On the Architectures in Decentralized Supervisory Control

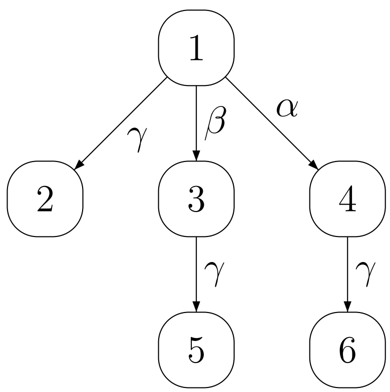
Sophie Pinchinat
IRISA-INRIA
Campus de Beaulieu
F-35042, Rennes
France
Sophie.Pinchinat@irisa.fr

joint work with

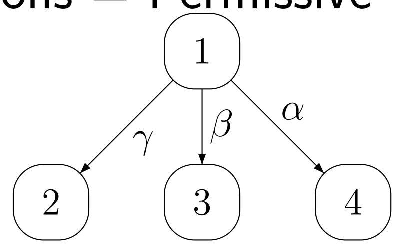
Stéphane Riedweg
Loria INRIA-Lorraine
Campus Scientifique
F-54506 Vandoeuvre-lès-Nancy
France
Stephane.Riedweg@loria.fr

An Introductory Example [Yoo-Lafortune02]

- $\Sigma_{o1} = \{\alpha\}$, $\Sigma_{o2} = \{\beta\}$, $\Sigma_{c1} = \Sigma_{c2} = \{\gamma\}$
- The C&P architecture
  Fusion Rule = Conjunction
  Local Decisions = Permissive



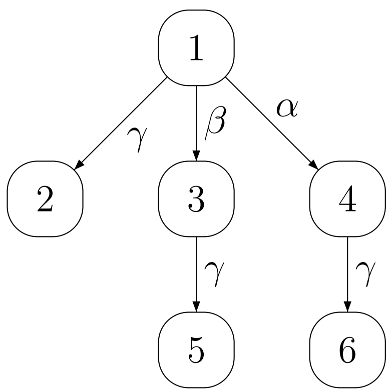
we want



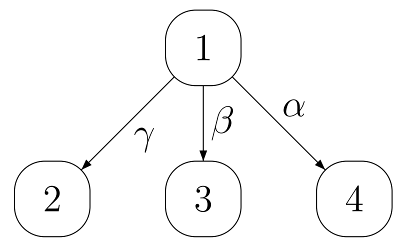
The Desired Behavior K

The uncontrolled system G

A Logical Specification of K



The uncontrolled system G

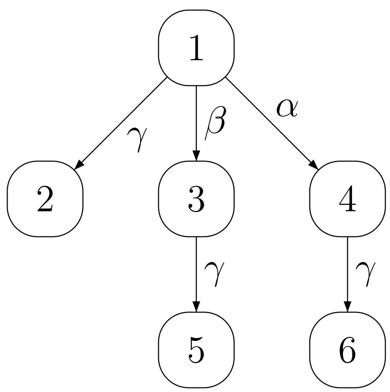


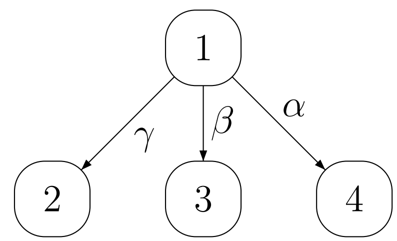
The Desired Behavior K

$$\langle\gamma\rangle\texttt{true} \;\wedge\; \langle\beta\rangle(\overbrace{\neg\langle\gamma\rangle\texttt{true}}^{\Delta_\gamma}) \;\wedge\; \langle\alpha\rangle(\overbrace{\neg\langle\gamma\rangle\texttt{true}}^{\Delta_\gamma})$$

