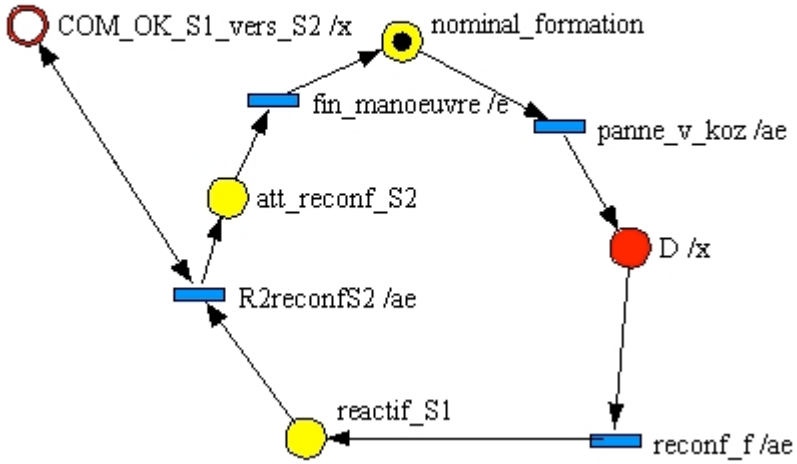
$distance'(sat1, sat2) \leq sat1.koz + sat2.koz$

Simbol-X specification using Z and ProCoSA

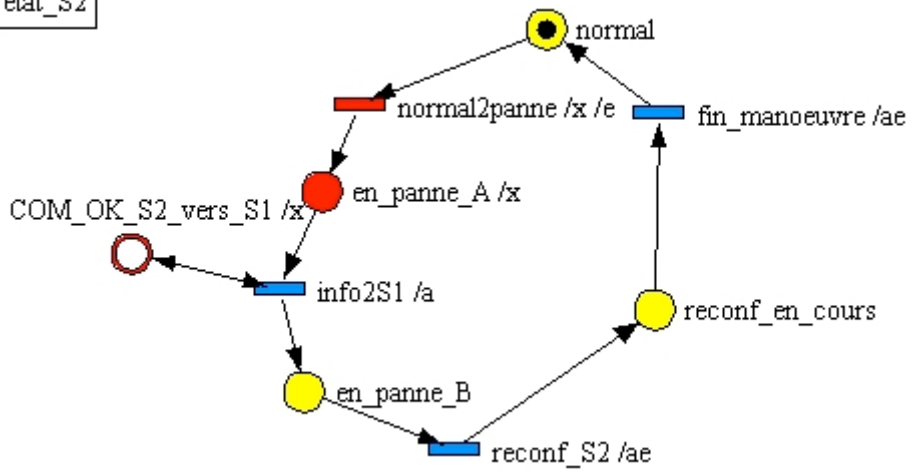
etat_S1



FDIR_S1



etat_S2



NORMAL2PANNE

$\Xi SIMBOLX$

$\Delta FDIR$

$anom\_S1? : DEFAUT$

$anom\_S2? : DEFAUT$

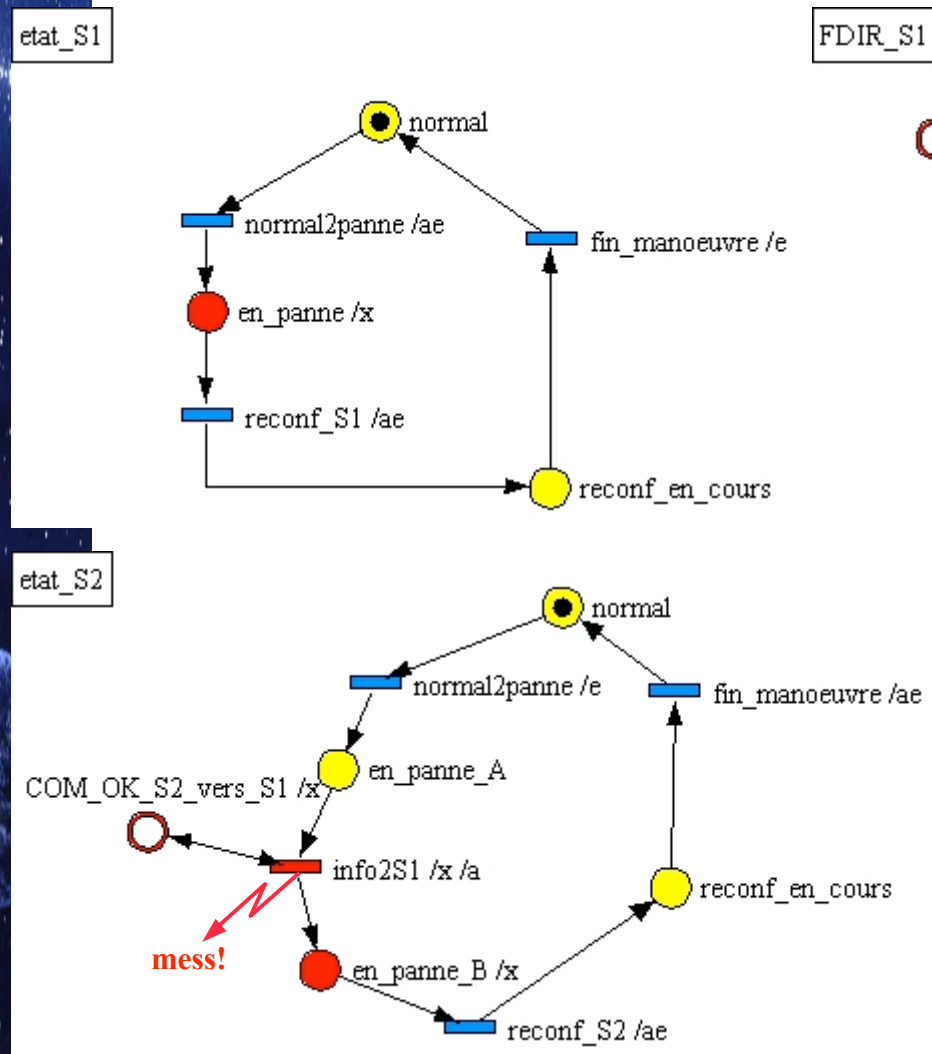
$anom\_S1? \in sat1.dispose\_de\_fdir.traite$