The Desired Property ϕ_K

A Logical Specification of K





The Desired Behavior K

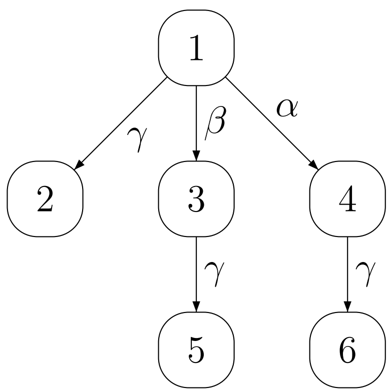
$\langle\gamma\rangle\texttt{true} \;\wedge\; \langle\beta\rangle(\;\Delta_\gamma\quad) \;\wedge\; \langle\alpha\rangle(\;\Delta_\gamma\quad)$

The uncontrolled system G

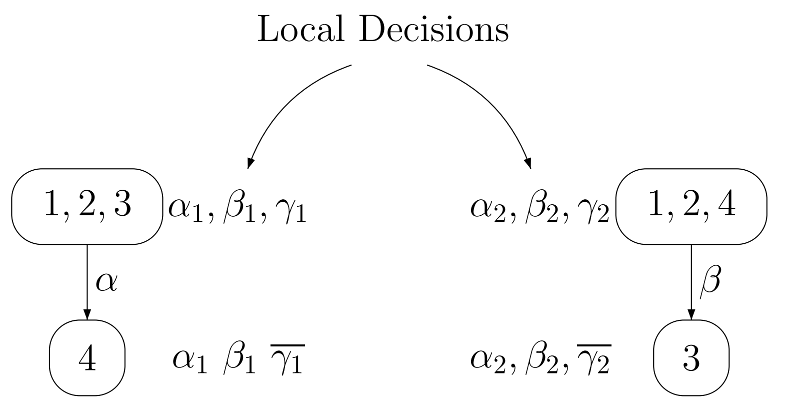
The Desired Property ϕ_K

The C&P Solution

$\langle\gamma\rangle\texttt{true} \;\wedge\; \langle\beta\rangle(\Delta_\gamma) \;\wedge\; \langle\alpha\rangle(\Delta_\gamma)$