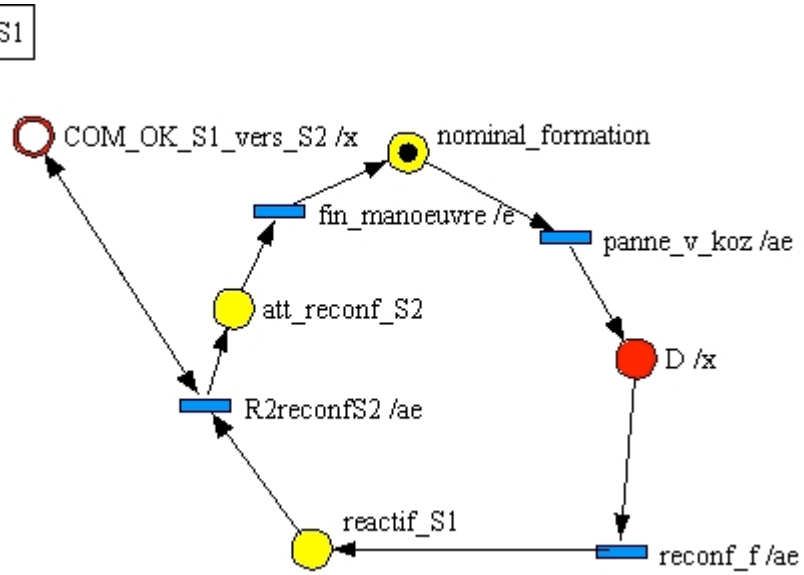
$anom\_S2? \in sat2.dispose\_de\_fdir.traite$

$sat1.dispose\_de\_fdir.detections \cap detections' \neq detections \cap sat1.dispose\_de\_fdir.detections$

$sat2.dispose\_de\_fdir.detections \cap detections' \neq detections \cap sat2.dispose\_de\_fdir.detections$

Simbol-X specification using Z and ProCoSA

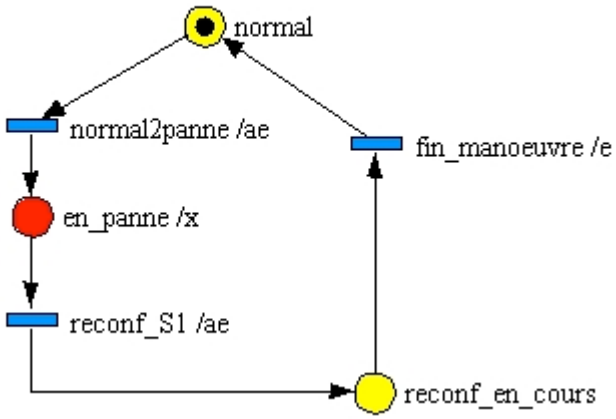




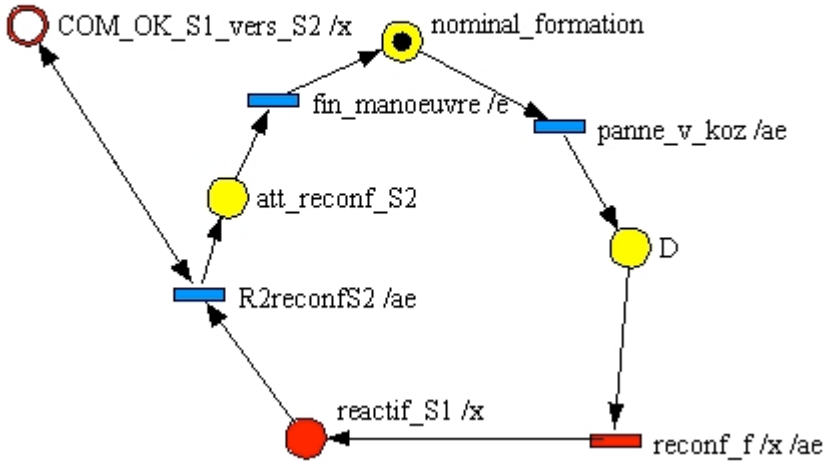
$$INFO2S1 \mathrel{\widehat=} [mess! : MESSAGE \mid mess! = messalarme]$$