The uncontrolled system G

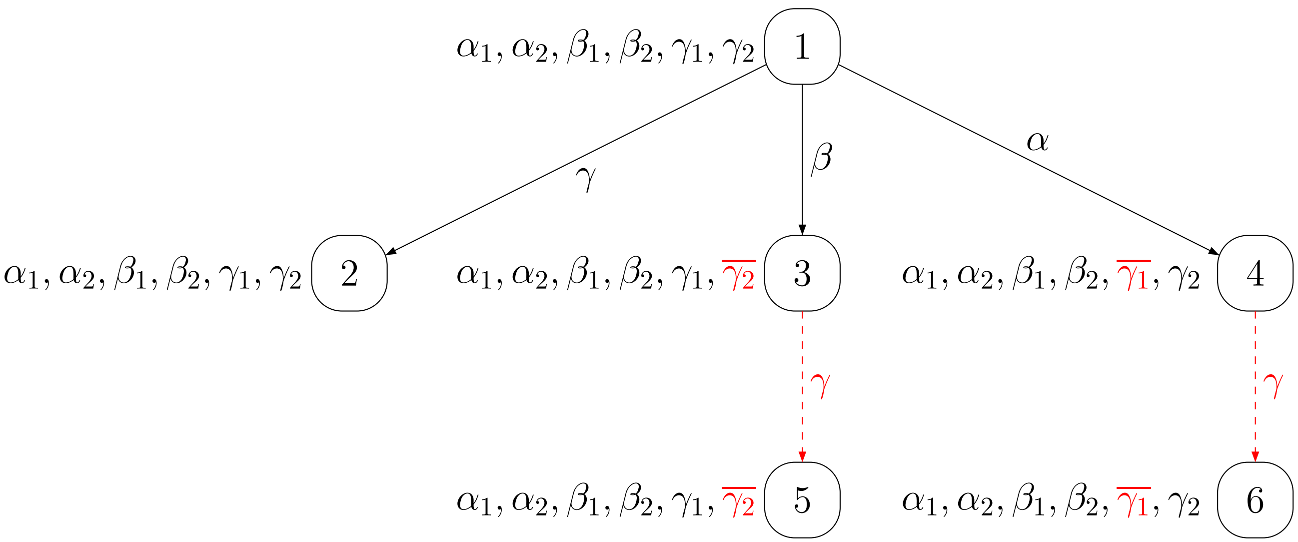


Supervisor S_1 Supervisor S_2

Put the decisions on G itself

A view of the controlled system $(S_1 \wedge S_2 / G)$

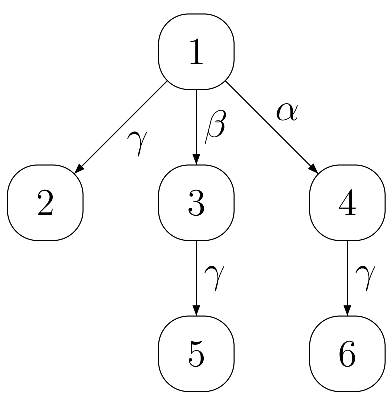
γ firable from state q whenever q is labeled γ_1 and q is labeled γ_2



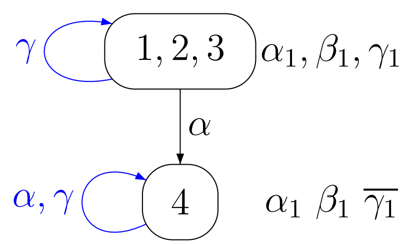
Label G with some synchronous product of completed automata

Labeling Processes

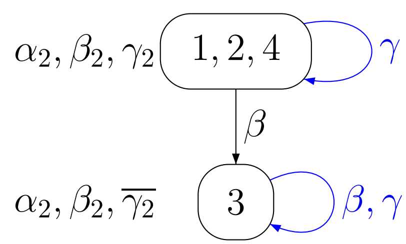
G



$\Lambda_1 =$ Completed S_1



$\Lambda_2 =$ Completed S_2



$Prop_1 = \{\alpha_1, \beta_1, \gamma_1\}$

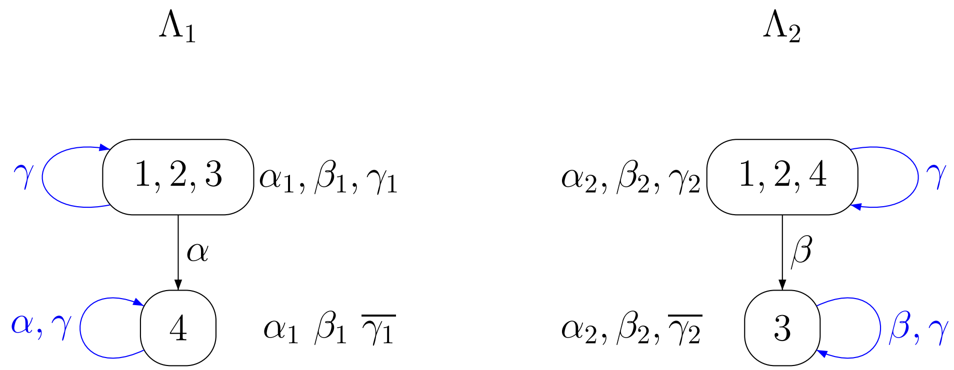
$\Sigma_1 = \{\alpha, \gamma\}, \Sigma_{o1} = \{\alpha\}$

$Prop_2 = \{\alpha_2, \beta_2, \gamma_2\}$

$\Sigma_2 = \{\alpha, \gamma\}, \Sigma_{o2} = \{\alpha\}$

Properties of a labeling process

Λ_1 verifies	$Inv(\beta_1)$	(since $\beta \notin \Sigma_1$)
	$Inv(\alpha_1)$	(since $\alpha \notin \Sigma_{c1}$)
	$Loop(\gamma_1)$	(since $\gamma \notin \Sigma_{o1}$)



Λ_i is permissive hence Λ_i verifies $\bigwedge_{\sigma \in \Sigma_c \setminus \Sigma_{o1}} Inv(\sigma_i)$

Properties of a labeling process

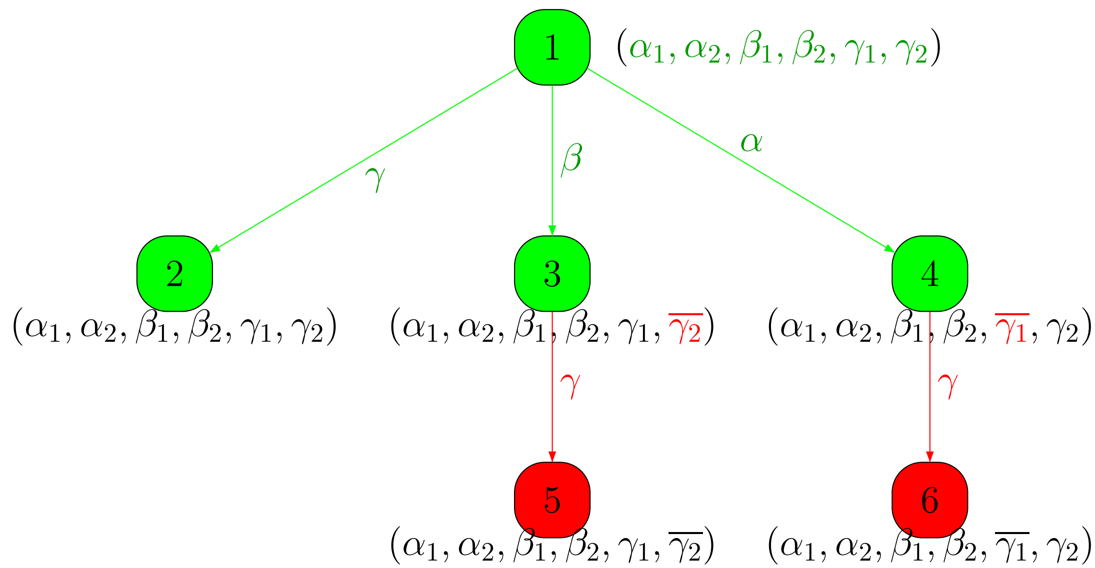
Λ_i is required to verify
$$\begin{cases} \text{Admissibility}: & \bigwedge_{\sigma \in \Sigma \setminus \Sigma_{ci}} Inv(\sigma_i) \\ \text{Observation}: & \bigwedge_{\sigma \in \Sigma_i \setminus \Sigma_{oi}} Loop(\sigma_i) \\ \ldots & \\ \text{Permissivity}: & \bigwedge_{\sigma \in \Sigma_c \setminus \Sigma_{c1}} Inv(\sigma_i) \\ \text{or Anti-Permissivity}: & \bigwedge_{\sigma \in \Sigma_c \setminus \Sigma_{c1}} Inv(\overline{\sigma_i}) \end{cases}$$

Properties of a labeling process

Λ_i is required to verify
$$\begin{cases} \text{Admissibility}: & \bigwedge_{\sigma\in\Sigma\setminus\Sigma_{ci}} Inv(\sigma_i) \\ \text{Observation}: & \bigwedge_{\sigma\in\Sigma_i\setminus\Sigma_{oi}} Loop(\sigma_i) \\ \ldots & \\ \text{Permissivity}: & \bigwedge_{\sigma\in\Sigma_c\setminus\Sigma_{c1}} Inv(\sigma_i) \\ \text{or Anti-Permissivity}: & \bigwedge_{\sigma\in\Sigma_c\setminus\Sigma_{c1}} Inv(\neg\sigma_i) \end{cases}$$