Simbol-X specification using Z and ProCoSA

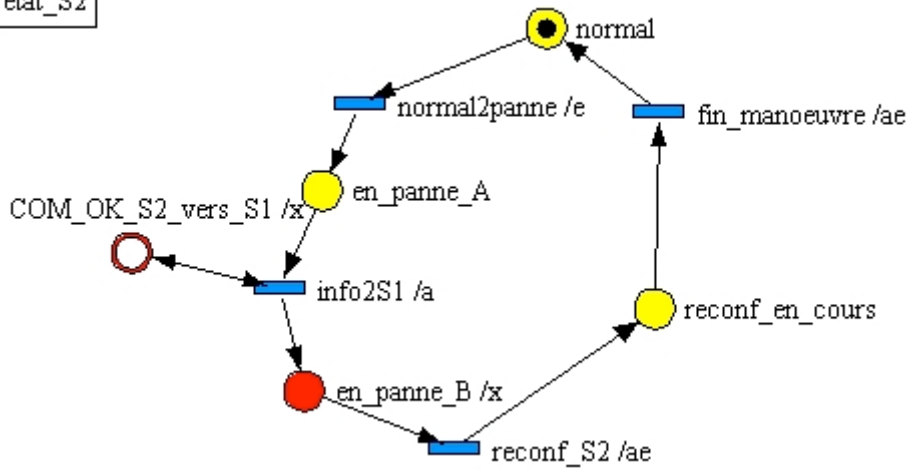
etat_S1



FDIR_S1



etat_S2

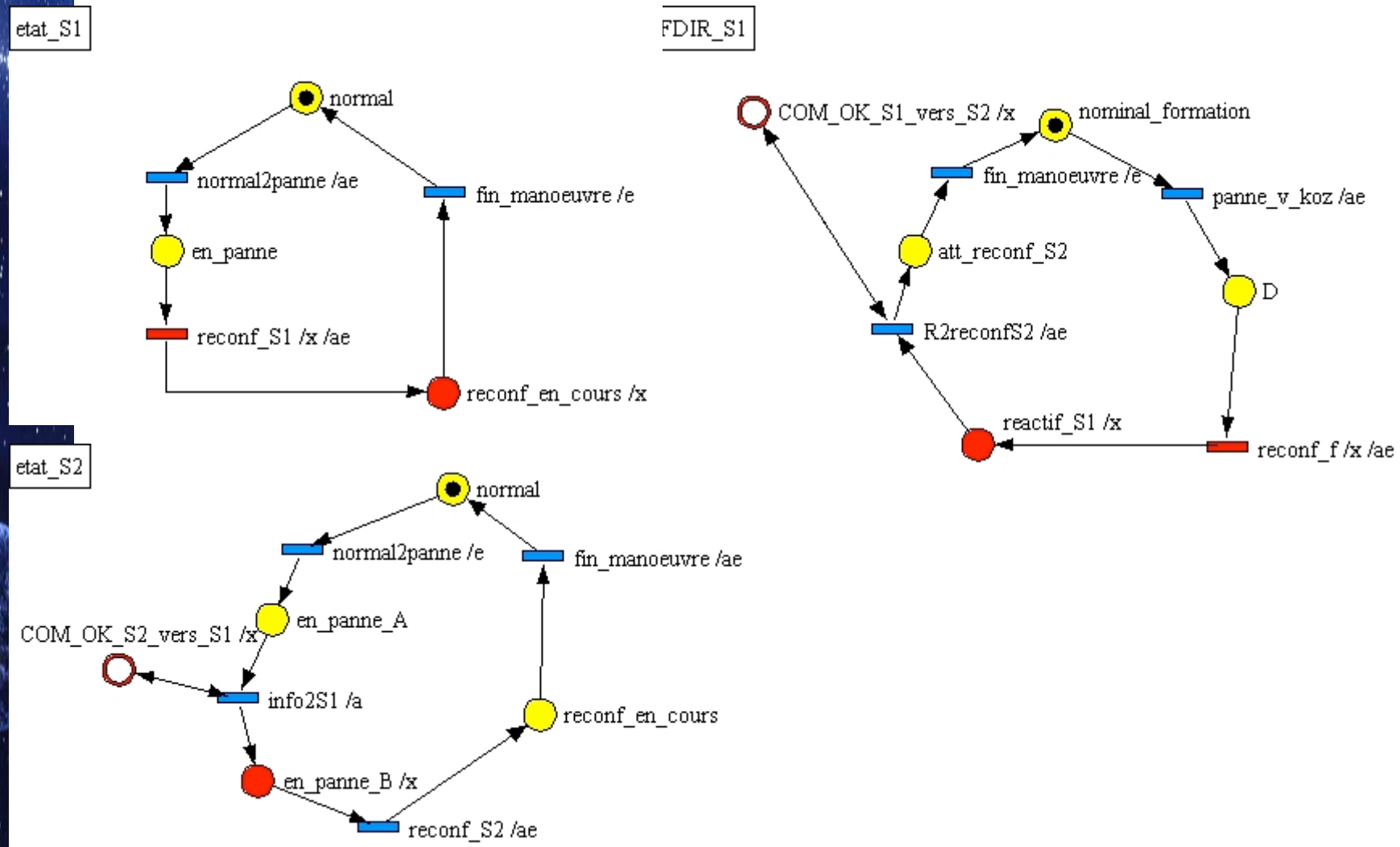


RECONF_F

$\Xi SIMBOLX$
$\Delta OPERATION$
$\Delta STRATEGIE\_FDIR$

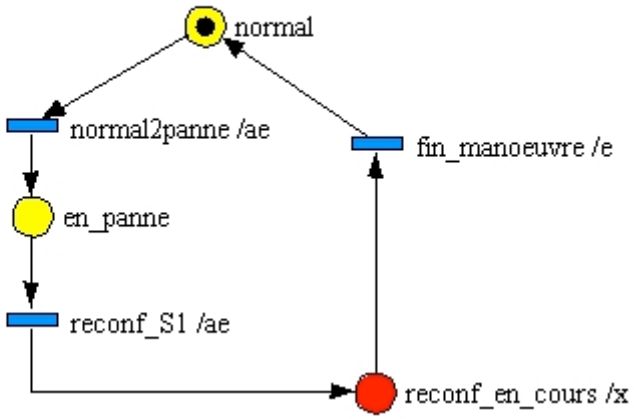
$nature' = manoeuvre$
$reconfig = \emptyset$
$reconfig' \neq \emptyset$