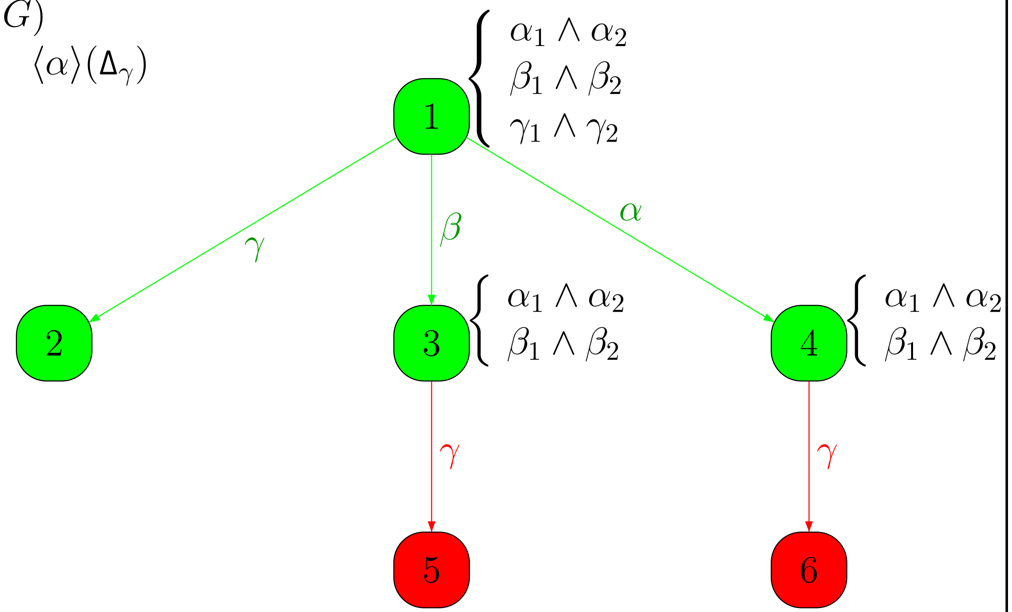
$Inv(.)$ and $Loop(.)$ are expressible in the logic

The controlled system $(S_1 \wedge S_2 / G)$



The controlled system $(S_1 \wedge S_2 / G)$

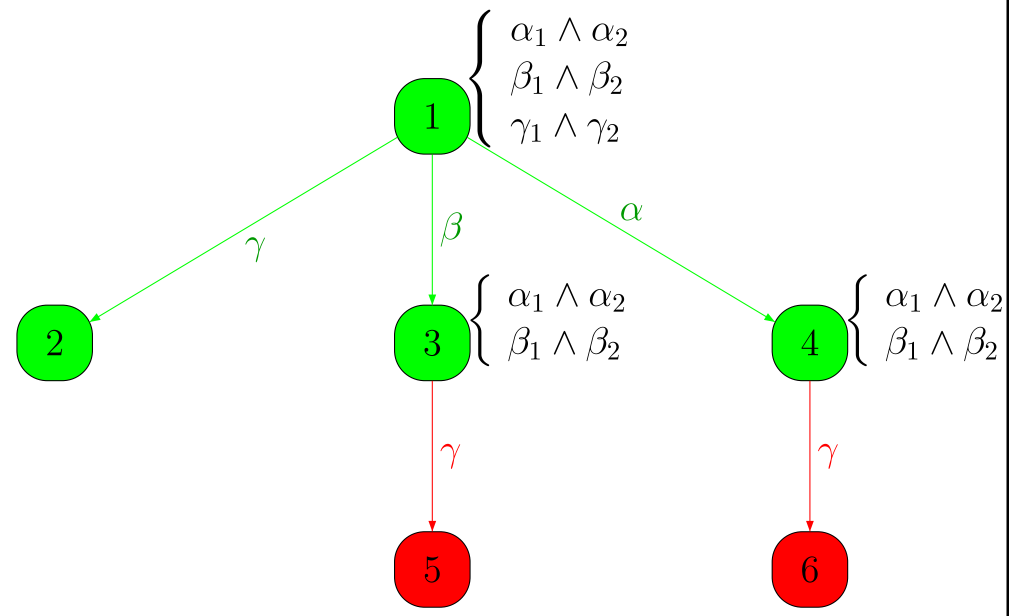
The controlled system $(S_1 \wedge S_2 / G)$
verifies $\langle\gamma\rangle\texttt{true} \;\wedge\; \langle\beta\rangle(\Delta_\gamma) \;\wedge\; \langle\alpha\rangle(\Delta_\gamma)$



Because the resulting labeling fulfills something

G (+ labels) verifies

$$\begin{cases} \gamma_1 \wedge \gamma_2 \wedge \langle\gamma\rangle\texttt{true} \\ \wedge \\ \beta_1 \wedge \beta_2 \wedge \langle\beta\rangle(\neg(\gamma_1 \wedge \gamma_2)) \\ \wedge \\ \alpha_1 \wedge \alpha_2 \wedge \langle\alpha\rangle(\neg(\gamma_1 \wedge \gamma_2)) \end{cases}$$

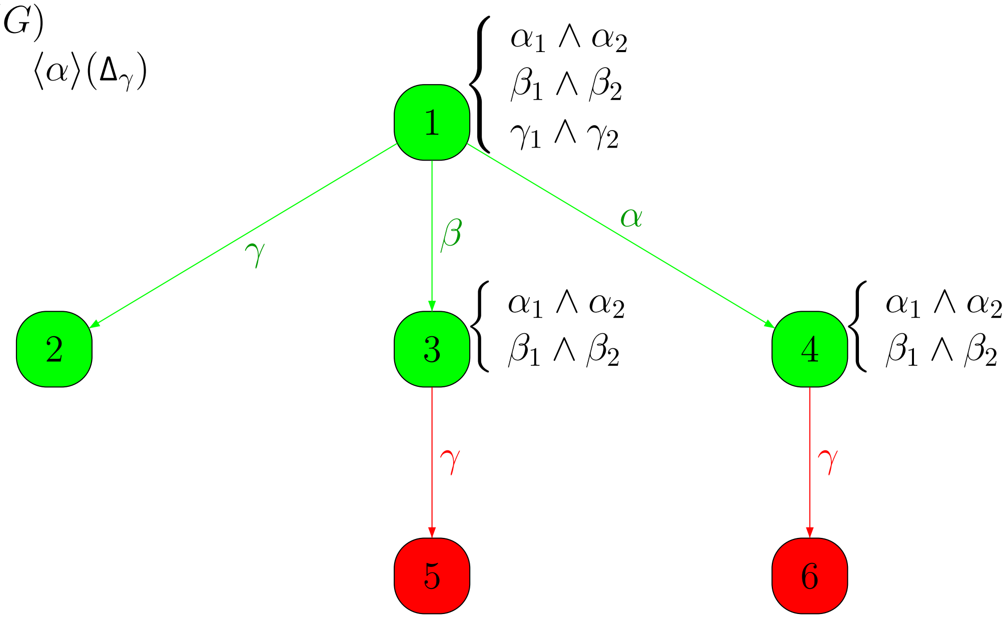


The resulting labeling fulfills the desired behavior ϕ_K

The controlled system $(S_1 \wedge S_2 / G)$
verifies $\langle\gamma\rangle\mathtt{true} \;\wedge\; \langle\beta\rangle(\Delta_\gamma) \;\wedge\; \langle\alpha\rangle(\Delta_\gamma)$

because

G (+ labels) verifies



$$\underbrace{\text{Relativization of } \phi_K}_{\tilde{\phi}_K^{\wedge}} \left\{ \begin{array}{l} \gamma_1 \wedge \gamma_2 \wedge \langle\gamma\rangle\mathtt{true} \\ \wedge \\ \beta_1 \wedge \beta_2 \wedge \langle\beta\rangle(\neg(\gamma_1 \wedge \gamma_2)) \\ \wedge \\ \alpha_1 \wedge \alpha_2 \wedge \langle\alpha\rangle(\neg(\gamma_1 \wedge \gamma_2)) \end{array} \right.$$

The Relativization according to $\wedge$

THEOREM

$(S_1 \wedge S_2/G)$	verifies	$\langle\sigma\rangle\phi$	resp.	$\phi_1 \wedge \phi_2$,	$\neg\phi$,	Δ_σ,	*true* ...
if and only if		$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
G (+ labels)	verifies	$\underbrace{\sigma_1 \wedge \sigma_2 \wedge \langle\sigma\rangle(\overset{\sim\wedge}{\phi})}$	resp.	$\underbrace{(\overset{\sim\wedge}{\phi_1}) \wedge (\overset{\sim\wedge}{\phi_2})}$,	$\underbrace{\neg(\overset{\sim\wedge}{\phi})}$,	$\underbrace{\neg(\sigma_1 \wedge \sigma_2) \vee \Delta_\sigma}$,	*true*...