Simbol-X specification using Z and ProCoSA

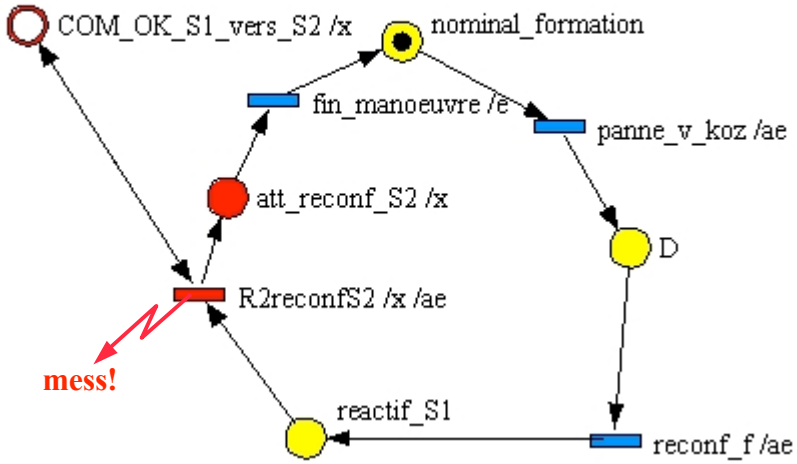


Simbol-X specification using Z and ProCoSA

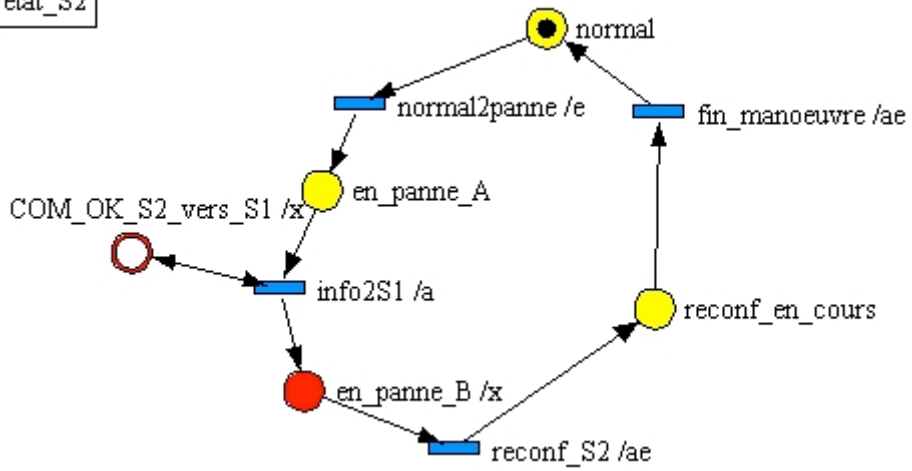
etat_S1



FDIR_S1

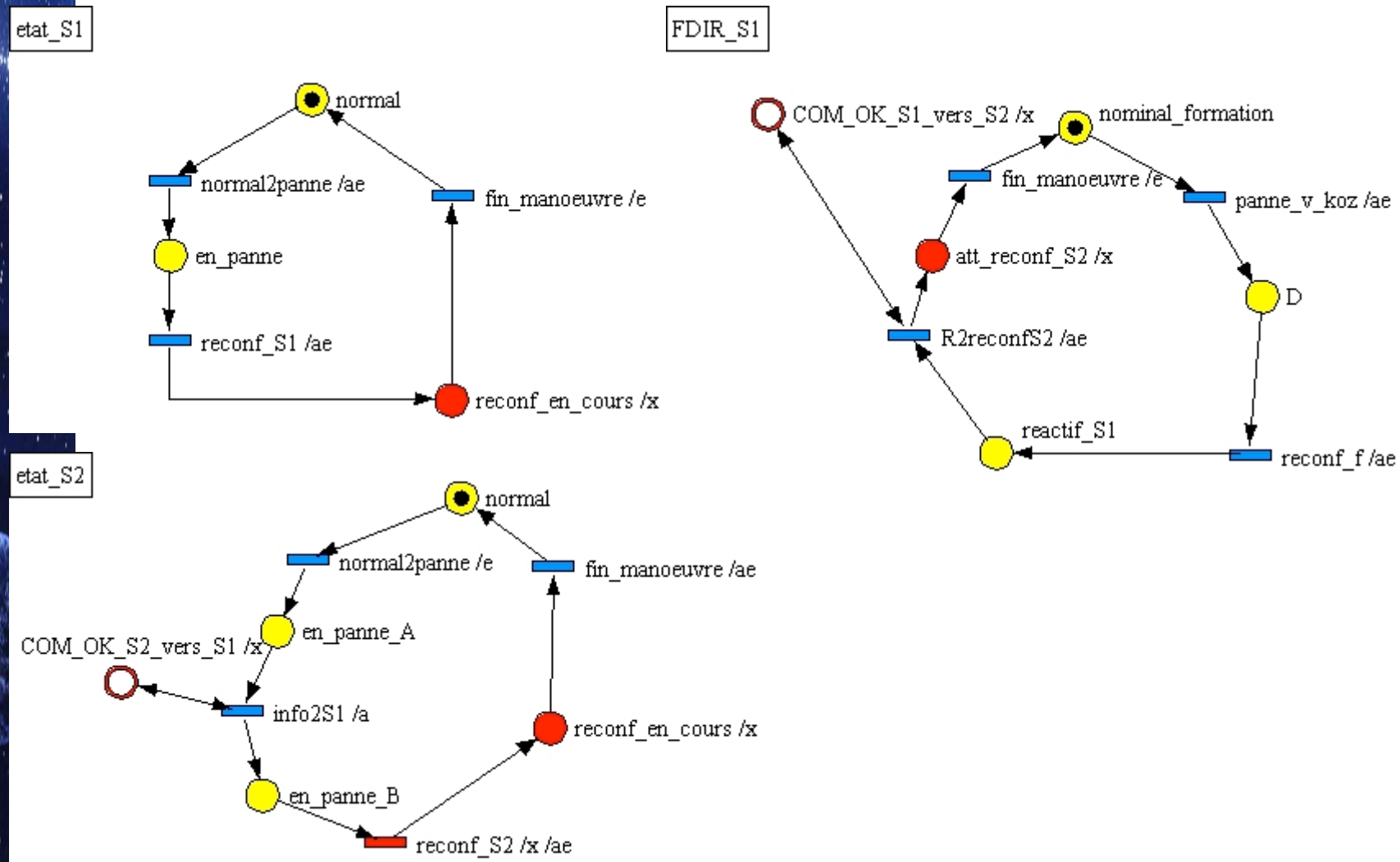


etat_S2

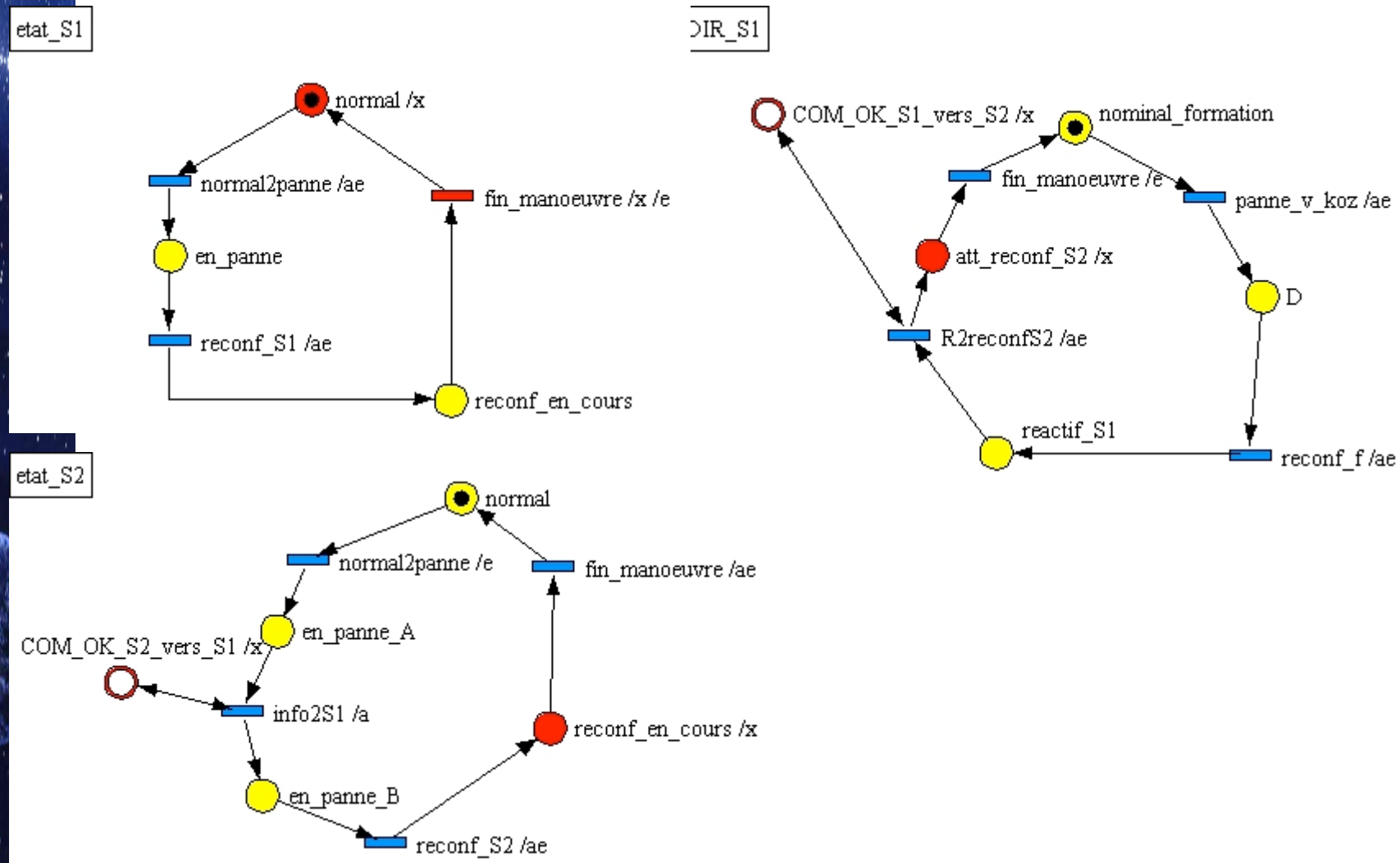


$$RECONF\_S2 \mathrel{\widehat=} [mess! : MESSAGE \mid mess! = messreconf \land mess! = messmanoeuvre]$$