The Relativization according to $\vee$

THEOREM

$(S_1 \vee S_2/G)$	verifies	$\langle\sigma\rangle\phi$	resp.	$\phi_1 \wedge \phi_2$,	$\neg\phi$,	Δ_σ,	*true* ...
if and only if		$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
G (+ labels)	verifies	$\underbrace{\sigma_1 \vee \sigma_2 \wedge \langle\sigma\rangle(\overset{\sim\vee}{\phi})}$	resp.	$\underbrace{(\overset{\sim\vee}{\phi_1}) \wedge (\overset{\sim\vee}{\phi_2})}$,	$\underbrace{\neg(\overset{\sim\vee}{\phi})}$,	$\underbrace{\neg(\sigma_1 \vee \sigma_2) \vee \Delta_\sigma}$,	*true*...

The Relativization according to $\vee$

THEOREM

$(S_1 \vee S_2/G)$	verifies	$\langle\sigma\rangle\phi$	resp.	$\phi_1 \wedge \phi_2$,	$\neg\phi$,	Δ_σ,	*true* ...
if and only if		$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
G (+ labels)	verifies	$\underbrace{\sigma_1 \vee \sigma_2 \wedge \langle\sigma\rangle(\overset{\sim\vee}{\phi})}$	resp.	$\underbrace{(\overset{\sim\vee}{\phi_1}) \wedge (\overset{\sim\vee}{\phi_2})}$,	$\underbrace{\neg(\overset{\sim\vee}{\phi})}$,	$\underbrace{\neg(\sigma_1 \vee \sigma_2) \vee \Delta_\sigma}$,	*true*...

Relativization according to Fusion Rules

Conjunctive : $(\overset{\sim\wedge}{\langle\sigma\rangle}\phi) = \sigma_1 \wedge \ldots \wedge \sigma_n \wedge \langle\sigma\rangle(\overset{\sim\wedge}{\phi})$

Disjunctive : $(\overset{\sim\vee}{\langle\sigma\rangle}\phi) = \sigma_1 \vee \ldots \vee \sigma_n \wedge \langle\sigma\rangle(\overset{\sim\vee}{\phi})$

The Relativization according to Fusion Rules

THEOREM

$(S_1 \vee S_2 / G)$ verifies $\langle\sigma\rangle\phi$ resp. $\phi_1 \wedge \phi_2$, $\neg\phi$, Δ_σ, *true* ...

if and only if $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$

G (+ labels) verifies $\underbrace{\sigma_1 \vee \sigma_2 \wedge \langle\sigma\rangle(\overset{\sim\vee}{\phi})}$ resp. $\underbrace{(\overset{\sim\vee}{\phi_1}) \wedge (\overset{\sim\vee}{\phi_2})}$, $\underbrace{\neg(\overset{\sim\vee}{\phi})}$, $\underbrace{\neg(\sigma_1 \vee \sigma_2) \vee \Delta_\sigma}$, *true*...

Relativization according to Fusion Rules

$$\text{Other kind : } \overset{\sim FR}{(\langle\alpha\rangle\phi)} = \overbrace{[(\alpha_1 \wedge \alpha_2) \vee (\alpha_2 \wedge \alpha_3) \vee (\alpha_1 \wedge \alpha_3)]}^{\text{Majority}} \wedge \langle\alpha\rangle(\overset{\sim FR}{\phi})$$

The Relativization according to Fusion Rules

THEOREM

$(S_1 \vee S_2/G)$ verifies $\langle\sigma\rangle\phi$ resp. $\phi_1 \wedge \phi_2$, $\neg\phi$, Δ_σ, $true$ ...

if and only if $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$

G (+ labels) verifies $\underbrace{\sigma_1 \vee \sigma_2 \wedge \langle\sigma\rangle(\overset{\sim\vee}{\phi})}$ resp. $\underbrace{(\overset{\sim\vee}{\phi_1}) \wedge (\overset{\sim\vee}{\phi_2})}$, $\underbrace{\neg(\overset{\sim\vee}{\phi})}$, $\underbrace{\neg(\sigma_1 \vee \sigma_2) \vee \Delta_\sigma}$, $true$...