Simbol-X specification using Z and ProCoSA

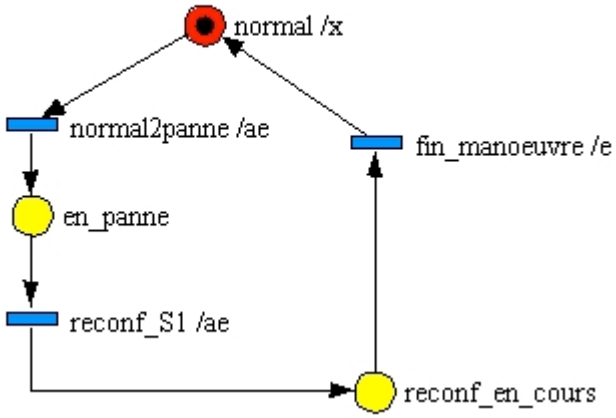


Simbol-X specification using Z and ProCoSA

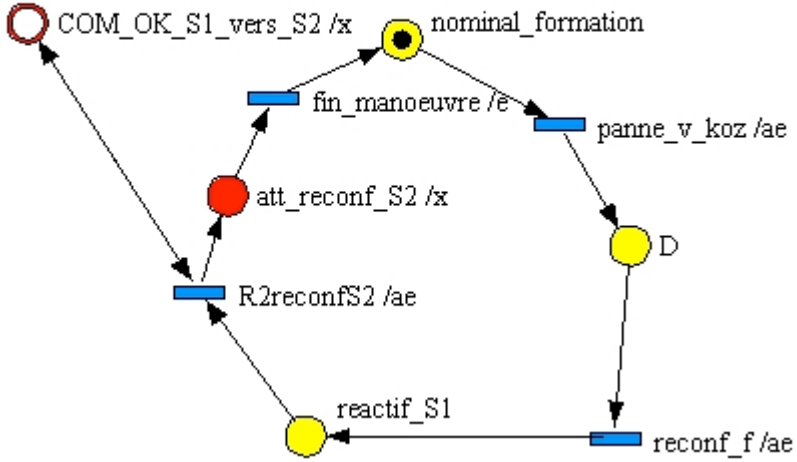


Simbol-X specification using Z and ProCoSA

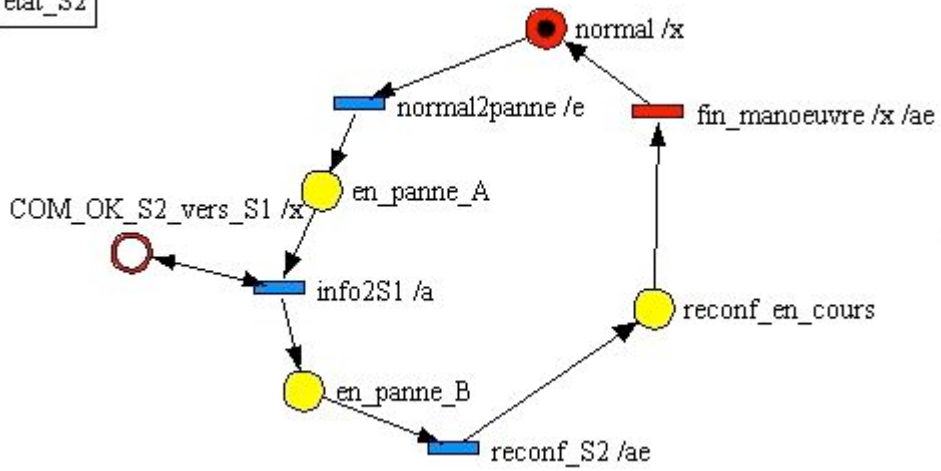
etat_S1



FDIR_S1

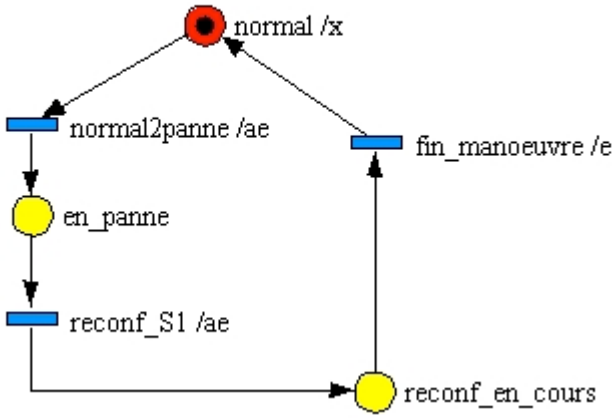


etat_S2

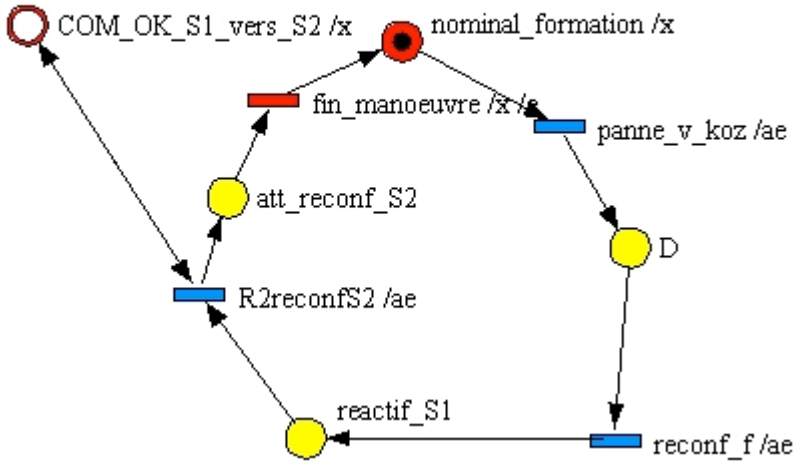


Simbol-X specification using Z and ProCoSA

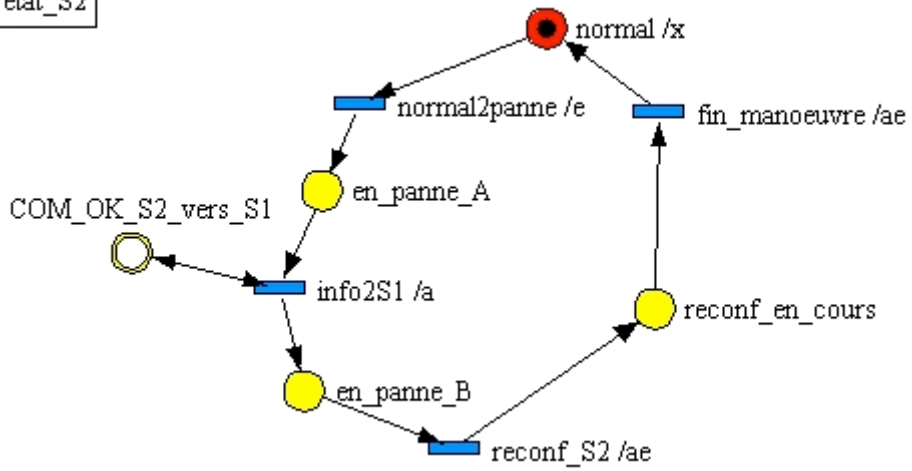
etat_S1



FDIR_S1