Relativization according to Fusion Rules

and if α is fired then global agreement on β
(the formula $\wedge[\alpha](\beta_1 \wedge \beta_2 \wedge \beta_3)$)

$$\text{Other kind :} \quad \overset{\sim FR}{(\langle\alpha\rangle\phi)} = [\overbrace{(\alpha_1 \wedge \alpha_2) \vee (\alpha_2 \wedge \alpha_3) \vee (\alpha_1 \wedge \alpha_3)}^{\text{Majority}}] \wedge \langle\alpha\rangle(\overset{\sim FR}{\phi})$$

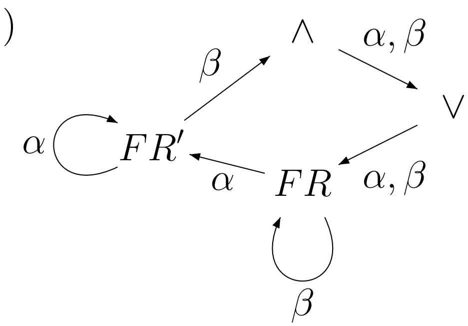
About Fusion Rules

Conjunctive : $(\langle \overset{\sim\wedge}{\sigma} \rangle \phi) = \sigma_1 \wedge \ldots \wedge \sigma_n \wedge \langle \sigma \rangle (\overset{\sim\wedge}{\phi})$

Disjunctive : $(\langle \overset{\sim\vee}{\sigma} \rangle \phi) = \sigma_1 \vee \ldots \vee \sigma_n \wedge \langle \sigma \rangle (\overset{\sim\vee}{\phi})$

Majority + "Agreement" : $(\langle \overset{\sim FR}{\alpha} \rangle \phi) = [(\alpha_1 \wedge \alpha_2) \vee (\alpha_2 \wedge \alpha_3) \vee (\alpha_1 \wedge \alpha_3) \wedge [\alpha](\beta_1 \wedge \beta_2 \wedge \beta_3)] \wedge \langle \alpha \rangle (\overset{\sim FR}{\phi})$

Dynamic change of Fusion Rules : $(\langle \overset{\sim FR}{\alpha} \rangle \phi) = formula(\vec{\alpha}, \vec{\beta}, \vec{\gamma}) \wedge \langle \alpha \rangle (\overset{\sim FR'}{\phi})$



.
.
.

Inifintely many kinds

Realizability Problem

- You want to achieve ϕ with a given ARCH :

  Fusion Rules for each $\sigma \in \Sigma$ (and a graph between them)

  Build the formula $(\overset{\sim FR}{\phi})$

  Local Decisions for each supervisor

  eg

  S_i observes Σ_{oi} and controls Σ_{ci}

  $\bigwedge_{\sigma \in \Sigma \setminus \Sigma_{oi}} Loop(\sigma_i) \wedge \bigwedge_{\sigma \in \Sigma \setminus \Sigma_{ci}} Inv(\sigma_i)$

  Build the formulas φ_i for each S_i

- In the paper, the logical counterpart of ARCH is $(\{\varphi_i\}, (\sim^{FR}))$

Specifying Realizability Problem

- In the paper, ϕ can be realized with ARCH on G

$$\text{iff} \qquad G \text{ verifies } \exists(\Lambda_1 \text{ satifying } \varphi_1)\ldots\exists(\Lambda_n \text{ satifying } \varphi_n).\ (\overset{\sim FR}{\phi})$$

- The semantics of such formulas is clean for any Mu-calculus definable Desired Behavior ϕ (any ω-regular tree language)
- The verification is decidable (and synthesis as well) whenever

$$\Sigma_{ok_1} \supseteq \Sigma_{ok_2} \supseteq \ldots \Sigma_{ok_n} \quad \text{[P\&Riedweg05]}$$

- Retrieving the pipeline of [Pnueli&Rosner92]
  see also X. Briand's "well-synchronized" assumption
- In the paper, also full decidability with complete information

Thank you !!

Sophie Pinchinat
IRISA-INRIA
Campus de Beaulieu
F-35042, Rennes
France
Sophie.Pinchinat@irisa.fr

Stéphane Riedweg
Loria INRIA-Lorraine
Campus Scientifique
F-54506 Vandoeuvre-lès-Nancy
France
Stephane.Riedweg@loria.fr