etat_S2



FIN_MANOEUVRE

$\Xi SIMBOLX$

$\Delta FORMATION$

$status\_vkoz = en\_panne$

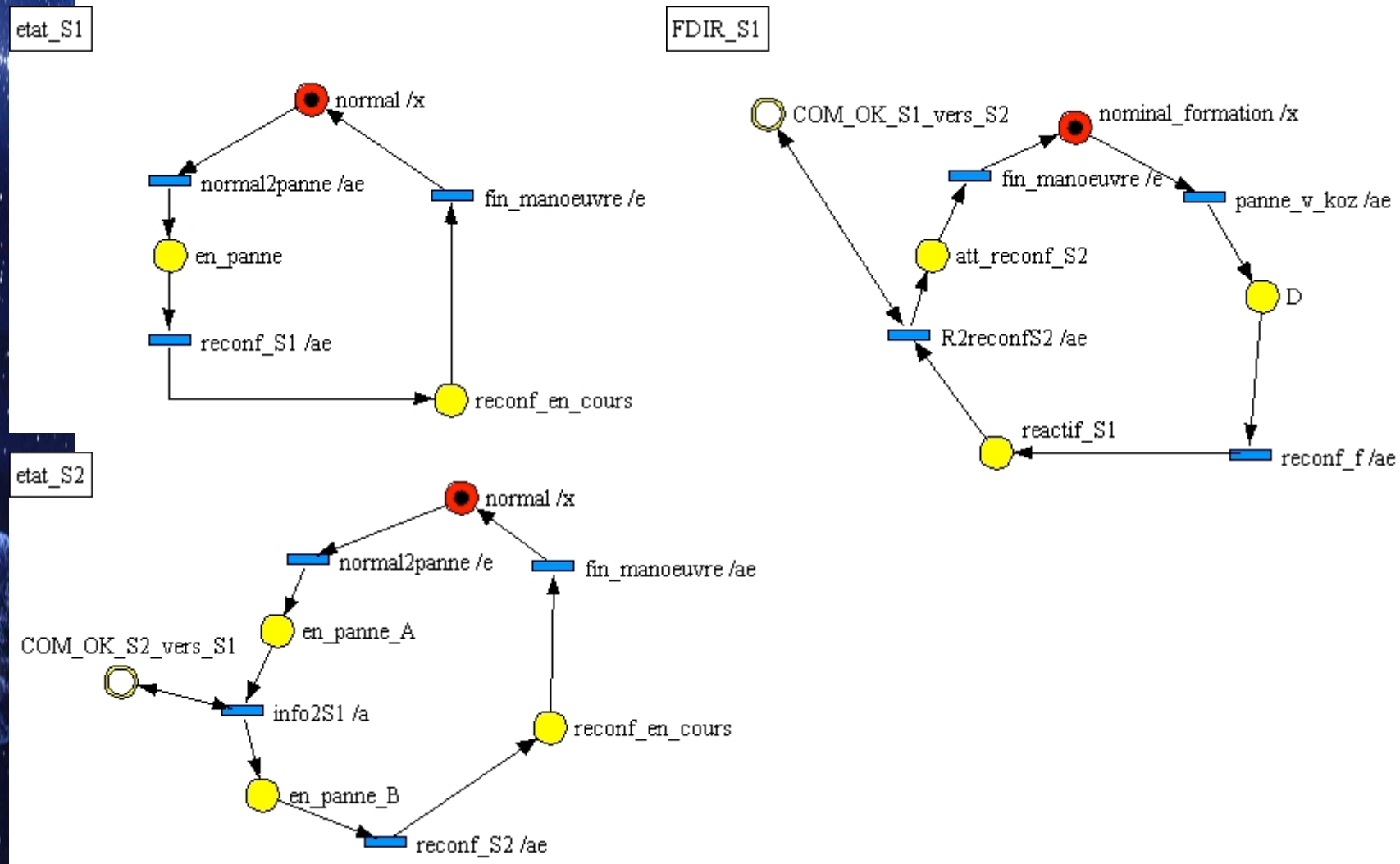
$status\_vkoz' = normal$

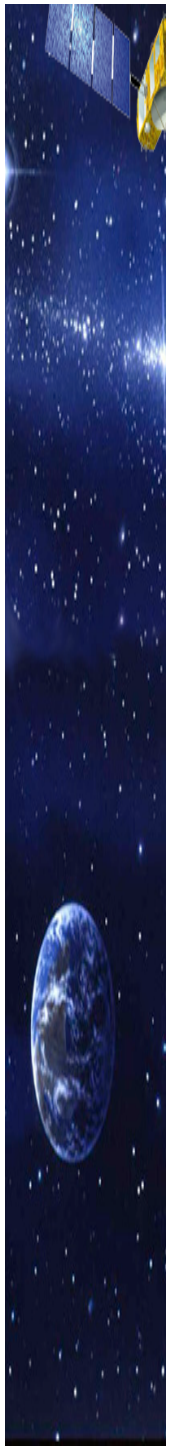
$(sat1, sat2) \in \mathrm{dom}\, distance$

$distance(sat1, sat2) \leq sat1.koz + sat2.koz$

$distance'(sat1, sat2) > sat1.koz + sat2.koz$

Simbol-X specification using Z and ProCoSA





Conclusion

- Linking Z and ProCoSA in a formal specification:

  Z : the formal data-oriented aspect

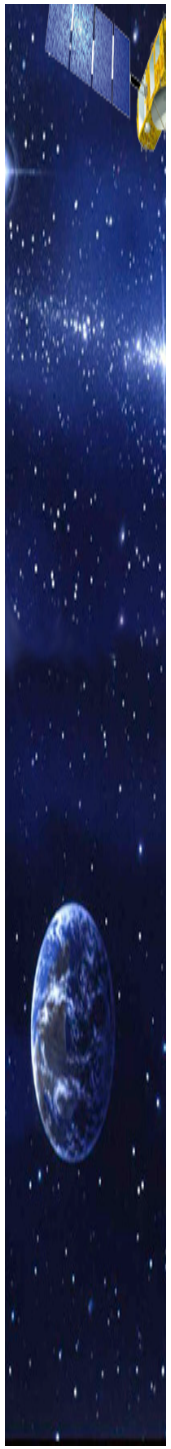
  ProCoSA : dynamic aspects , sequences of the state variations

- Benefits:

  better understanding of the formation behaviour

  clearer communication between project actors

  validation of some requirements



Future work

- Implement a hybrid simulation with discrete and continuous state variables
- Refine the simulation

  state duration, delay, concurrence
- Define a formal methodology combining Z and Petri net specifications